CUADERNOS
DE LA FUNDACIÓN

C / 229

Las aplicaciones del *Big Data* en el ámbito asegurador y el tratamiento legal de sus datos

Una perspectiva desde el derecho internacional privado

Alfonso Ortega Giménez

Fundación
MAPFRE

Área de Seguro y Previsión Social

Las aplicaciones del *Big Data* en el ámbito asegurador y el tratamiento legal de sus datos

Una perspectiva desde el derecho internacional privado

Alfonso Ortega Giménez

Fundación MAPFRE

Paseo de Recoletos, 23
28004 Madrid (España)

www.fundacionmapfre.org

ISBN: 978-84-9844-723-1
Depósito Legal: M-9617-2019
Maquetación y producción editorial: Edipack Gráfico

PRESENTACIÓN

Desde 1975 Fundación MAPFRE desarrolla actividades de interés general para la sociedad en distintos ámbitos profesionales y culturales, así como acciones destinadas a la mejora de las condiciones económicas y sociales de las personas y de los sectores menos favorecidos de la sociedad.

El área de Seguro y Previsión Social trabaja con el objetivo de promover y difundir el conocimiento y la cultura del seguro y la previsión social.

En cuanto a las actividades orientadas hacia la sociedad en general, creamos contenidos gratuitos y universales en materia de seguros que divulgamos a través de la página web Seguros y Pensiones para Todos. Organizamos actividades educativas y de sensibilización mediante cursos de formación para el profesorado, talleres para escolares y visitas gratuitas para grupos al Museo del Seguro. Asimismo, publicamos guías divulgativas para dar a conocer aspectos básicos del seguro.

Además de esta labor divulgativa, apoyamos la investigación mediante la publicación de informes sobre mercados aseguradores y otros temas de interés, la concesión de ayudas para la investigación en seguros y previsión social, la publicación de libros y cuadernos de temática aseguradora y la organización de jornadas y seminarios. Nuestro compromiso con el conocimiento se materializa en un centro de documentación especializado que da soporte a todas nuestras actividades y que está abierto al público en general.

Dentro de estas actividades se encuadra la concesión de una Ayuda a la Investigación "Ignacio H. de Larramendi" 2016 en Seguros a: Alfonso Ortega Giménez, para el desarrollo del trabajo de investigación titulado: *Las aplicaciones del* Big Data *en el ámbito asegurador y el tratamiento legal de sus datos*, tutorizado por Elena Mora González, subdirectora de Marco Regulatorio de Seguridad de MAPFRE.

Todas nuestras actividades se encuentran disponibles y accesibles en Internet, para usuarios de todo el mundo, de una manera rápida y eficaz, a través de nuestra página web: www.fundacionmapfre.org.

Fundación MAPFRE

Alfonso Ortega Giménez es doctor en Derecho, 2014; Premio extraordinario de Doctorado, 2018; licenciado en Derecho, 2000; y máster en Comercio Internacional también por la Universidad de Alicante, 2001. Profesor contratado doctor de Derecho internacional privado de la Universidad Miguel Hernández de Elche. Vicedecano de Grado en Derecho de la Facultad de Ciencias Sociales y Jurídicas de Elche. Ha sido subdirector del máster en Comercio Internacional, organizado por la Universidad de Alicante durante los cursos académicos 2007/2008 a 2017/2018. Director del máster *online* en Internacionalización de la Empresa (MIE), organizado por el Instituto Superior de Derecho y Economía (ISDE). Director del Observatorio Provincial de la Inmigración de Alicante. Reconocidos dos Sexenios de Investigación correspondientes al tramo 2009-2017 por la CNEAI y al tramo 2010-2016 por la AVAP. Nombrado, recientemente, académico de honor por la Junta de Gobierno de la Academia Internacional de Ciencias, Tecnología, Educación y Humanidades.

Consultor de derecho internacional privado de la Universitat Oberta de Catalunya (UOC). Consejero académico de PELLICER & HEREDIA ABOGADOS. Director del Observatorio provincial de Inmigración de Alicante desde 2016. Director del Observatorio de la Inmigración de la ciudad de Elche, 2011-2015; y vocal del Observatorio Valenciano de la Inmigración.

Miembro del Consejo Asesor de la revista *Economist & Jurist*. Miembro del Consejo Asesor de *Barataria. Revista Castellano-Manchega de Ciencias Sociales*. Responsable de la sección de derecho internacional privado de la *Revista Boliviana de Derecho* y del Instituto de Derecho Iberoamericano (IBIDE). Miembro del Consejo de Redacción de la revista *Actualidad Jurídica Iberoamericana.*

Ha recibido numerosos premios en investigación y a la excelencia en la práctica jurídica, a la productividad investigadora, así como al talento docente. Ponente habitual en numerosos cursos organizados en España y en el extranjero en materia de derecho internacional privado, derecho de la nacionalidad, derecho de extranjería, derecho del comercio internacional, contratación internacional y protección de datos de carácter personal, entre otros.

Autor de multitud de artículos publicados en revistas científicas, técnicas y de divulgación, españolas y extranjeras; además de participar como autor, coautor, y/o director o coordinador en más de 110 libros.

ÍNDICE

RESUMEN

El presente trabajo tiene como fin abordar las implicaciones legales del *Big Data,* en especial su incidencia en la protección de datos en el entorno asegurador.

El estudio se ha desarrollado en torno a la explicación de lo que entendemos por *Big Data,* elemento cuya explicación no resulta tan sencilla vista las diferentes posturas que puede dar la doctrina, y, en concreto, sobre las características más relevantes del concepto, y la continua evolución de la cual es objeto; además del uso de otras tecnologías como el *Cloud Computing* y su relación con el *Big Data*.

Hemos podido observar los diferentes tipos de datos personales que son utilizados en el *Big Data,* que provienen de muy diversas fuentes que todos poseemos, como p. ej. ordenadores, *smartphones, smartwatches,* o cualquier dispositivo con acceso a Internet que sea capaz de generar datos. A su vez, tales datos son clasificados según sea su origen (medio generado) y el medio por los cuales se recaban (mediante bases de datos o no).

Destacamos diferentes aplicaciones que puede tener el *Big Data* en el entorno asegurador: por un lado, la detección del fraude mediante la observación de determinados ítems relevantes como patrones de comportamiento; por otro lado, el análisis y tarificación del riesgo que podemos destacar, en concreto, en los seguros de automóvil y de salud, además de referenciar la elaboración de perfiles y los supuestos de gamificación que esto supone; y, finalmente, la fidelización del cliente.

De cualquier forma, las afecciones legales que supone el *Big Data* son varias. Por un lado, la implicación en la normativa de protección de datos personales que esto conlleva en lo relativo al cumplimiento de los principios rectores de la protección de datos, como el principio de minimización de datos y el principio de consentimiento como base jurídica para el tratamiento de datos. Se ha querido resaltar el importante riesgo que supone la elaboración de perfiles y el grave impacto que pueden llegar a tener en los derechos de los individuos. Tal es así que los posicionamientos realizados por varias instituciones internacionales demuestran la magnitud del problema. Por otro lado, los

mecanismos de defensa jurídica que podemos articular para defender dos de los elementos de los que una empresa aseguradora se nutre para aplicar el *Big Data,* como son el algoritmo y las bases de datos.

Hemos reflexionado acerca del concepto de dato personal, redefiniendo la importancia de este plasmado en el marco normativo de la protección de datos, y su implicación en el derecho fundamental a protección de datos derivado del artículo 18.4 CE que realiza la jurisprudencia española. Ha sido núcleo fundamental del trabajo el estudio de los posteriores apartados a la luz del RGPD, norma que viene a reformar el panorama europeo sobre la protección de datos. De ella, hemos analizado la definición de «dato personal» junto con los documentos que ha aportado el CEPD. A todo esto, a finales de 2017 fue publicado el PLOPD, texto que se pondrá en comparación tanto con el RGPD como con la LOPD vigente.

Ya que el *Big Data* implica el uso de varias calidades de datos, se ha visto necesario catalogar los diferentes datos personales generados por un individuo y que pueden ser utilizados por una empresa aseguradora.

Los datos generados por servicios de geolocalización presentan una gran fuente de información que genera tanto beneficios como perjuicios. Por eso se ha defendido que los datos derivados de los servicios de geolocalización deban incluirse dentro de los datos catalogados como sensibles; asimismo, los datos biométricos y los relacionados con la salud suponen también un gran activo para el *Big Data,* además de ser considerados como datos sensibles y, debido a ello, estar protegidos por los más altos niveles de seguridad que puede otorgar la legislación sobre protección de datos, y a los principios específicos que aporta el CEPD. En este sentido, el consentimiento explícito se erige como la base jurídica más utilizada para legitimar el tratamiento de los datos. El RGPD ha venido a modificar la definición de consentimiento con el fin de eliminar la posibilidad de la admisión del consentimiento tácito para el tratamiento de datos, al optar entre varios medios para declarar la afirmación al tratamiento; aunque el núcleo fundamental de la definición sigue intacto. La carga de la prueba deberá recaer sobre aquella entidad aseguradora que recabe el consentimiento.

Debido al gran riesgo que genera el tratamiento masivo de estos datos personales sensibles, la anonimización de los datos se presenta como solución, pero es uno de los

elementos más complicados y comprometidos de la protección de datos, puesto que la consecución de tal objetivo significa la no aplicación de la normativa sobre protección de datos y, por consiguiente, la exención de una gran cantidad de obligaciones civiles y administrativas.

La consideración de «tratamiento» sobre unos datos supone el punto de partida para la aplicación del marco normativo sobre protección de datos a unos supuestos de hecho marcados por la deslocalización del tratamiento. El RGPD no es ajeno al *Big Data*, y contempla un supuesto de hecho específico para sujetar a la norma cualquier tratamiento de datos que tenga como destino controlar el comportamiento humano. La deslocalización del tratamiento es otro de los supuestos modernos y derivados del auge de las nuevas tecnologías. El RGPD viene a tratar este problema mediante la aplicación extraterritorial de la norma cuando los datos tratados correspondan a residentes en la Unión. En este sentido, las transferencias internacionales de datos personales continúan siendo uno de los elementos más importantes de las normas de protección de datos. Esto se demuestra en la gran extensión de su régimen en comparación con lo estipulado en la directiva.

La institucionalización de las normas corporativas vinculantes supone una gran estandarización y normativización de uno de los pilares de las transferencias, con el objetivo de alcanzar una importancia similar a las cláusulas contractuales tipo, cuya seguridad está cuestionada. En consecuencia, con el refuerzo de las transferencias internacionales de datos, el *Privacy Shield* supone un nuevo régimen para las transferencias internacionales de datos con Estados Unidos, que sustituye al derogado *Safe Habour*, y aumenta la protección sobre los datos personales. Pero el Escudo no protege tanto como pretende ensalzar la Comisión Europea, como se ha visto reflejado en la última revisión.

Un gran avance para la protección del titular del derecho a la protección de datos es la regulación *ex novo* que realiza el RGPD respecto al derecho a la indemnización. La anterior directiva no resolvía de manera eficaz esta cuestión y la consecuencia resultante era un sistema desproporcional en la Unión Europea. Con la nueva regulación, el sistema creado responde a las necesidades de homogenización de una cuestión tan relevante como el derecho a la indemnización del afectado. Por ello, el RGPD ha creado nuevas normas de derecho internacional privado con el fin de proteger al afectado

en supuestos de vulneración de su derecho a la protección de datos. La posibilidad que otorga el reglamento de litigar en el propio domicilio del demandado cumple con la función protectora que siempre ha de tener una norma de protección de datos. La compatibilidad con el reglamento «Bruselas I bis» supone una ampliación de los foros disponibles, que variarán dependiendo del contrato en el que ejerciten tales acciones. Además, cabe destacar la posibilidad de no invocar la acción de responsabilidad del RGPD, sino reclamar a la entidad aseguradora por un incumplimiento contractual en el caso de haberse comprometido contractualmente a proteger los datos conforme a la legislación vigente.

SUMMARY

The purpose of this paper is to approach the legal implications of *Big Data,* especially its impact on data protection in the insurance environment.

The study has been developed around of what we mean by *Big Data,* an element whose explanation is not so simple given the different postures that can be given by the doctrine and, in particular, the most relevant features of the concept, and the continuous evolution of which it is object, besides the use of other technologies such as Cloud Computing and its relationship with *Big Data.*

We have been able to observe the different types of personal data that are used in the *Big Data,* which come from many different sources that we all have, such as computers, Smartphones, Smartwatches, or any device with Internet access that is capable of generating data. In turn, such data are classified according to their origin (generated medium) and according to the means by which they are collected (by databases or not).

We highligt the different applications that *Big Data* can have in the insurance environment. On the one hand, the detection of fraud by observing certain relevant items as behaviour patterns; and, on the other hand, risk analysis and pricing. Which can be highlighted, in particular, in auto and health insurance; in addition to reference the elaboration of profiles and the assumptions of gamification that this supposes, and finally, customer loyalty. Anyway, the legal conditions of the *Big Data* are various. On the one hand, it is remarkable the implication in the rules of personal data protection that this entails in respect of compliance with the guiding principles of data protection as the principle of data minimization and the principle of Consent as a legal basis for data processing. It was wanted to highlight the important risk involved in the development of profiles and the serious impact they may have on the rights of individuals. Such is the way the positions made by several international institutions demonstrate the magnitude of the problem. On the other hand, the legal defense mechanisms that we can articulate to defend two of the elements of which an insurance company nourishes to apply the *Big Data,* such as the algorithm and the bases of data.

We have reflected on the concept of personal data, redefining the importance of the concept embodied in the normative framework of data protection, and its implication in the fundamental right to data protection derived from Article 18.4 EC that carries out spanish jurisprudence. From it, the GDPR has been a fundamental nucleus of the work, a norm that reshapes the European panorama on data protection. From it, we have analysed the definition of «personal data» together with the documents provided by WP 29, and that in the light of both parties, there is hardly any difference with Directive 95/46. To all this, in June 2017 was published the Draft LOPD, text that is in some way with the GDPR as with the current LOPD.

Since *Big Data* implies the use of several data qualities, it has been necessary to catalogue the different personal data generated by an individual and that can be used by an insurance company.

The data generated by geolocation services present a great source of information that generates both benefits and damages. That is why it has been argued that data derived from geolocation services should be included within the data classified as sensitive; besides, biometric and health-related data are also a major asset for *Big Data*, as well as being considered as sensitive data and therefore protected by the highest levels of security that can be afforded by data protection legislation, And the specific principles provided by WP 29. Because of that, explicit consent is one of the most used legal bases to legitimize the treatment of data. The GDPR has modified the definition of consent in order to eliminate the possibility of admitting tacit consent for data processing, choosing among several means to declare the claim to treatment; Although the core of the definition remains intact. The burden of proof must be borne by the insurer seeking the consent.

Due to the great risk that the massive treatment of this sensitive personal data generates, data anonymisation is one of the most complicated and compromised elements of data protection, since the achievement of such an objective means the non-application of data protection regulations and, consequently, the exemption of a large number of civil and administrative obligations.

The consideration of 'processing' on data is the starting point for the application of the regulatory framework on data protection to factual assumptions marked by the

delocalisation of treatment. The GDPR is no stranger to *Big Data*, and contemplates a specific case of fact to subject to the norm any data treatment that has as a destination to control human behaviour. The relocation of treatment is another of the modern assumptions and derived from the rise of new technologies. GDPR addresses this problem through the extraterritorial application of the standard when the data processed correspond to residents in the Union. In this sense, international data transfers continue to be one of the most important elements of personal data protection standards. This is demonstrated by the large extent of its scheme compared to the provisions of the Directive.

The institutionalization of the Binding Corporate Rules means a great standardization and regulation of one of the pillars of the transfers, with the aim of achieving a similar importance to standard contractual clauses, whose safety is questioned. Consequently, with the strengthening of international data transfers, the Privacy Shield is a new regime for international data transfers with the United States, replacing the repealed *Safe Harbour*, and increasing the protection of personal data. But the shield does not protect as much as the European Commission wishes to extol. But the shield does not protect as much as the European Commission wants to praise and has been reflected in the latest revision.

A breakthrough for the protection of the holder of the right to data protection in the GDPR regulation on the right to compensation. The previous Directive did not resolve this issue effectively and the consequence was a disproportionate system in the European Union. With the new regulation, the system created responds to the needs of homogenization of a matter as relevant as the right to compensation for damages. Due to this, the GDPR has created new rules of private international law in order to protect those affected in cases of vulnerability of their right to data protection. The possibility given by the Regulation to litigate in the defendant's own home fulfils the protective function that a data protection standard must always have. The compatibility with the «Brussels I bis» Regulation is an extension of the available forums, which vary depending on the contract in which the story actions are exercised. In addition, it is worth noting the possibility of not invoking the liability action of the GDPR, but rather claiming to the insurance company for a breach of contract in the case of having contractually committed to protect the data in accordance with current legislation.

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos.
AN	Audiencia Nacional.
APD	Autoridad de Protección de Datos.
BI	Busisness Intelligence.
BOE	Boletín Oficial del Estado.
CE	Comisión Europea.
CEPD	Comité Europeo de Protección de Datos.
DOUE	Diario Oficial de la Unión Europea.
GB	Gigabyte.
IP	Internet Protocol.
LOPD	Ley Orgánica de Protección de Datos.
LOPJ	Ley Orgánica del Poder Judicial.
MAC	Media Access Control.
Mbps	Megabit por segundo.
NCV	Normas Corporativas Vinculantes.
PLOPD	Proyecto de Ley Orgánica de Protección de Datos.
RAL	Resolución Alternativa de Litigios.
RGPD	Reglamento General de Protección de Datos de la Unión Europea.
RLOPD	Reglamento de la Ley Orgánica de Protección de Datos.
SAN/SSAN	Sentencia/s de la Audiencia Nacional.
STC/SSTC	Sentencia/s del Tribunal Constitucional.
STJUE/SSTJUE	Sentencia/s del Tribunal de Justicia de la Unión Europea.
STS/SSTS	Sentencia/s del Tribunal Supremo.
TC	Tribunal Constitucional.
TID	Transferencia Internacional de Datos.
TJUE	Tribunal de Justicia de la Unión Europea.
TS	Tribunal Supremo.
UE	Unión Europea.

I. PLANTEAMIENTO

El *Big Data* y las nuevas tecnologías están cambiando el mundo. No estamos redescubriendo la pólvora, estamos constatando una realidad.

Numerosos son los artículos y noticias explicando las bondades de tecnologías como el *Big Data, Cloud Computing* y el *Internet of Things,* vocablos que para una persona corriente le puedan parecer extraños (al menos, los dos últimos), pero que para una empresa deben estar presente si quiere sobrevivir en este nuevo mercado, como el incremento del 60 % en el margen de beneficio en empresas que operan en *retail*[1], la mejora de su posición competitiva, la capacidad de proporcionar nuevos productos o servicios, o la posibilidad de desarrollar campañas de marketing dirigido más eficaces[2].

Pero no todas las empresas son capaces de obtener rentabilidad a sus datos. Un dato preocupante demuestra un estudio conjunto de PwC y Iron Mountain que el 43 % de las empresas no son capaces de sacar el máximo partido de su información y un 23 % no extraen ningún tipo de beneficio[3].

Son numerosos también los datos personales que se pueden recoger para la ejecución del uso del *Big Data* en el negocio asegurador como, por ejemplo, los datos biométricos que proporcionan las pulseras inteligentes destinadas al rendimiento deportivo, datos sobre la geolocalización del asegurado para observar la peligrosidad de las rutas que toma, sus hábitos en Internet a la hora de diseñar productos específicos para el cliente, o la recopilación de reclamaciones fraudulentas para establecer modelos predictivos.

---

[1] *Vid.* MCKINSEY GLOBAL INSTITUTE, «Big data: The next frontier for innovation, competition, and productivity», 2011.

[2] *Vid.* VANSON BOURNE, «The State of Big Data Infrastructure: Benchmarking global Big Data users to drive future performance», 2015.

[3] *Vid.* PWC y IRON MOUNTAIN, «Seizing the information advantage. How organisations can unlock value and insight from the information they hold», 2015.

Pero el *Big Data puede traer tantos problemas como beneficios si tales datos personales no son tratados correctamente.* El uso masivo de datos masivos implica un riesgo para los derechos fundamentales de los individuos, como el derecho a la intimidad y a la protección de datos. Muchos de esos datos tienen mucha incidencia en los derechos mencionados (p. ej. los datos biométricos o los datos relativos a la salud), y por ello el marco jurídico de la protección de datos otorga una protección especial a tales categorías con el fin de preservar la inviolabilidad de los derechos y libertades fundamentales. Tal es la preocupación e importancia del *Big Data* que el Comité Conjunto Europeo de Autoridades de Supervisión elaboró el «Joint Commitee Discusion Paper on the use of Big Data by Financial Institutions»[4], con el objetivo de recabar las opiniones de los principales proveedores de *Big Data* del mercado, que respondieron a preguntas redactadas por el Comité relacionadas con el fenómeno del *Big Data,* los sectores más afectados, el marco regulatorio, y aplicaciones, y que obtuvo una gran respuesta por parte de diversos actores.

Otro dato relevante aportado por las empresas PwC y Iron Mountain, el 41 % de empresas de tamaño medio en Europa no cumplirían con la normativa europea debido a que guardan datos «por si acaso», creando así un riesgo latente con graves consecuencias[5].

Por ello, la rápida evolución tecnológica y la globalización *han planteado nuevos retos para la protección de los datos personales.* La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, y garantizar al mismo tiempo un elevado nivel de protección de los datos personales[6].

---

[4] JC/2016/86.

[5] *Vid*. PWC y IRON MOUNTAIN, «Beyond good intentions. The need to move from intention to action to manage information risk in the mid-market», 2016.

[6] *Vid*. Considerando 6 RGPD.

Una vez planteado el objeto de estudio, el objetivo general que se busca lograr con el presente trabajo es observar las aplicaciones legales derivadas del tratamiento de datos en el ámbito asegurador a la luz del uso del *Big Data*. Además, como otros objetivos específicos, se pretende:

a) Explicar la tecnología conocida como *Big Data* desde su concepto y características definitorias hasta su aplicación en el ámbito asegurador.

b) Elucidar el nuevo régimen sobre protección de datos que otorga el nuevo Reglamento (UE) 679/2016 General de Protección de Datos (en adelante, RGPD)[7], y destacar algunas menciones al futuro reglamento sobre privacidad pendiente de aprobación; sin olvidar el actual régimen jurídico dado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[8], y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD)[9], además de hacer mención al nuevo Proyecto de LOPD de 2017, comparándolo con la actual LOPD.

c) Dar a conocer el catálogo de datos objeto de recolección por la industria aseguradora, con especial hincapié en aquellos considerados «sensibles». Para ello, se partirá de la concreción del concepto «dato personal», hasta la explicación de las técnicas de anonimización, que tienen el objetivo de convertir los datos en «anónimos» para evitar la aplicación de la normativa europea.

d) Delimitar la aplicación de la legislación europea de protección de datos personales del artículo 3 del RGPD a las operaciones de tratamiento llevadas a cabo por las aseguradoras sitas tanto en la Unión Europea mediante sus filiales o por un tratamiento de datos realizado fuera del territorio comunitario.

---

[7] DOUE L 119/1, 4 de mayo de 2016.

[8] DOCE L 281, 23 de noviembre de 1995.

[9] BOE, n.º 298, 14 de diciembre de 1999.

e) Estudiar el nuevo régimen jurídico de las transferencias internacionales de datos en relación no solo al nuevo reglamento, sino también a la luz de las sentencias del Tribunal de Justicia de la Unión Europea y del nuevo contexto internacional.

f) Observar las cuestiones legales derivadas de una responsabilidad civil tanto contractual como extracontractual por el uso ilícito de los datos personales tratados desde la perspectiva del derecho internacional privado.

El *Big Data* ha demostrado producir graves riesgos en la privacidad y en la protección de datos generados en parte por la innovación tecnológica que ello supone y su desconocimiento por parte de las personas que son objeto de tal tecnología. Por eso se ha abordado la explicación del *Big Data* desde una perspectiva práctica, sin llegar a inspeccionar sus elementos técnicos y matemáticos en profundidad, ya que inmiscuirnos en tales elementos diferiría demasiado en el objeto de estudio.

La explicación de las implicaciones legales del *Big Data* se ha llevado a cabo desde el estudio, basándose en fuentes legales de ámbito institucional, como son los reglamentos, directivas, decisiones y sentencias europeas; en particular, del nuevo RGPD, y en textos de un contenido más técnico como los dictámenes emitidos por el Comité Europeo de Protección de Datos, que contienen una enriquecedora combinación de consideraciones científico-jurídicas. Todo ello con el fin de constatar su incidencia en la protección de datos.

Se han estudiado las implicaciones derivadas del uso ilícito de los datos personales desde una perspectiva eminentemente jurídica, y desde el punto de vista del derecho internacional privado, ya que la situación geográfica de las partes y la pluralidad de lugares en los que se puede cometer el hecho dañoso que derive una responsabilidad civil extracontractual han demostrado que esta rama del Derecho es la más adecuada para dar respuesta a los diversos problemas que suscita la reclamación económica de los afectados.

En primer lugar, se partirá del estudio del *Big Data* a partir de su concreción conceptual. Se analizarán las características propias del *Big Data,* conocidas como «V's», y se clasificarán los tipos de datos que son objeto del *Big Data* desde un punto de vista técnico, para estudiar así las aplicaciones tanto económicas como legales.

En segundo lugar, se estudiarán las variedades de datos recolectados por las aseguradoras desde el punto de vista jurídico, mediante la concreción del concepto de dato personal y las técnicas de anonimización que son utilizadas para eliminar el sometimiento a la legislación sobre protección de datos.

En tercer lugar, nos referiremos al tratamiento legal de los datos personales en apartados concretos como los supuestos de aplicación del reglamento, las condiciones en las que debe prestarse el consentimiento del afectado y las medidas de seguridad que ofrece el RGPD.

En cuarto lugar, fijado el marco conceptual, nos referiremos al régimen de las transferencias internacionales de datos, concretando el concepto objeto de estudio, el procedimiento de transferencia y los medios que otorga el nuevo reglamento. También se hará alusión al nuevo marco de transferencia de datos entre la UE y EE. UU. conocido como *Privacy Shield,* debido a las diferencias que presenta respecto a marcos regulatorios de otros Estados, y por la gran importancia que presentan las filiales de aseguradoras estadounidenses en la Unión Europea.

Por último, se tratará la reclamación de los afectados debido al uso ilícito de los datos personales tratados desde la perspectiva del derecho internacional privado tanto desde el ámbito de la responsabilidad contractual como desde la responsabilidad contractual, abordando las cuestiones sobre la determinación de la competencia judicial internacional y de la ley aplicable en cada supuesto.

II. LAS APLICACIONES DEL *BIG DATA* EN EL NEGOCIO ASEGURADOR

II.1. CONCEPTO Y CARACTERÍSTICAS DEL *BIG DATA*: DESDE EL 3V's HASTA EL *3²V*

II.1.1. Concepto

La sociedad está inmersa en una constante digitalización, no solo social, sino también económica e industrial[10]. El ascenso de nuevas tecnologías tales como las redes sociales, el *Cloud Computing* o el *Internet of Things*, además de la aparición de los dispositivos inteligentes, lleva consigo un aumento exponencial del volumen de datos generados que, a su vez, otorgan una valiosa información a quien los trata. Esta nueva «sociedad del dato» es el resultado del ascenso del *Big Data.*

Este nuevo concepto *(Big Data) constituye un término básico y fundamental en la tecnología de la información debido al uso que empresas,* ya sean tecnológicas o no, dan para potenciar o reestructurar su modelo económico sobre la base de los datos.

Pero es imposible concebir el *Big Data* como una figura autónoma respecto a otros conceptos tecnológicos, como es el caso del *Internet of Things,* que consiste en una combinación de sensores métricos que permiten captar un gran volumen de datos. De ahí tal concepción intrínseca entre ambos conceptos.

La relación del *Big Data* con otras tecnologías no acaba ahí, pues toma un significado adicional con el auge de las redes sociales, puesto que cualquier comentario, *like* o valoración hecha en Twitter, Facebook, YouTube, o en cualquier red social, constituye una información, un dato al fin y al cabo.

---

[10] *Vid.* HUA TAN, Kim, JI, Guojun, PENG LIM, Chee y TSENG, Ming-Lang, «Using big data to make better decisions in thedigital economy», en *International Journal of Production Research*, vol. 55, n.º 17, Taylor & Francis, 2017, p. 4999.

También tiene una gran interrelación con el *Cloud Computing,* puesto que esos datos, una vez recabados, son almacenados en servidores con unas capacidades de almacenamiento sobredimensionadas, diseñadas específicamente para este cometido.

Big Data, en español, puede ser traducido de varias maneras, por ejemplo, y de forma literal, como «grandes datos», o de una forma más correcta a nuestro entender y en el entorno de las tecnologías de la información, como «macrodatos»[11]. Este nuevo término ha sido adoptado para hacer referencia a la manipulación de un gran volumen de datos.

Y aunque demos especial importancia a una de las características principales del *Big Data,* como es el volumen, no debemos olvidar que esa ingente cantidad de datos generada proviene de diversas fuentes, que otorgan una gran diversidad cualitativa de datos. Por eso otra de las características principales del *Big Data* es la variedad.

Por último, esa cantidad inmensa de datos de diversa calidad suelen fluir en tiempo real. El *Big Data* analiza los datos en tiempo real, por lo que el análisis de datos de hace unas horas o, incluso, minutos puede arrojar resultados no apropiados al fin que buscamos con el *Big Data.* Tan fundamental es la velocidad, que este término es el último de los tres conceptos principales que conforma el *Big Data,* los cuales se les han añadido nuevas características complementarias debido a la rápida evolución de su práctica, y que posteriormente analizaremos pormenorizado.

Consecuencia del gran número de elementos que conforman el *Big Data, encontrar una definición que explique de forma rigurosa qué es el* Big Data *es complicada*[12]. Aunque podemos encontrar autores que se han atrevido a aportar alguna definición relativamente formal, como la que muestra STARMANS, que lo define como «muchos o demasiados datos de lo que solemos usar, o los cuales no pueden ser manejados, accedidos, analizados, interpretados y validados por medios convencionales, como base para obtener información útil y conocimiento confiable»[13].

---

[11] *Vid*. TASCÓN, Mario y COULLAUT, Arantza, *Big Data y el Internet de las Cosas*. Qué hay detrás y cómo nos va a cambiar, Catarata, Madrid, 2016, p. 12.

[12] *Vid*. MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth, *Big Data. A Revolution That Will Transform How We Live*, Houghton Mifflin Harcourt, Nueva York, 2013, p. 6.

[13] *Vid.* STARMANS. J. C. M, Richard, «The Advent of Data Science: Some Considerations on the Unreasonable Effectiveness of Data», en BÜHLMANN, Peter, DRINEAS, Petros, KANE, Michael y VAN DER LAAN, Mark, *Handbook of Big Data*, CRC Press, 2016, p. 6.

JOYANES AGUILAR comparte la misma opinión en cuanto a la gran complejidad para encontrar una definición que explique a la perfección qué es el *Big Data*. El mismo autor, habida cuenta de ello, destaca que la concepción del *Big Data* varía según la importancia que el autor dé sobre una característica concreta. Podemos ver así que algunas de las empresas pioneras y punteras a nivel mundial sobre el *Big Data* destaquen el volumen generado de los datos (la cantidad de datos obtenidos), como McKinsey Global Institute[14], o Deloitte[15]; otras, la variedad (tipos de fuentes de datos no estructurados, como la interacción social, video, audio, o cualquier cosa catalogable en una base de datos)[16], como Gartner[17], o la velocidad (de creación y utilización), como IDC[18].

Pero no todos los autores otorgan definiciones centradas en sus características. El *Big Data* es visto también desde perspectivas que llegan a trascender los datos y buscan destacar elementos más pragmáticos que las propias características (o uves) por las que fundamentar el *Big Data*[19]:

1. *El* Big Data *como tecnología.* Orientada fundamentalmente al desarrollo tecnológico, los usuarios de estas tecnologías vieron la necesidad de diferenciarse de las demás tecnologías existentes hasta la fecha, por lo que crearon este concepto como una «nueva tecnología».

2. *El* Big Data *como aplicación.* Esta definición enfatiza en las diferentes aplicaciones basadas en los diversos tipos de *Big Data*. Puede ser definida como una aplicación de procesamiento mediato de datos de la información generada por personas y por máquinas.

---

[14] *Vid.* MCKINSEY GLOBAL INSTITUTE, *op. cit.,* p. 6.

[15] *Vid.* DELOITTE, «Big Data, Big Brother? Striking the right balance with privacy», 2015, p. 4.

[16] *Vid*. JOYANES AGUILAR, Luis, *op. cit.,* p. 19.

[17] *Vid*. ELIAS, Howard, «El desafío de *Big Data:* Cómo desarrollar una estrategia ganadora», CIO, julio, 2012. Disponible en: http://cioperu.pe/articulo/10442/el-desafio-de-big-data-como-desarrollar-una-estrategia-ganadora/

[18] *Vid*. IDC, Worldwide Big Data Technology and Services 2012-2015 Forecast, marzo, 2012, p. 1.

[19] *Vid*. BUYYA, Rajkumar, CALHEIROS, Rodrigo y VAHID DASTJERDI, *Big Data: Principles and Paradigms*, Elsevier, Ámsterdam, 2016, p. 10.

3. *El* Big Data *como fuente de señales.* Es una concepción orientada al *Big Data* como aplicación, pero se centra en el *timing* más que en la variedad de los datos. Se busca que los datos creen una previsión respecto a una situación, o un nuevo patrón respecto del conjunto de datos.

4. *El* Big Data *como oportunidad. El Big Data* surge por los avances tecnológicos, cuando años atrás no se podía acceder a ello por la tecnología existente en ese momento; por lo que las bases de datos de las empresas cobraron un sentido tras la llegada del *Big Data*.

5. *El* Big Data *como metáfora.* Es definido como un proceso de pensamiento humano, una extensión del cerebro humano, al tener como objetivo crear un sistema nervioso propio para el planeta.

6. *El* Big Data *como nuevo término para las viejas cosas.* En contraposición a la segunda definición, se considera que los proyectos actuales podían hacerse con la tecnología anterior, sin tener que acudir al renombramiento de aquellas con *Business Intellingence* o *Big Data Analytics.*

Tampoco debemos olvidarnos de que el *Big Data* requiere de *los elementos materiales necesarios para llevar a cabo su aplicación.* Estos son los sistemas informáticos, y no cualesquiera. PUYOL MONTERO incluye tales medios en la concepción del *Big Data*[20].

Una vez analizados los elementos que, unidos todos ellos, conforman el *Big Data,* podemos definirlo como «el análisis de macrodatos de calidades variadas derivados de diversas fuentes que fluctúan a gran velocidad mediante los sistemas informáticos adecuados, con el objetivo de obtener un valor añadido en los productos ofrecidos».

II.1.2. Características: las *V's*

Como hemos adelantado, *las características del Big Data est*án conformadas por *las «uves»,* que vienen a ser uno de sus rasgos más representativos. Hemos observado

[20] *Vid*. PUYOL MONTERO, Javier, *Aproximación jurídica y económica al Big Data,* Tirant lo Blanch, Valencia, 2016, p. 286.

que inicialmente se basaban en tres características o «uves», pero con la evolución del *Big Data,* dichas características se han quedado cortas a la hora de afianzar lo que es este concepto. Debido a su expansión, las características se han ido agrupando en *domains* o dominios, que podemos definirlos como sectores especializados de un determinado campo.

El primer conjunto de características clásicas está agrupado en el llamado *Data domain*[21]*.* En los albores de su entendimiento, se consideraba que las características del *Big Data* eran:

- *Velocidad:* se refiere a la velocidad de adquisición de datos y su procesamiento, la velocidad a la que fluyen los datos. El *Big Data* añade un plus de velocidad que permite acelerar el proceso. El ritmo de los datos usados para apoyar interacciones y los generados por las interacciones.

- *Volumen:* la cantidad masiva de datos generados y guardados por las empresas. Tal es la información, que tiene que ser medida en petabytes o, incluso, exabytes.

- *Variedad:* consiste en las dinámicas y crecientes fuentes de obtención de datos. Las fuentes pueden ser datos de sensores, audio, videos, tráfico *online* y muchos más tipos. Los datos pueden venir de forma estructurada, semiestructurada o no estructurada[22]. Como ejemplos, un dato semiestructurado puede consistir en el texto de un correo electrónico, y uno no estructurado sería los apuntes que realiza el servicio de atención al cliente, escritos en un formato libre sobre el problema de un cliente.

Estas tres características se interrelacionan. Así, el volumen de datos se relaciona directamente con la variedad de las diferentes fuentes; y la velocidad del flujo de datos se

---

[21] El *Data domain* está basado en la categoría del dato, consistente tanto en una lista enumerada de valores determinados, como en un conjunto de normas con restricciones específicas en los valores dentro de esa categoría de datos. Un ejemplo sería atribuir en una tabla de una base de datos una columna destinada al «género». A esta columna se le atribuye uno o dos «códigos valores»; en este caso, «M» para masculino y «F» para femenino. Por lo tanto, el *Data domain* para la columna de género será «M», «F». *Vid*. LOSHIN, David, *Enterprise Knowledge Management: The Data Quality Approach,* Morgan Kaufmann, San Diego (CA), 2003, p. 302.

[22] *Vid*. JAIN, Vijay Kumar, *Big data and Hadoop,* Khanna Publishing, Nueva Delhi, 2017, p. 4.

relaciona con el volumen de datos y la variedad de sus fuentes. En el *Data domain,* la característica determinante es el «volumen». La cantidad de datos siempre es mayor que su variedad o su velocidad.

Posteriormente, el modelo primitivo fue ampliado sucesivamente con nuevas «uves», añadiéndose como características el valor, la visibilidad, el veredicto, la veracidad, la validez y la variabilidad[23]; derivadas todas ellas de las nuevas perspectivas que otorga el *Business Intelligence domain* y el *statistic domain*.

Las características aportadas por el *Business Intelligence domain*[24] son:

- *Valor:* ¿los datos recogidos tienen información valiosa para mis necesidades empresariales? Es la pregunta que se busca responder. Es uno de los aspectos críticos en el caso del *Big Data*. No tiene sentido la recolección de todos los datos a menos que seamos capaces de generar algún valor fuera de ella. Recomendaciones dadas por varios sitios basados en las preferencias del usuario y los datos de flujo de clics son uno de los mejores ejemplos para delinear esta característica del *Big Data*[25].

- *Visibilidad:* los datos pueden ser recogidos, seleccionados y procesados, pero para llevar a la práctica un efectivo uso del *Big Data,* los datos deben ser presentados de una manera accesible y entendible para encontrar patrones de datos con el objetivo de crear una línea de trabajo sobre ellos. Una manera muy útil para representar esos datos es el uso de una infografía. Una representación gráfica de información de una manera directa y visual (ver figura 1).

- *Veredicto:* es la potencial elección o decisión que debe ser realizada por el tomador de decisiones basado en la amplitud del problema, la disponibilidad de los recursos y su capacidad computacional. Este último valor es el más difícil de cuantificar.

---

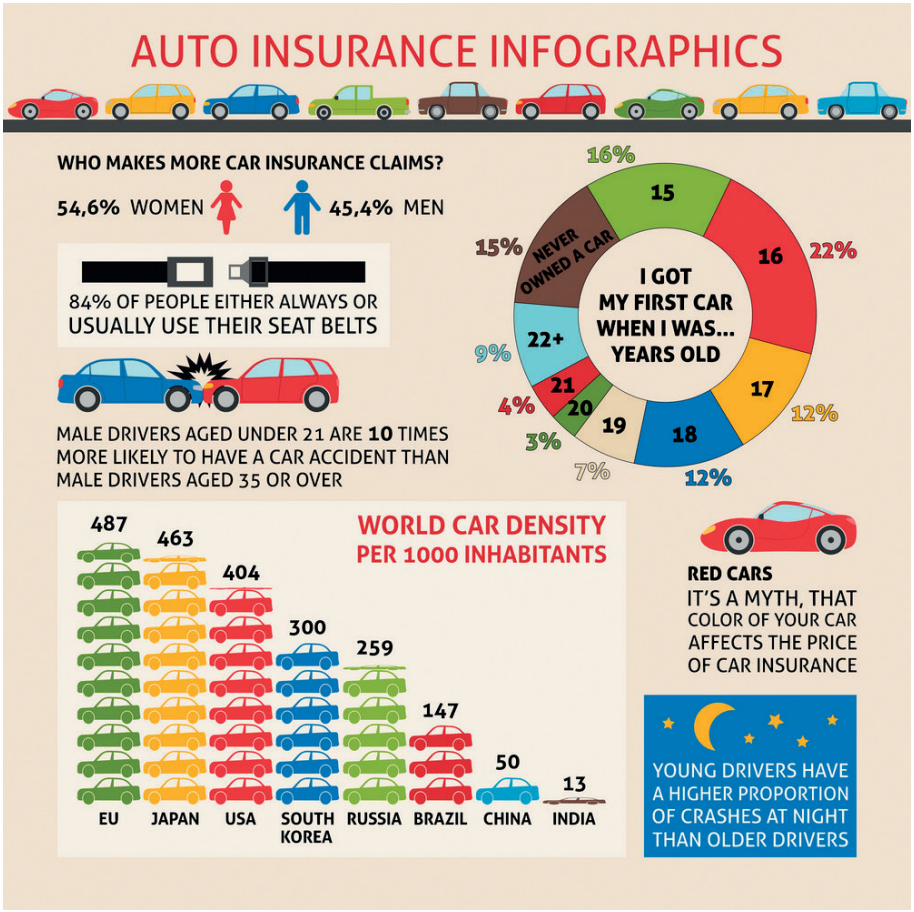
[23] *Vid*. BUYYA, Rajkumar, CALHEIROS, Rodrigo y VAHID DASTJERDI, *op. cit.,* pp. 10-14.

[24] Es el conjunto de metodologías, aplicaciones, prácticas y capacidades enfocadas a la creación y administración de información que permite tomar mejores decisiones mediante la creación de modelos predictivos a los usuarios de una organización. En este sentido, *Vid*. CONESA CARALT, Jordi (coord.) y CURTO DÍAZ, Josep, *Introducción al Business Intelligence,* Editorial UOC, Barcelona, 2012, p. 18.

[25] *Vid.* VICTOR, Nancy y LÓPEZ, Daphne, «Privacy models for big data: a survey», en *International Journal of Big Data Intelligence,* vol. 3, n.º 1, 2016, p. 62.

Si desde el inicio contamos con demasiadas hipótesis, los costes derivados de las ejecuciones de proyectos de *Big Data* aumentarán, ya que se amplía el campo de actuación para buscar los datos que puedan solucionar los nuevos problemas surgidos.

Figura 1. Ejemplo de una infografía sobre los seguros de vehículos



Fuente: Dreamstime.

En este *domain,* la característica clave es la visibilidad. Si los datos no son lo suficientemente visibles, no podemos darles valor; en consecuencia, tampoco seremos capaces de tomar una decisión meridianamente segura.

El último sector lo conforma el *statistic domain*. Las siguientes características deben establecer los modelos estadísticos basados en la hipótesis correcta (¿qué pasaría si...?), que es la fiabilidad de los conjuntos de datos y la fiabilidad de las fuentes de datos. Si la hipótesis es inadecuada, la fuente de datos está contaminada o el modelo estadístico es incorrecto, el análisis llegará a una conclusión incorrecta.

- *Veracidad:* la veracidad deriva en respuesta a los problemas de la calidad y de fuentes de datos que las empresas empezaban a encontrarse al crear iniciativas con *Big Data*[26]. Algunos de los elementos que afectan a la veracidad de los datos son la integridad, autenticidad, origen, reputación, disponibilidad y responsabilidad.

- *Validez:* se trata de verificar la calidad de los datos siendo lógicamente sólidos. Enfatiza la precisión de los datos y la evasión de prejuicios.

- *Variabilidad:* trata con la inconsistencia en la velocidad de la carga de datos en las bases de datos; dicho de un modo más sencillo, la variabilidad se refiere a la variación en las tasas de flujo de datos. A menudo, la gran velocidad de datos no es consistente y tiene picos y valles periódicos[27].

La característica clave de este aspecto es la veracidad, que enfatiza en cómo construir un modelo estadístico cercano a la realidad.

Una vez atribuidas y separadas las características que forman el *Big Data,* es conveniente, para una mejor explicación gráfica, la agrupación de estas mediante un Diagrama de Venn que agrupe todas las características y *domains* que conforman el *Big Data* en la teoría de las *V* (ver figura 2). Si los atributos de datos originales de 3Vs representaban un significado sintáctico de *Big Data,* entonces *V* (o 9Vs) representan el

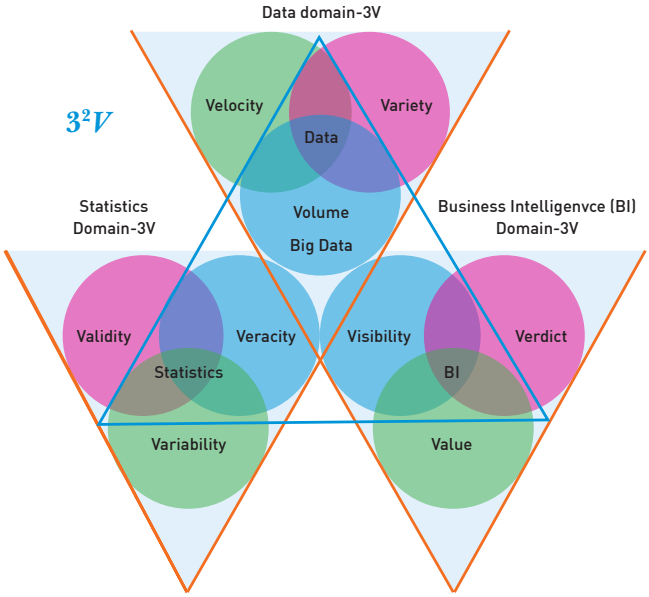
---

[26] *Vid*. ZIKOPOULOS, Paul, *Harness the power of big data, the IBM Big data platform,* McGraw-Hill, 2013, p. 9.

[27] *Vid*. GANDOMI, Amir y HAIDER, Murtaza, «Beyond the hype: Big data concepts, methods, and analytics», en *International Journal of Information Management*, n.º 35, Elsevier, Amsterdam, 2015, p. 139.

significado semántico (relación de datos, BI y estadísticas). Para muchos problemas o aplicaciones complejas, las *V* podrían ser interpretados como un modelo jerárquico, para el cual tres atributos claves forman un nivel superior de 3Vs.

Figura 2. Diagrama de Venn creado sobre una estructura jerárquica



Fuente: *Big Data: Principles and Paradigms*, p. 14.

Por otra parte, desde un punto de vista de arquitectura y tecnología, se puede estructurar un sistema *Big Data* en cinco capas principales[28]:

- *Capa de fuentes de datos:* en esta capa estarían todos los orígenes de la información, desde bases de datos relacionales hasta cualquier tipo de datos, estructurados o no.

- *Capa de integración:* aquí se adquieren los datos y se integran en conjuntos con el formato adecuado.

---

[28] *Vid*. ISMS FORUM-AEPD, *Código de buenas prácticas para proyectos de Big Data*, Madrid, 2017, p. 4.

- *Capa de almacenamiento de datos:* se trata del conjunto de recursos adecuados para el almacenamiento de grandes volúmenes de datos.

- *Capa de análisis y modelos de computación:* contiene diversas herramientas de manejo de datos que operan sobre los recursos de almacenamiento e incluyen la gestión de los datos y los modelos de programación.

- *Capa de presentación y aplicación:* engloba las tecnologías de visualización tales como dispositivos móviles, navegadores, etc. Una vez obtenido el conocimiento, este se puede aplicar en distintos procesos.

II.2. TIPOS DE *BIG DATA*

Los datos se clasifican en tres tipos[29]:

1. *Datos estructurados:* hace referencia a todo dato que puede ser recabado mediante una base de datos SQL[30] con filas y columnas. Tienen clave relacional y pueden ser asignados fácilmente en los campos prediseñados. Estos datos son los más procesados y la forma más simple de manejar la información.

   Los datos estructurados dependen de crear un *dato modelo.* Un modelo de los diferentes datos que necesita una empresa que serán recolectados, y cómo serán almacenados, procesados y accedidos a ellos. Esto implica también definir qué campos de datos serán almacenados y cómo ese dato será almacenado: tipo de dato (numérico, divisa, alfabético, nombre, fecha, dirección) y cualquier restricción en la entrada de datos (número de caracteres; restricción a ciertos términos –valores– como «M», «F»; o «D», «Dña.»)[31].

---

[29] *Vid*. JAIN, Vijay Kumar, *Big data and Hadoop*, *op. cit.,* p. 12.

[30] SQL (Structure Query Language) es un lenguaje de programación creado para manejar y ordenar datos en sistemas de bases de datos relacionales.

[31] Los datos que concurren al rellenar un formulario de google son datos estructurados, puesto que son ordenados en un soporte que facilita la creación de una base de datos relacional, cuando ligamos la pregunta a la respuesta que damos.

2. *Datos semiestructurados:* es información que no reside en una base de datos relacional, pero que tiene determinadas propiedades organizativas que lo hacen fácil de analizar. Con determinados procesos, pueden llegar a incluirse en una base de datos relacional. Los documentos CSV, XML y JSON son documentos semiestructurados.

3. *Datos no estructurados:* se refiere a la información que no tiene predefinido un *dato modelo,* o no está organizado de una manera predefinida. La información no estructurada suele ser textos con una alta densidad de contenido, pero puede contener datos tales como fechas, números y también hechos. Esto deriva en irregularidades y ambigüedades que lo hacen difícil para comprender el uso de programas tradicionales en comparación con datos almacenados en forma de ficheros en bases de datos, o anotados en documentos.

   Técnicas como la minería de datos, el procesamiento de lenguajes naturales y la analítica de texto proporcionan diferentes métodos para encontrar patrones en esa información o, de otra forma, interpretarla.

   Ejemplos de datos no estructurados son los libros, periódicos, documentos, metadatos, audio, video, dato analógico, imágenes, ficheros y texto desestructurado como el cuerpo de un mensaje de correo electrónico, una página web o un procesador de texto. Los datos no estructurados son los más numerosos. Se estima que el 80 % de los datos que posee una empresa no están estructurados. Los datos no estructurados están por todas partes. Estos pueden ser generados tanto por una máquina como por una persona.

   1) *Como ejemplos de datos no estructurados generados por una máquina:*

      a) Imágenes por satélite, que incluyen los datos meteorológicos, o los datos generados por los satélites de vigilancia.

      b) Datos científicos: imágenes sísmicas o datos atmosféricos.

      c) Fotografías y videos: respecto a seguridad, vigilancia y tráfico.

      d) Datos de radares o sonares: datos de vehículos, meteorológicos y perfiles sísmicos-oceanográficos.

2) *Como ejemplos de datos generados por humanos:*

   a) Textos internos de una empresa: logo, e-mails, encuestas, resultados, etc.

   b) Datos de los *social media:* datos generados de webs con fuerte contenido social como YouTube, Facebook, Twitter, LinkedIn y Flickr.

   c) Datos móviles: mensajes de texto, localización, tráfico *online,* etc.

   d) Contenido web: proviene de cualquier sitio con un contenido deliberadamente no estructurado, como YouTube, Flickr o Instagram.

II.3. FUENTES DE DATOS

El origen de los datos es el primer aspecto que debe tenerse en cuenta en la cadena de tratamientos contemplados en un sistema de *Big Data*. Una parte importante de la complejidad del análisis de estos tratamientos ocurrirá en aquellos casos en que el sistema se nutra de información proveniente de múltiples orígenes.

Según el nivel de confiabilidad que ofrezcan los diferentes orígenes de datos, la calidad de los datos primarios puede quedar comprometida de inicio y arrastrarse durante todo su ciclo de vida.

Cada día generamos una cantidad ingente de datos. Todos esos de datos son generados por tabletas, teléfonos y sistemas inteligentes, como los conocidos *smartwatch*. Como ejemplos de datos que generamos día a día[32]:

- Sensores inteligentes aplicados a diferentes verticales de la industria, que almacenan continuamente datos de las líneas de producción que son posteriormente analizados para, por ejemplo, mejorar procesos industriales.

---

[32] *Vid*. PUYOL MORENO, Javier, «Una aproximación al Big Data», en *Revista de Derecho UNED,* n.º 14, Madrid, 2014, p. 474.

- Horas de video grabadas para vigilancia u otros fines.
- Miles de pagos con tarjeta de crédito cada segundo alrededor del mundo.
- Flujo de datos en tiempo real generados por aplicaciones deportivas.
- Millones de *tweets* por día. Miles de *tweets* por segundo.
- Numerosos comentarios en las páginas corporativas de las redes sociales.
- Gigas de archivos de documentos, planos, formularios y muchos otros tipos de datos desestructurados que son digitalizados para hacer más eficiente su almacenamiento.
- Información de transacciones en la bolsa, cotizaciones de *commodities*.
- Movimiento de vehículos, carga, seguimiento por GPS.
- Información del clima: temperatura, presión, humedad, vientos, precipitaciones.

Para hacernos una idea de la cantidad de datos generados[33]:

- El tráfico global de IP superó el umbral del *zettabyte* (ZB, 1.000 exabytes [EB]) en 2016 y alcanzará 2,3 ZB en 2020. El tráfico IP global alcanzará 1,1 ZB por año o 88,7 EB (un billón de gigabytes [GB]) por mes en 2016. Para 2020, el tráfico mundial de IP alcanzará 2,3 ZB por año, o 194 EB al mes.
- El tráfico de Internet de hora en hora está creciendo más rápidamente que el tráfico promedio de Internet. El tráfico de Internet aumentó 51 % en 2015, en comparación con un crecimiento del 29 % en el tráfico promedio. El tráfico de Internet de hora en hora aumentará por un factor de 4,6 entre 2015 y 2020, mientras que el tráfico promedio en Internet se duplicará.

---

[33] *Vid*. CISCO, «Cisco Visual Networking Index: Forecast and Methodology, 2015-2020», 2015, p. 1.

- El tráfico de teléfonos inteligentes superará el tráfico de PC en 2020. En 2015, los PC representaron el 53 % del tráfico total de IP, pero para 2020 los PC representarán solo el 29 % del tráfico. Los teléfonos inteligentes representarán el 30 % del tráfico IP total en 2020, frente al 8 % en 2015.

- El tráfico de dispositivos inalámbricos y móviles representará dos tercios del tráfico IP total en 2020. Ese año, los dispositivos con cable representarán el 34 % del tráfico IP, frente al 66% del uso del wifi y los dispositivos móviles que representarán el 66% del tráfico IP. En 2015, los dispositivos cableados representaron la mayoría del tráfico IP en 52 %.

- El tráfico global de Internet en 2020 equivaldrá a 95 veces el volumen de toda la Internet mundial en 2005. Globalmente, el tráfico de Internet alcanzará los 21 GB per cápita en 2020, frente a los 7 GB per cápita en 2015.

- El número de dispositivos conectados a redes IP será tres veces mayor que la población mundial en 2020. Habrá 3,4 dispositivos en red per cápita en 2020, frente a 2,2 dispositivos en red per cápita en 2015. Acelerado en parte por el aumento de dispositivos y las capacidades de estos, el tráfico IP per cápita alcanzará los 25 GB per cápita en 2020, frente a los 10 GB per cápita en 2015.

- Las velocidades de banda ancha casi se duplicarán para 2020. Para esa fecha, las velocidades globales de banda ancha fija alcanzarán los 47,7 Mbps, frente a los 24,7 Mbps en 2015.

Como vimos anteriormente, los datos pueden ser estructurados, semiestructurados y no estructurados; ahora bien, esos datos se pueden clasificar también según la fuente de la que procedan. SOARES realiza una clasificación de estas fuentes[34]:

1. *Web y social media.* Consiste en contenido web, y en la información obtenida por las redes sociales como Facebook, Twitter, LinkedIn y demás redes. Estos datos se

[34] SOARES, Sunil, «Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today», disponible en: http://www.dataversity.net/not-your-type-big-data-matchmaker-on-five-data-types-you-need-to-explore-today/; y *Big Data Governance. An Emerging Imperative*, MC Press, Boise (ID), 2012, pp. 7-8.

capturan, almacenan y distribuyen dependiendo de su suborigen: los datos generados en las redes sociales como consecuencia de determinadas acciones realizadas en estas (*clicks*, *tweets*, *retweets*, y demás entradas en Twitter, entradas en Tumblr, *posts* de Facebook), sistemas de contenidos web como YouTube o Flickr, y sitios de almacenamiento de información (Cloud) como Dropbox, Box.com, SugarSync o OneDrive.

2. *Machine-to-machine data.* Máquina-a-máquina (M2M) se refiere a tecnologías que permiten que tanto los sistemas inalámbricos como los cableados se comuniquen con otros dispositivos. M2M utiliza un dispositivo como un sensor o un medidor para capturar un evento (como velocidad, temperatura, presión, flujo o salinidad) que se transmite a través de una red inalámbrica, cableada o híbrida a una aplicación que traduce el evento capturado en información relevante. Las comunicaciones M2M crean el llamado «Internet de las cosas».

3. *Grandes transacciones de datos.* Esto incluye las demandas de atención médica, registros de detalle de llamadas de telecomunicaciones, registros de facturación y reclamaciones de consumidores. Los grandes datos de transacciones están cada vez más disponibles en formatos semiestructurados y no estructurados.

4. *Biometría.* La información biométrica incluye huellas dactilares, reconocimiento de voz, escáneres de retina e iris, reconocimiento facial y genético. Los avances tecnológicos han aumentado enormemente los datos biométricos disponibles. La aplicación de la ley, el sistema legal y las agencias de inteligencia han estado usando esta información por mucho tiempo. Sin embargo, los datos biométricos están cada vez más disponibles en el ámbito comercial donde se puede mezclar con otros tipos de datos como los medios de comunicación social, lo que hace aumentar el volumen de datos generados por los biométricos.

5. *Datos generados por humanos.* Los seres humanos generan grandes cantidades de datos tales como notas de los agentes del centro de llamadas, grabaciones de voz, correo electrónico, documentos en papel, encuestas y registros médicos electrónicos. Estos datos pueden contener información sensible que debe ser enmascarada. Puede contener ideas que pueden mejorar la calidad de los conjuntos de datos estructurados y deben integrarse con MDM *(Mobile Device Managment).* Finalmente,

las organizaciones deben establecer políticas sobre el periodo de retención para que estos datos se adhieran a las regulaciones y para administrar los costos de almacenamiento.

II.4. CÓMO AFECTA EL *BIG DATA* AL ÁMBITO ASEGURADOR

La entrada del *Big Data* en el negocio asegurador ha conllevado una serie de cambios a la hora de la toma de decisiones. Los datos de reclamaciones de seguros pueden prepararse para el análisis de datos en un periodo de unos pocos meses, si no semanas, después de la adjudicación de la exactitud[35]. Como beneficios que aporta esta tecnología encontramos principalmente dos[36]: por un lado, la detección del fraude, y, por otro lado, el análisis y la tarificación de los riesgos, a lo que hay que añadirle la fidelización del cliente.

1. *Detección del fraude.* Es el objetivo principal que se busca con el *Big Data*. Se puede definir el fraude asegurador como el *uso doloso del engaño con el objetivo de obtener una póliza de seguros que de otra manera no sería expedida, o el pago de una reclamación bajo una póliza de seguros que de otra forma no sería pagada.* Ese engaño puede recaer sobre la cantidad reclamada, la cantidad de objetos siniestrados o sobre cualquier conducta dirigida a obtener una mayor indemnización que la debida legalmente. Podemos encontrar dos variedades principales de fraude[37]:

   a) *Fraude oportunista.* Cuando una persona se aprovecha del relleno deliberado o inflado de un reclamo de seguro legítimo. Este tipo de fraude es muy común, pero el incidente está relacionado con una cantidad reducida.

   b) *Fraude profesional.* Generalmente realizado por grupos organizados de personas que pueden tener identidades múltiples y falsas. Conocen muy bien cómo organizar el

---

[35] *Vid. et al.* WASSER, Thomas, «Using 'big data' to validate claims made in the pharmaceutical approval process», en *Journal of Medical Economics*, vol. 18, n.º 12, Taylor & Francis, 2015, p. 1016.

[36] «Big Data en el sector seguros: Entrevista a José Antonio Álvarez Jareño», en *Rankia*. Disponible en: https://www.rankia.com/blog/mejores-seguros/2791779-big-data-sector-seguros-entrevista-jose-antonio-alvarez-jareno.

[37] *Vid.* BOOBIER, Tony, *Analitics for Insurance,* WILEY, Chichester (RU), 2016, pp. 63-65.

sistema y, a menudo, trabajan juntos con personas dentro del mismo. La incidencia de estos eventos es menor, pero la cantidad relacionada con un incidente es mucho mayor.

En este campo, podemos encontrar varios ejemplos sobre cómo detectar la existencia de indicios de fraudes en un supuesto estándar respecto a un siniestro (vehículo u hogar) en el que intervienen un perito, un mediador, la empresa reparadora y el cliente:

a) *Patrones.* Debemos analizar la casuística anterior y similar a la ocurrida actualmente, y observar la existencia de patrones de conducta entre los agentes intervinientes. Conductas frecuentes que nos podemos encontrar son:

   - Siniestros y argumentos similares por parte del cliente y actuando las mismas personas que en otros (tramas organizadas que cambian los roles).

   - Talleres que reportan siniestros del mismo tipo a la aseguradora con un porcentaje más alto que la media.

   - Periodicidad de repetición de esos partes.

   - Mediadores que tramitan siniestros muy parecidos a lo largo del tiempo.

b) *Anomalías.* Se busca profundizar más en la naturaleza del siniestro y de la póliza. Como ejemplos:

   - Analizar si ese siniestro relacionado con las inclemencias meteorológicas tiene un impacto en otros clientes que están en los alrededores del beneficiario.

   - Analizar si esa póliza está a punto de caducar y el cliente ha mostrado malestar con el seguro. Los modelos nos dicen que cuando alguien quiere defraudar y salir del seguro, lo hace en los últimos meses de este.

   - Conocer si ese usuario ha accedido vía web a su póliza o bien por el *contact center,* preguntando por alguna cobertura.

- Comprobar con los datos meteorológicos si realmente se ha producido ese fenómeno.

En este ámbito se debe destacar el uso de modelos predictivos supervisados, que significa crear un modelo partiendo del histórico de fraude de una aseguradora concreta, analizar los patrones y extrapolarlos a las pólizas futuras para determinar la probabilidad de que la reclamación presente sea considerada fraudulenta.

c) *Redes sociales.* Consiste en entender cómo se relacionan esas personas en las redes sociales, mails y los comentarios que generan.

d) *Documentación.* Comparar versiones de la documentación que recogemos de los diferentes actores: análisis de peritos, partes amistosos.

e) *Conversaciones en el* call center, *correos electrónicos, etc*. La experiencia demuestra que en caliente se suele informar de la realidad del daño causado, y que a medida que se enfría temporalmente el siniestro, este incrementa en daños y contenido. En un siniestro se genera mucha información y la mayor parte de ella es de carácter humano.

En definitiva, el *Big Data* ayuda a las aseguradoras a reducir las pérdidas por fraude y reducir el número de denuncias. A todo esto, debemos tener en cuenta varios factores[38]:

- Los estilos múltiples del fraude pueden suceder casi de forma simultánea. Cada estilo puede tener una característica temporal regular, ocasional, estacional o una sola vez.

- Las leyes, y por tanto las conductas asociadas a estas, cambian.

- En un futuro cercano, después de descubrir el *modus operandi* actual de los defraudadores profesionales, estos mismos estafadores suministrarán

[38] *Vid*. BOLOGA, Ana-Ramona, BOLOGA, Razvan y FLOREA, Alexandra, «Big Data and Specific Analysis Methods for Insurance Fraud Detection», *Database Systems Journal,* vol. I, n.º 1, The Bucharest University of Economic Studies, Bucarest, 2010, p. 35.

continuamente estilos nuevos o modificados de fraude hasta que los sistemas de detección vuelvan a generar falsos negativos.

2. *Análisis y tarificación de los riesgos.* Con el análisis de riesgos tratamos de describir y, en la medida de lo posible, cuantificar qué puede ir mal y qué daño puede hacer[39]. En el negocio asegurador se traduce también en crear un producto adaptado a cada cliente. Utilizar los datos para concretar el riesgo real y adaptar la póliza. La evaluación del riesgo es muy importante para las compañías de seguros. La determinación del nivel de primas basado en el riesgo evaluado (prima de riesgo neto) permite a la compañía de seguros evitar la selección negativa, es decir, perder buenos clientes debido a las altas primas[40]. Podemos encontrar varios ejemplos en los que es aplicable esta fórmula[41]:

   a) *Seguro de vehículos.* Es un sector clave entre los conductores debido a su obligatoriedad y la diversidad de pluses añadidos a la cobertura. Es destacable el aumento de precio que sufren los conductores jóvenes y noveles, ya que históricamente se ha asociado ese perfil con un aumento de riesgo. Muchas aseguradoras ofrecen ahora paquetes basados en la telemetría, donde la información real de conducción es devuelta a su sistema a un perfil personalizado y altamente preciso del comportamiento de un cliente individual. Utilizando el modelo predictivo como se mencionó anteriormente, el asegurador puede calcular una evaluación precisa de la probabilidad de que el conductor se involucre en un accidente, o que su coche sea robado, comparando sus datos de comportamiento con la de miles de otros conductores en su base de datos. Estos datos a veces se capturan y transmiten desde una caja especialmente instalada en el coche o, cada vez más, desde una aplicación en el teléfono inteligente de un conductor.

---

[39] *Vid.* ALE, Ben, «Risk analysis and big data», en *Safety and Reliability*, vol. 36, n.º 3, Taylor & Francis, 2016, p. 154.

[40] *Vid.* KAŠĆELAN, Vladimir, KAŠĆELAN, Ljiljana y NOVOVIĆ BURIĆ, Milijana, «A nonparametric data mining approach for riskprediction in car insurance: a case study from the Montenegrin market», en *Economic Research-Ekonomska Istraživanja*, vol. 29, n.º 1, 2016, Informa UK, 2016, p. 547.

[41] *Vid*. MARR, Bernard, «How Big Data Is Changing Insurance Forever», en *Forbes*, diciembre de 2015. Disponible en: https://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/#19b2facb289b.

b) *Seguros de salud y vida.* Su evolución es similar debido al aumento de los *wearables* como los *smartwatches* o las aplicaciones deportivas (Fitbit, Nike+, etc.), que puede monitorizar los hábitos de una persona y proporcionar una evaluación continua de su estilo de vida y niveles de actividad. Actualmente diversas aseguradoras ofrecen *wearables* a los beneficiarios, como pulseras, *smartwatches* o *smartphones* con tales aplicaciones para dar una cobertura adaptada al asegurado de forma gratuita, puesto que el precio que pagan los usuarios son sus datos personales[42]. Los tipos de datos que recaban pueden llegar a ser bastante sensibles, siendo la mayoría de ellos biométricos.

   Es de destacar una de las consecuencias de los anteriores casos, y es la elaboración de perfiles sobre la base del uso y comparación de clientes anteriores con similares características (datos relativos a los vehículos, conductores, zona geográfica, hábitos, etc.) que demuestren un perfil de riesgo determinado y más pormenorizado de lo habitual sobre posibles casos de fraude, precios respecto a la póliza o, incluso, denegar el servicio.

CASO PRÁCTICO 1. Cliente con problemas de salud

Se presenta un cliente de 40 años, casado y con dos hijos menores con la intención de contratar un seguro de vida a favor de sus descendientes en vista de la dependencia única y exclusiva de los ingresos que aporta este miembro. Los datos aportados por el cliente revelan problemas de salud con enfermedades tales como una fibrosis de grado 3, sumado la consideración de persona con alto sobrepeso. Se ha constatado mediante datos de otros clientes con las mismas características de nuestro cliente que la esperanza de edad media que aporta este perfil (69) es bastante reducida en comparación con asegurados sin enfermedades (87), por lo que se demuestra que si la aseguradora hace un contrato de seguro con este perfil, nunca será rentable. La aseguradora, al evaluar todos estos datos, revela que el perfil presentado encaja con los patrones antes demostrados, por lo que se decide casi de inmediato, una vez recibidos los datos, no realizar ningún contrato de seguro.

---

[42] *Vid.* SCHROEDER, Ralph, «Big data business models: Challenges and opportunities», en *Cogent Social Sciences*, vol. 2, n.º 1, Taylor & Francis, 2016, p. 9.

Por ejemplo, si realizas conductas que disminuyan el riesgo asegurado, el precio de tu póliza bajará de manera proporcional, y a la inversa si creas conductas que aumenten tal riesgo. Esto puede compararse con la gamificación, que es «el uso de las mecánicas aplicables a un juego en contextos no lúdicos»[43]; mecánicas como recompensas, logros, competiciones, sorpresas y misiones hacen que el asegurado pase de ser el sujeto pasivo del riesgo, para ser el principal mitigador y gestor de este[44].

3. *Fidelización del cliente*[45]. Con una estrategia de orientación con el *Big Data* hacia el cliente podemos fomentar:

   a) *Relación con los clientes.* El *Big Data* proporciona información sobre quiénes son sus clientes e información asociada a ellos como dónde están, qué necesitan, cómo y cuándo desean ser contactados.

   b) *Lealtad y retención.* El *Big Data* puede descubrir qué influye en la lealtad de los clientes y qué hace que acudan a su marca una y otra vez, apoyándose en la estadística.

   c) *Optimización de recursos.* Es un elemento vital en el ámbito empresarial. El *Big Data* ayuda a determinar el gasto óptimo para los diferentes canales comerciales y perfeccionar los programas de *marketing*.

---

[43] *Vid.* VV. AA., «Gamification: Toward a Definition», artículo presentado en el *Conference on Human Factors in Computing Systems*, Vancouver, 2011, p. 2.

[44] *Vid.* RODRÍGUEZ-PRADO, José Miguel, «Los seguros gamificados de vida y salud. Insurance telematics (tendencias actuales y oportunidades en seguros de personas)», en *Revista Española de Seguros: Publicación Doctrinal de Derecho y Economía de los Seguros Privados*, n.º 167, SEAIDA, Madrid, 2016, p. 467.

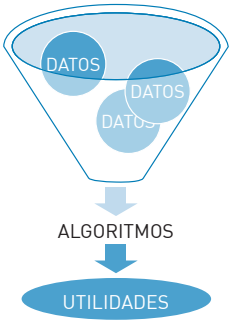
[45] *Vid.* ALCAIDE CASADO, Juan Carlos, *Fidelización de clientes,* 2.ª ed., ESIC, Madrid, 2015, p. 93.

CASO PRÁCTICO 2. Conductor asegurado con póliza a medida

Un conductor de 24 años tiene la intención de contratar un seguro de circulación. Los datos que presenta a la aseguradora son: a) vehículo de gama baja; b) baja edad; c) novel; 4) uso asiduo del vehículo, y 5) el cliente suele circular por vías en las que los accidentes son comunes. En vista de los datos presentados, la aseguradora le ofrece una alta póliza, pero le ofrece la posibilidad de rebajar la póliza si cambia sus hábitos de conducción. Para ello, instala en el vehículo un aparato geolocalizador que controlará las rutas que el usuario tome.

Los casos prácticos comentados con anterioridad son el resultado de la aplicación concreta de los datos obtenidos a modelos y patrones derivados de esos datos. Esos patrones son hallados mediante la aplicación de un algoritmo específico. Los algoritmos son «procesos lógicos formados por una serie de instrucciones o reglas que permiten resolver problemas partiendo de unos datos de entrada, mediante la obtención de unos datos de salida»[46]. Los algoritmos son codificados por un programador en un lenguaje algorítmico antes de ser traducidos a una secuencia binaria legible por máquina. El lenguaje algorítmico es un lenguaje especialmente diseñado para expresar cálculos matemáticos o simbólicos, y así expresar operaciones algebraicas en una notación, que recuerda a la lógica y está relacionada con la matemática[47]. El algoritmo es el paso intermedio entre la recolecta masiva de datos y su aplicación práctica (ver figura 3).

Figura 3.
Explicación simplificada del funcionamiento del *Big Data*



Fuente: elaboración propia.

[46] *Vid.* GONZÁLEZ ROYO y PINA, Carolina, «¿Cómo se protegen legalmente los algoritmos?», en *Diario La Ley*, n.º 8776, La Ley, Madrid, 2016, p. 1.

[47] *Vid.* VEDDER, Anton, «Accountability for the use of algorithms in a big data environment», en *International Review of Law, Computers & Technology,* vol. 31, n.º 2, Routledge, 2017, p. 210.

II.5. IMPLICACIONES LEGALES DEL *BIG DATA*

El *Big Data* puede llegar a tener implicaciones legales en tres sentidos: respecto a la normativa de protección de datos, la protección legal del algoritmo y la protección legal de las bases de datos.

II.5.1. Implicaciones en la normativa sobre protección de datos

El *Big Data* se basa no solo en la creciente capacidad de la tecnología para apoyar la recogida y el almacenamiento de grandes cantidades de datos, sino también en su poder, al utilizar algoritmos para ayudar a analizar, comprender y aprovechar el valor total de los datos para informar, permitiendo la identificación de patrones entre diferentes fuentes y conjuntos de datos[48]. Sin embargo, es el creciente uso de grandes datos para monitorizar el comportamiento humano, ya sea para fines de perfilado de los consumidores o para la vigilancia y el control sobre la base del gran potencial predictivo del *Big Data*[49]. Además, dicha tecnología permite hacer personales datos que antes no lo eran, aumentando el riesgo sobre los derechos fundamentales[50].

En cuanto a las implicaciones en la normativa sobre protección de datos, podemos destacar algunas resoluciones que ofrecen las instituciones especializadas, como la resolución aportada sobre el *Big Data* por el Grupo de Trabajo Internacional sobre Protección de Datos de las Telecomunicaciones (IWGDPT), en la que se destacan problemas como[51]:

- Datos utilizados para nuevos propósitos;
- maximización de datos y la falta de transparencia en su tratamiento;

---

[48] *Vid*. GANDOMI, Amir y HAIDER, Murtaza, «Beyond the hype: Big data concepts, methods..., *op. cit.,* p. 62.

[49] *Vid.* GONÇALVES, Maria Eduarda, «The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward», en *Information & Communications Technology Law*, vol. 26, n.º 2, Taylor & Francis, 2017, p. 6.

[50] *Vid*. GIL GONZÁLEZ, Elena, «Big Data y datos personales, ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley*, nº 9050, La Ley, Madrid, 2017, p. 3.

[51] *Vid*. International Working Group on Data Protection in Telecommunications. *Working Paper on Big Data and Privacy: Privacy Principles Under Pressure in the Age of Big Data Analytics [675.48.12],* 6 de mayo de 2014, pp. 1-18. Disponible en: <http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf?1407931243>.

- información sensible que puede ser recolectada;
- riesgo de reidentificación;
- implicaciones en la seguridad;
- inexactitud, y
- «efecto enfriamiento», debido a la huella digital generada en Internet a lo largo de los años.

Es destacable la resolución de la 36.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que otorga unas reglas de comportamiento[52]:

- Respetar el principio de especificación de finalidad.

- Obtener el consentimiento válido del titular de los datos.

- Ofrecer acceso a la información sobre los criterios para la toma de decisiones (algoritmos) que se han utilizado como base para el desarrollo del perfil.

- Llevar a cabo una evaluación de impacto en la privacidad, especialmente cuando el análisis del *Big Data* implica usos novedosos o inesperados de los datos personales.

- Desarrollar y utilizar tecnologías del *Big Data* de acuerdo con los principios de la privacidad por diseño.

- Considerar cuándo los datos anónimos mejorarán la protección de la privacidad. La anonimización de datos ayuda a mitigar los riesgos, pero solo si está diseñada y gestionada apropiadamente; además de usarse combinadamente con otras técnicas.

- Aplicar la legislación sobre protección de datos cuando se utilicen datos seudonimizados.

- Utilizar las decisiones que otorga el *Big Data* de forma transparente, evitando la injusticia de unos resultados automatizados.

---

[52] *Vid*. Resolución de la 36.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Mauricio. Octubre de 2014. http://www.redipd.es/documentacion/otrosdocumentos/common/2014/ResolucionBigData.pdf.

Es de destacar que *el legislador europeo se ha nutrido de tales recomendaciones para desarrollar el RGPD, ya que tales principios se han materializado en varios artículos del reglamento*[53].

Desde las propias instituciones de la Unión Europea se ha visto necesario pronunciarse respecto del desarrollo del *Big Data* y su incidencia en la privacidad de los individuos. Destacamos en primer lugar el «Statement on Statement of the WP 29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU»[54]. En dicha opinión, el CEPD[55] resalta *los beneficios económicos que puede generar en la sociedad, pero es consciente de las implicaciones directas sobre los datos personales de los sujetos involucrados.* El Comité es consciente de que los principios relativos a la protección de datos pueden quedar obsoletos, por lo que ve conveniente una reforma del marco legal de la protección de datos. Por eso se hace necesario una constante cooperación entre las autoridades de protección de datos no solo europeas, sino también de otros países, con el fin de proporcionar una orientación unificada y respuestas operativas sobre la aplicación de las normas de protección de datos a los actores mundiales, así como llevar a cabo la aplicación conjunta de estas normas, siempre que sea posible. También es necesario asegurar a las personas que la protección de sus derechos e intereses de protección de datos es considerada fundamental por todas las partes interesadas.

Pero ha sido el Supervisor Europeo de Protección de Datos (SEPD) quien más ha contribuido a esclarecer el impacto del *Big Data* en la protección de datos[56]. De los

---

[53] *Vid.* Artículos 22, 25, 35 y considerando 28 del RGPD.

[54] WP 221. Adoptado el 17 de septiembre de 2014.

[55] El CEPD pasará a llamarse «Comité Europeo de Protección de Datos», según el artículo 61 del RGPD, a partir del 25 de mayo de 2018.

[56] *Vid*. los documentos: *Preliminary Opinion on Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy,* marzo de 2014; Discurso de Giovanni Buttarelli, *The EU Data Protection Reform: Updated Perspectives and the Challenges posed by Big Data*, Istanbul, mayo de 2014; *Report of EDPS workshop on privacy, consumers, competition and big data*, junio de 2014; Discurso de Giovanni Buttarelli, *Privacy and Competition in the Digital Economy*, enero de 2015; Discurso de Giovanni Buttarelli, *Antitrust, Privacy and Big Data*, febrero de 2015; EDPS Opinion 4/2015, *Towards a New Digital Ethics: Data, Dignity and Technology*, septiembre de 2015; Discurso de Giovanni Buttarelli, *Competition Rebooted: Enforcement and Personal Data in Digital Markets*, septiembre de 2015; EDPS Opinion 7/2015, *Meeting the Challenges of Big Data: A Call for transparency, user control, data protection by design and accountability*, EDPS Opinion 8/2016, *Coherent Enforcement of Fundamental Rights in the Age of Big Data*; EDPS-BEUC Conference, Big Data: Individual Rights and Smart Enforcement, 29 de septiembre de 2016; EDPS blog post, *Big Data Rights: Let's Get Together*, octubre de 2016.

documentos relacionados con el *Big Data,* debemos destacar el dictamen del supervisor europeo de protección de datos sobre «hacer frente a los desafíos que se plantean en relación con los macrodatos: llamamiento a la transparencia, el control por parte de los usuarios, la protección de datos desde el diseño y la rendición de cuentas»[57], el cual destaca, en el mismo sentido que el CEPD, *que los macrodatos, si se gestionan de manera responsable, pueden aportar beneficios significativos y una mayor eficiencia para la sociedad y las personas no solo en temas relacionados con la salud, la investigación científica, el medio ambiente y otros ámbitos específicos.* Pero existe una profunda inquietud en relación con las repercusiones reales y potenciales del tratamiento de grandes cantidades de datos sobre los derechos y las libertades de las personas, incluido el derecho a la intimidad. Los desafíos y los riesgos que plantean los macrodatos exigen, por tanto, una protección de datos más efectiva.

El SEPD considera que el desarrollo sostenible y responsable de los macrodatos deberá basarse en *cuatro elementos esenciales:*

- Las organizaciones deberán ser más transparentes en relación con el modo en que tratan los datos personales.

- Deberá permitirse a los usuarios un elevado nivel de control sobre el modo en que se utilizan sus datos.

- Deberá integrarse una protección de datos con un diseño de fácil uso en los productos y servicios.

- Las organizaciones deberán ser más responsables de sus actos.

Una vez analizado lo anterior, podemos destacar las siguientes reflexiones[58]:

1.ª *El principio de «minimización de datos» no se cumple en la práctica.* Este principio implica que los datos recopilados no deben ser excesivos, sino que debe recopilarse solo

[57] (2016/C 67/05).

[58] *Vid*. GIL GONZÁLEZ, Elena, *Big Data, privacidad y protección de datos,* AEPD, Madrid, 2016, pp. 52-53.

la cantidad mínima necesaria para el fin por el que se recogen. Pero en contadas ocasiones las autoridades de protección de datos obligan de forma eficaz a las empresas a rediseñar sus procesos para minimizar los datos recabados. Sin embargo, observamos que este principio se opone al fundamento mismo del *Big Data:* la recolección masiva de datos. Como dice el IWGDPT, prima la «maximización de datos».

2.ª *La normativa confía demasiado en el consentimiento informado del individuo para recopilar y tratar sus datos de carácter personal.* Esto supone un problema, dada la experiencia de que la gran mayoría de los individuos no lee las políticas de privacidad antes de prestar su consentimiento; y aquellos que lo hacen no las comprenden. Así, otorgar el consentimiento es, con carácter general, un ejercicio vacío.

3.ª *La anonimización ha demostrado tener limitaciones.* Si bien se presentaba como la mejor solución para tratar los datos protegiendo la privacidad de los sujetos, en los últimos años se han dado numerosos casos de reidentificación de bases de datos que habían sido anonimizadas. Cada vez se hace más sencillo reidentificar a los sujetos, ya no solo a través del análisis de distintas fuentes que contienen datos personales parciales de una persona, sino a través de datos no personales. Esto supone un debilitamiento de la anonimización como medida para asegurar la privacidad durante el tratamiento de datos.

4.ª *El* Big Data *aumenta el riesgo relacionado con la toma de decisiones de forma automática.* La consecuencia es que actos importantes para las personas queden sujetas a algoritmos ejecutados de forma automática. El problema surge cuando los datos son analizados por medio de algoritmos inexactos, pero los individuos no tienen incentivos para corregirlos porque no son conscientes de que están siendo utilizados para tomar decisiones que les afectan.

En definitiva, el mayor riesgo destacado por las fuentes es la posibilidad de la reidentificación del individuo, en parte no solo debido a las capacidades del *Big Data,* sino también por la imposibilidad de las técnicas de anonimización de conseguir una probabilidad de reidentificación «cero».

Debemos destacar la incidencia en *uno de los elementos fundamentales del derecho a la protección de datos: el consentimiento.* Si la utilización de las herramientas del *Big*

Data comprende la interrelación de grandes bases de datos y la cesión o comunicación de datos de carácter personal entre ellas, *esto exige el consentimiento específico, libre, inequívoco e informado del titular de los datos.* Teniendo en cuenta que este consentimiento no puede ser recabado genéricamente y, mucho menos, para grandes volúmenes de datos que se encuentran desestructurados en diferentes almacenamientos y entornos de acceso telemático, la dificultad de su utilización lícita resulta evidente[59].

Mención especial debemos hacer a *uno de los efectos con más impacto a raíz del* Big Data: *la elaboración de perfiles.*

La elaboración de perfiles comprende la salida del proceso algorítmico automatizado, e implica el reconocimiento de patrones para propósitos predictivos o de evaluación basados en datos voluntarios, observados y obtenidos en la nube[60].

Tal y como hemos demostrado en el apartado II.3 del presente trabajo, pusimos de relieve en los ejemplos 1 y 2 claras demostraciones de las consecuencias de la elaboración de un perfil[61] por parte de una empresa a determinados afectados[62]. *Un perfil implica encuadrar a una persona, en función del resultado del tratamiento informatizado de sus datos, en un grupo concreto al que se le atribuyen unos comportamientos futuros, cuya utilización en la toma de decisiones puede suponer una valoración desfavorable de sus características y, por consiguiente, su discriminación en varios actos de su vida*[63]. Por ello, los perfiles suponen un impacto en los derechos de los afectados por la gran cantidad de datos recogidos y utilizados para elaborarlos, combinando y cruzando los

---

[59] *Vid.* DAVARA RODRÍGUEZ, Miguel Ángel, «*Big Data*», en *El Consultor de los Ayuntamientos,* n.º 15, Wolters Kluwer, Madrid, 2013, p. 1.

[60] *Vid.* SAVIRIMUTHU, Joseph, «Do algorithms dream of 'data' without bodies?», en *International Review of Law, Computers & Technology,* vol. 31, n.º 2, Routledge, 2017, p. 256.

[61] El artículo 4. 4) del RGPD lo define como 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.

[62] Es más adecuado utilizar el término «afectado» que «interesado»: los interesados en los datos personales pueden ser muchos, y algunos de ellos no muy buenos.

[63] *Vid*. GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua,* Dykinson, Madrid, p. 67.

distintos datos recogidos por varias vías[64]. Esos datos por los cuales se basan para la creación de perfiles suelen ser enfermedades que padecimos o padecemos actualmente, accidentes de tráfico que hemos sufrido, deudas pasadas y presentes, y una de sus principales manifestaciones es la creación de «listas negras»[65], con graves efectos negativos sobre los individuos tanto en el entorno asegurador como en el crediticio.

Debido a los problemas resaltados, el Comité de Ministros del Consejo de Europa adoptó el 23 de noviembre de 2010 la Recomendación (2010)13 sobre la protección de las personas físicas con respecto al tratamiento automatizado de datos de carácter personal. En la recomendación reconocen los usos del *Big Data* como *medio para recopilar y tratar datos a gran escala tanto en el sector público como en el privado, además de mejorar y segmentar el mercado en busca de mayores beneficios y en la prevención de conductas fraudulentas, pero también resalta los problemas derivados de su uso:*

a) *La creación de perfiles puede conducir a incluir a las personas en categorías predeterminadas sin que tengan conocimiento de ello*. La falta de precisión por el tratamiento automatizado puede suponer graves riesgos para los derechos y libertades.

b) *La atribución de perfiles puede generar datos personales no proporcionados por el afectado,* se ve afectado el control sobre la identidad de la persona interesada, y siendo privada de manera arbitraria del acceso a ciertos bienes y servicios, violando el principio de no discriminación.

También debemos recalcar los principios planteados en la resolución de Varsovia sobre *profiling* de la 35.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad:

- Garantizar la necesidad del *profiling* y establecer las garantías adecuadas para tal operación.

---

[64] *Vid*. SÁNCHEZ BRAVO, Álvaro (ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez*, Punto Rojo Libros, Sevilla, 2014, p. 18.

[65] *Vid*. WP 65 Documento de trabajo sobre las listas negras. Adoptado el 3 de octubre de 2002.

- Respetar los principios de calidad de datos, finalidad, exactitud y veracidad, de acuerdo con el principio de privacidad por diseño.

- Validar continuamente los perfiles y los algoritmos.

- Respetar el principio de información para permitir que el afectado controle sus datos en todo momento.

- Respetar los derechos de rectificación, acceso, y a no ser objeto de una decisión basada en un tratamiento automatizado.

- Supervisar adecuadamente las operaciones.

Es por todos los riesgos presentados por lo que existe *el derecho a no ser objeto de una decisión basada únicamente en un tratamiento automatizado en las diferentes normas sobre protección de datos europeas.* El nuevo RGPD materializa este derecho en el artículo 22, al establecer que el afectado tendrá derecho a no ser objeto de tales conductas cuando le afecten jurídicamente o tengan un efecto similar. *Este derecho es diferente a otros que podemos encontrar en el RGPD,* como el derecho de oposición (artículo 21), el derecho de supresión (artículo 17), o el derecho a la rectificación (artículo 16), *puesto que este derecho puede parecer que no se ejerce por parte del afectado.* Esta misma disposición puede dividirse teóricamente en dos vertientes: por un lado, el apartado 1 es configurado como un «derecho» del afectado a que, en cualquier decisión que pueda tener efectos jurídicos, exista intervención humana; y por el otro, el apartado 4 establece la «prohibición» de que las decisiones automatizadas no se basen en categorías especiales de datos. Dependiendo de cómo se tratase, las consecuencias pueden ser varias[66]:

1. *Tratándolo como un derecho*[67] de oposición hace depender su efecto de la acción de la persona afectada, al menos para los procesos de decisión que no entran dentro de las tres categorías de excepciones del párrafo segundo. Este es claramente un resultado más débil de una perspectiva de privacidad y protección de datos que si el artículo 22.1 es tratado como una prohibición.

---

[66] *Ibidem*, p. 10.

[67] A favor de esta consideración, *Vid*. SAVIRIMUTHU, Joseph, «Do algorithms dream of 'data'..., *op. cit.,* p. 259.

2. *Considerándolo una prohibición,* se prohíben aquellos procesos de decisión que no estén comprendidos en las excepciones previstas en el apartado 2, independientemente de la acción o inacción de la persona afectada, permitiendo únicamente los procesos decisorios especificados en el apartado 2 (con las calificaciones indicadas en los párrafos tercero y cuarto). Tal resultado es mejor respecto al objetivo general del artículo 22 y, de hecho, del RGPD en general: proteger la privacidad y la protección de datos como derechos humanos fundamentales frente a la evolución tecnológica y de cualquier otro tipo.

Además, si el derecho del artículo 22.1 es ejercitado por el afectado, funcionaría efectivamente como un derecho a garantizar la participación humana en la toma de decisiones en cuestión. Esto haría superflua la salvaguardia de la «implicación humana» que se establece en el artículo 22.3 como requisito previo para la aplicación de las excepciones a) y b) al artículo 22.1. Según lo visto, tanto desde un punto de vista lógico como desde una perspectiva más teleológica, basada en la preocupación por la privacidad y la protección de datos como derechos fundamentales, tiene más sentido concluir que el derecho aparente proporcionado por el artículo 22.1 no tiene que ser ejercida por el interesado. Lo más probable es que el «derecho» funcione, en otras palabras, como una prohibición (calificada) con la que el tomador de la decisión debe cumplir con independencia de si el «titular del derecho» lo invoca o no[68].

En la normativa española, este derecho se restringía solamente a la toma de decisiones, y se consideraba una modalidad del ejercicio del derecho de oposición de la LOPD manifestado en el artículo 13 respecto a la impugnación de valoraciones, en los artículos 16 de la LOPD (artículo 18 del Proyecto de LOPD de 2017) y 36 del RLOPD en cuanto al derecho de oposición. Ahora, con el nuevo RGPD, el derecho se configura de forma autónoma respecto al derecho de oposición. El artículo 11 del Proyecto de LOPD de 2017 contempla que si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que pudieran producir efectos jurídicos sobre él o afectarle significativamente.

---

[68] *Ibidem*, p. 11.

II.5.2. Implicaciones en la protección legal del algoritmo

En cuanto a la protección legal del algoritmo, se ha mostrado complicada su defensa legal:

a) *Patentes.* En el ámbito nacional, está descartado su patentabilidad debido a su consideración como mero método matemático por el artículo 4.4 de la Ley 24/2015 de Patentes[69,70]. Respecto al ámbito europeo, también se rechaza su patentabilidad por los mismos motivos en el artículo 52 del Convenio de Múnich. La cámara de recursos de la Oficina Europea de Patentes ha rechazado varias solicitudes de patente de algoritmos[71].

b) *Propiedad intelectual.* Aunque podemos encuadrar como software un algoritmo, el artículo 96.4 del TRLPI no protege «las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador incluidos los que sirven de fundamento a sus interfaces». En este sentido, se ha pronunciado el TJUE en el asunto C-406/2010 *SAS Institute Inc. vs. World Programming Ltd.*[72].

c) *Secreto industrial o comercial/Know-How.* Como última vía frente a las anteriores, el Know-How puede ser una solución adecuada. Su definición no se encierra recogida legalmente, sino que ha sido el Tribunal Supremo, en su STS de 19 de diciembre de 2002, quien la ha definido como «conjunto no divulgado de informaciones técnicas, patentadas o no, que son necesarias para la reproducción industrial directamente y en las mismas condiciones de un producto o un procedimiento». La protección del

---

[69] BOE-A-2017-3550.

[70] El Real Decreto 316/2017, de 31 de marzo, por el que se aprueba el reglamento para la ejecución de la Ley 24/2015 tampoco ofrece novedades respecto a esta materia.

[71] Vicom Systems Inc. (1986); IBM (1989); Pension Benefit System Partnership (2000); Infineon Technologies AG (2006).

[72] «[N]i la funcionalidad de un programa de ordenador ni el lenguaje de programación o el formato de los archivos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones constituyen una forma de expresión de ese programa y, por ello, carecen de la protección del derecho de autor sobre los programas de ordenador en el sentido de la Directiva 91/250».

Know-How, como secreto industrial, está recogido en la ley de Competencia Desleal[73] y en el Código Penal (artículos 278 y ss.).

Recientemente se ha aprobado la Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas[74], que permite aumentar el nivel de protección de los secretos comerciales. La directiva define al Know-How en su considerando 1 como «obtención, desarrollo y aplicación de conocimientos técnicos». Para que se considere «secreto comercial» a efectos de la directiva, debe reunir determinados elementos:

1. ser secreta;

2. tener un valor comercial, y

3. haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control.

Teniendo en cuenta estas características, podemos afirmar que *los algoritmos pueden considerarse como secretos comerciales, y estar protegidos tanto por la directiva como por la ley de Competencia Desleal.*

Aunque lo siguiente no afecte al negocio asegurador, es necesario mencionar que las negociaciones basadas en algoritmos se encuentran reguladas en la Unión Europea por el Reglamento Delegado (UE) 2017/589 de la Comisión, de 19 de julio de 2016, por

---

[73] «Artículo 13. Violación de secretos:
1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14.
2. Tendrán, asimismo, la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo.
3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto».

[74] DOUE L 157/1, 15 de junio de 2016.

el que se completa la Directiva 2014/65/UE del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación que especifican los requisitos organizativos de las empresas de servicios de inversión dedicadas a la negociación algorítmica[75], pero cuya exclusión a las entidades aseguradoras se produce por el artículo 2.1.a) de la Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros[76].

II.5.3. Implicaciones legales sobre las bases de datos

Gran parte del valor de las empresas que utilizan el *Big Data* basan sus activos en los datos que van acumulando y organizando en bases de datos para su análisis. Esta actividad requiere ser conscientes de la protección de las bases de datos que brinda nuestra Ley de Propiedad Intelectual (LPI)[77].

La LPI, en el artículo 12, define a las bases de datos como «las colecciones de obras, de datos o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma».

Los datos en sí mismos no son protegibles, salvando los datos de carácter personal que protege el RPGD o aquellos datos que pudieran beneficiarse de una protección especial por razón de lo que son. Sin embargo, las bases de datos que los contienen sí que se benefician de una doble protección otorgada por la Ley de Propiedad Intelectual:

a) *Protección de la base de datos por el derecho de autor.* Es la protección otorgada por el artículo 12 LPI. Es bastante complicada de obtener, pues la ley exige que la base de datos sea original en cuanto a la estructura y la disposición de sus contenidos (12.1 LPI), lo cual deberá evaluarse caso por caso. Esta protección alcanza a dicha

---

[75] DOUE L 87/417, 31 de marzo de 2017.

[76] DOUE L 173/349, 12 de junio de 2014.

[77] *Vid*. VIVAS TESÓN, Inmaculada, «La tutela "sui generis" de las bases de datos», en *Revista de Derecho Patrimonial*, n.º 21, Aranzadi, Cizur Menor, 2008; GONZÁLEZ ROYO, Ignacio, «La protección de los intangibles intelectuales e industriales en el contexto del Fintech», en *Diario La Ley*, n.º 8795, La Ley, Madrid, 2016.

estructura y disposición, lo que impediría la fabricación de una base de datos idéntica aunque de distinto contenido.

b) *Protección de la base de datos por el derecho* sui generis, *respecto de su contenido, impidiendo la extracción y la reutilización.* Es la protección más usual, encaminada a la protección de la inversión en la creación de la base de datos, pues impide que se pueda extraer y reutilizar su contenido sin autorización del titular. El régimen de esta protección se encuentra en los artículos 133-136 LPI, y cuyo régimen se debe a la transposición de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

   Esta protección corresponde al fabricante de la base de datos (persona física o jurídica que realiza la inversión) y se extiende durante quince años desde la elaboración o divulgación de la base de datos, con posibilidad de obtener una protección adicional por ese plazo en caso de realizarse una nueva modificación sustancial de la misma. Es muy importante probar la inversión que se ha hecho, no en la creación de los datos, sino en la organización y disposición de estos, como viene señalando el TJUE[78].

II.6. *CLOUD COMPUTING* Y SU RELACIÓN CON EL *BIG DATA*

Cabe destacar la relación entre dichas tecnologías para la consecución de un resultado aplicando la tecnología *Big Data*. No hay que olvidar que una de las claves del *Big Data* es el procesamiento de una gran cantidad de datos que requiere gran capacidad de procesamiento y espacio para lograrlo, y esto se consigue mediante un servicio tal como el *Cloud Computing*. Es decir, la aplicación del *Cloud Computing* al *Big Data* se denomina *Big Data Computing*[79].

El *Big Data* y el *Cloud Computing* juegan un papel complementario: el avance de una tecnología condiciona al otro. El *Big Data* requiere nuevos elementos para adaptar su

---

[78] SSTJCE, 9 de noviembre de 2004, asuntos C-46/02 (TJCE 2004, 320), C-203/02 (TJCE 2004, 321), 338/02 (TJCE 2004, 319) y 644/02 SIC (TJCE 2004, 318).

[79] *Vid.* POKORNY, Jaroslav y STANTIC, Bela, «Challenges and opportunities in Big Data Processing», en MA, Zongmin, *Managin Big Data in Cloud Computing environments*, IGI Global, Pensilvania, 2016, p. 2.

procesamiento, y esto se traduce en la necesidad de una nueva infraestructura. El *Cloud* ofrece flexibilidad y eficiencias para el acceso al dato y la generación de conclusiones de estos datos[80].

Una solución *Cloud Computing* permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura, sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones[81].

En el entorno *Cloud,* hay que destacar las diferentes modalidades del servicio:

1. *Software como servicio.* Podemos hablar de una nube de software cuando el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un *workflow,* un programa para la gestión documental de su empresa, etc. *En esta modalidad solo te tienes que preocupar de recoger y analizar los datos.*

2. *Infraestructura como servicio.* Si el valor añadido es nulo, se puede hablar de una nube de infraestructura (IaaS). En ese caso, el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero.

3. *Plataforma como servicio.* Entre estas dos aproximaciones se pueden encontrar otras intermedias llamadas PaaS (Plataforma como Servicio), en las que se proporcionan utilidades para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones. *Te proporciona un entorno para trabajar directamente con* Big Data. *Se puede hacer el procesamiento y análisis de los datos de una manera transparente en cuanto a detalles de infraestructura.*

---

[80] *Vid.* KSHETRI, Nir, FREDRIKSSON, Torbjörn y ROJAS TORRES, Diana Carolina, *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South*, Routledge, Oxford, 2017, p. 8.

[81] *Vid*. AEPD, *Guía para clientes que contraten servicios de Cloud Computing,* Madrid, 2013, p. 3.

El *Cloud Computing* implica la entrada de un nuevo actor en el proceso de tratamiento de datos, al entregar toda la información en los servidores de una empresa externa. Por lo tanto, el proveedor de servicios en la nube es considerado un encargado de tratamiento.

Debemos acercarnos a este fenómeno empresarial desde una perspectiva funcional, jurisdiccional y contractual:

1. *Perspectiva funcional:* estudiará qué funciones y servicios *(Cloud Computing)* generan consecuencias legales para los participantes, tales como: a) las exigencias del cumplimiento normativo de un determinado servicio prestado a través de la nube; b) el reparto de las responsabilidades de cumplimiento normativo entre el proveedor de la nube y su cliente; c) que la capacidad del proveedor de servicios en la nube para generar evidencias electrónicas resulta necesaria para dar debida respuesta al cumplimiento normativo, y d) el papel que debe desempeñar la empresa cliente a la hora de aproximar las posiciones del proveedor de servicios en la nube y sus auditores y asesores externos.

2. *Perspectiva jurisdiccional:* analiza la forma en la que los gobiernos administran las leyes que afectan a los servicios de *Cloud Computing*. Problema del «principio de territorialidad»: resulta complicado determinar dónde se ubican los servidores en los que se aloja la información y resulta complejo determinar qué norma puede llegar a aplicarse en cada momento. No debe servir para excusar el incumplimiento por parte de las empresas que prestan servicios de *Cloud Computing* de los principios jurídicos de la protección de datos y la privacidad que protegen a los ciudadanos. Problema: las autoridades extranjeras podrían tener competencia para «confiscar» tal información. Solución: el proveedor de servicios de *Cloud Computing* debería obligarse a no transferir la información a otros países sin el previo consentimiento expreso del cliente.

3. *Perspectiva contractual:* debe encargarse de examinar los contenidos de los contratos y sus mecanismos de aplicación. Es muy recomendable que las partes de un contrato de prestación de servicios en la nube anticipen en su clausulado las fórmulas de resolución de la problemática relacionada con la recuperación de la información y de los datos personales, que son responsabilidad del cliente una vez extinguida

la relación contractual. Otra cuestión relativa a la responsabilidad entre las partes es delimitar las obligaciones técnicas mediante un *acuerdo de nivel de servicio*. Este clausurado determina la calidad que debe garantizar el proveedor del servicio, tanto el rendimiento y disponibilidad del servicio, como las indemnizaciones por incumplimiento del nivel acordado del servicio.

Por otra parte, la externalización del tratamiento de datos siempre supone un riesgo para la empresa, puesto que siempre será considerada responsable última. En este sentido, el contrato de encargado formalizado entre ambas partes debe contener:

- Modelo de relación/gobierno del contrato donde, entre otras cosas, se establezca los canales de comunicación entre el proveedor y la empresa.

- Ubicación de los datos y posibles transferencias asociadas (por ejemplo, por labores de mantenimiento de la propia infraestructura soporte al servicio) tanto para limitar tales transferencias, como para conocer en todo momento dónde van a residir los datos, y establecer contractualmente qué ubicaciones pueden ser consideradas adecuadas. No debe perderse de vista que los proveedores de servicios *Cloud* suelen tener *data center* en diversas ubicaciones.

- El deber de secreto y confidencialidad.

- La obligación de cumplir con las normativas de privacidad y protección.

- Las medidas y políticas de seguridad que deberá tener en consideración e implantar para garantizar la protección de los datos.

- Procedimiento de comunicación y gestión de incidentes de seguridad.

- La obligación de conocer a los subencargados y que garantice que se les ha transmitido las mismas obligaciones y responsabilidades que el proveedor haya asumido con la entidad contratante.

- La necesidad de garantizar la portabilidad de los datos y la existencia de un plan de reversión del servicio.

- La necesidad de colaborar en todo momento ante peticiones que pudiera recibir la compañía tanto de reguladores como de supervisores, etc.

- La posibilidad de realizar revisiones y auditorías del cumplimiento tanto del contrato como de las normativas que pudieran ser de aplicación.

- Consideraciones sobre la propiedad intelectual que dependerá precisamente del tipo de servicio que se esté contratando.

III. DATOS PERSONALES QUE PUEDEN SER TRATADOS

III.1. CONCEPTO DATO PERSONAL

III.1.1. Importancia del concepto

Siguiendo a PIÑAR MAÑAS, la importancia del concepto de «dato personal» es resaltada por los objetivos concretos que busca, y que están recogidos en el articulado del Convenio 108 del Consejo de Europa[82], la Carta Europea de Derechos Fundamentales[83], del RGPD[84] y de la LOPD[85], que puede resumirse en la protección de manera eficaz del derecho fundamental a la protección de datos (18.4 de la CE). Visto que la norma busca la definición de dato personal, y crea un conjunto de elementos de protección frente a estos datos, la consideración de un dato como «personal» implica la afectación al derecho a la protección de datos, y la aplicación de todas sus normas.

La protección de datos comenzó siendo definida como «el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad»[86]. El Tribunal Constitucional se pronunció por primera vez sobre el alcance del derecho fundamental a la protección de datos en

---

[82] «Artículo 1: garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueran su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos)».

[83] «Artículo 8.º: toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan».

[84] «Artículo 1: proteger las libertades y los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».

[85] «Artículo 1: garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar».

[86] *Vid*. DAVARA RODRÍGUEZ, Miguel Ángel, *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones,* Fundación VODAFONE, Madrid, 2004, p. 3.

la STC 254/1993 (fundamento jurídico 6.º), configurándolo como un derecho autónomo, «una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza a la dignidad y a los derechos de las personas [...] un instituto que es, en sí mismo, un derecho o libertad fundamental: el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de los datos, lo que el Constitucional llama "informática"».

En una sentencia posterior se precisa la definición y contenido del derecho, considerando el derecho a la protección de datos como «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, sea el Estado o un particular» (fundamento jurídico 7.º STC 292/2002).

«El objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de datos personales sean o no íntimos, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado, porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituye una amenaza para el individuo» (fundamento jurídico 6.º STS 292/2002).

El concepto de protección de datos ha evolucionado a lo largo de los años con la aprobación de las posteriores normas. Con el Convenio 108, el alcance de la protección de datos llegaba hasta los tratamientos automatizados[87]. El siguiente hito normativo en España es la promulgación de la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal donde, aunque generalmente estaba destinada a proteger los datos en un tratamiento automatizado, sí preveía el tratamiento no automatizado de datos para el uso posterior en el tratamiento de los mismos[88].

El punto de inflexión lo encontramos en la Directiva 95/46/CE[89] cuando se aplica indistintamente a los tratamientos automatizados como no automatizados, y esta consideración se ha visto transpuesta en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Ahora con el RGPD el concepto de protección de datos cambia al ampliarse el alcance de lo que supone la «protección» de los datos. La seguridad de la información se ha vuelto un concepto clave que pretende proteger la información garantizando su disponibilidad, integridad y la confidencialidad de la misma[90].

Que el derecho a la protección de datos tenga el carácter de fundamental comporta una serie de garantías[91]:

1. *Eficacia directa de los derechos fundamentales.* Nuestra Constitución consagra la eficacia directa entre los particulares *(Drittwirkung)*[92] en el artículo 9.1, en el que estipula que «los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico». El significado de esto es que los derechos fundamentales

---

[87] *Vid.* Artículo 1.

[88] *Vid.* Artículo 2.1.

[89] *Vid.* Artículo 3.1.

[90] Como herramienta jurídica para garantizar dichos elementos, es necesario aplicar el Real Decreto 3/2010, por el que se aprueba el Esquema Nacional de Seguridad.

[91] *Vid*. ROSELLÓ MALLOL, Víctor, «Marketing y protección de datos (I). Concepto de dato personal», en *Noticias Jurídicas*. Disponible en: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4479-marketing-y-proteccion-de-datos-i-:-concepto-de-dato-personal.

[92] *Vid*. SCHWABE, Jürgen, «Bundesverfassungsgericht und 'Drittwirkung' der Grundrechte», en *Archiv für offentliches Recht*, n.º 100, 1975, p. 442 y ss.

no solo rigen directamente para los poderes públicos, sino también para los particulares, es decir, existe una eficacia directa tanto vertical como horizontal[93]. La existencia de la Constitución obliga a los jueces a interpretar las normas conforme a ella, en especial, conforme a los derechos fundamentales. Por lo que son, en primer lugar, los garantes de los derechos fundamentales y de las libertades públicas.

2. *Reserva de Ley Orgánica.* El artículo 81 CE dicta que el desarrollo de los derechos fundamentales y de las libertades públicas debe hacerse mediante una ley orgánica, que supone un procedimiento agravado con el fin de que la futura ley cuente con el respaldo de la mayoría de la ciudadanía a través de sus representantes parlamentarios. La Ley Orgánica del Tribunal Constitucional (LOTC) limita el catálogo de derechos fundamentales a los comprendidos en la Sección 1.ª del capítulo II del Título I (artículos 14 al 29 y el 30.2).

3. *Recurso de amparo ante el Tribunal Constitucional.* Es una de las garantías que establece la CE en su artículo 53.2 para la protección de los derechos fundamentales. El artículo 41 LOTC establece como objeto del recurso de amparo los derechos fundamentales anteriormente mencionados.

4. *Recurso directo ante el Tribunal Europeo de Derechos Humanos, en virtud de la Carta Europea de Derechos Fundamentales.* El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales recoge en su artículo 34 la posibilidad de que cualquier particular que considere que los derechos reconocidos en el texto han sido violados, podrá recurrir ante el citado tribunal. El propio artículo 8 del convenio regula el derecho al respeto de la vida privada y familiar[94], por lo que este derecho es reclamable ante el Tribunal Europeo de Derechos Humanos.

---

[93] *Vid. et al.* BATISDA FREIJEDO, Francisco José, *Teoría general de los derechos fundamentales en la Constitución Española de 1978,* Tecnos, Madrid, 2004, pp. 179-195.

[94] «Artículo 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

III.1.2. Concepto legal

Son varios los textos que nos otorgan una descripción del concepto en las diferentes escalas jerárquicas de un sistema legal. Podemos empezar por la definición que otorga el Convenio 108 del Consejo de Europa en su artículo 2 a): *información sobre una persona física identificada o identificable*[95]. Esta definición servirá como base para las siguientes normas sucesivas sobre el material.

La Directiva 95/46/CE mostraba la definición en su artículo 2 a): «toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

Nuestra Ley Orgánica de Protección de Datos copia la definición de la propia Directiva en su artículo 3 a). A lo que su reglamento de desarrollo amplía la definición en su artículo 5.1 f) con cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables[96].

A todo esto, cabe destacar la definición otorgada por el nuevo RGPD en su artículo 4.1): «Toda información sobre una persona física identificada o identificable; 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».

---

[95] STJCE en el asunto C-101/2001(Lindqvist) de 6 de noviembre de 2003, apartado 24: El concepto de «datos personales» que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha directiva «toda información sobre una persona física identificada o identificable». Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones.

[96] *Vid.* BERNAL RIOBOO, Lourdes, «Diccionario de conceptos relativo a la protección de datos», en *Diario La Ley*, nº 6921, La Ley, Madrid.

Como observamos, todas las definiciones tienen un carácter abierto, y no solo se pueden limitar a los datos clásicos como son los nombres, apellidos o datos genéticos, sino a cualquier elemento que nos haga «identificables». Véase, por ejemplo, los rastros que dejamos en las redes sociales como Facebook o Twitter a través de *likes* o *tweets,* que muestran nuestras preferencias ante los demás miembros de estas.

La Opinión 4/2007 del Comité Europeo de Protección de Datos (CEPD) señala unos criterios interpretativos que deben rodear la definición de «dato personal»: a) la definición de «dato personal» tiene una concepción amplia, con el fin de que no exista fugas en su aplicación práctica; b) el objetivo principal de las normas de protección de datos es la propia protección del individuo; c) se busca flexibilidad dependiendo de las circunstancias del caso concreto; d) el ámbito de aplicación de las normas de protección de datos no debe ser demasiado amplio; e) pero también debe evitarse la restricción indebida de la interpretación del concepto de datos personales.

La propia definición de *dato personal* cabe subdividirla y desarrollarla en el mismo sentido que la Opinión 4/2007:

1. «*Cualquier información*». El término tiene un concepto amplio, por lo que es objeto de amplia interpretación. Según la STJUE, Nowak[97] no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, y siempre que sean «sobre» la persona en cuestión.

   Este último requisito se cumple cuando, debido a su contenido, finalidad o efectos, la información está relacionada con una persona concreta. En este punto, caben distinguir tres dimensiones:

   a) *Naturaleza de la información.* Incluye cualquier tipo de identificación sobre una persona. Cubre información objetiva (los datos biométricos) como datos subjetivos, aquellos generados sobre un elemento fáctico, como puede ser una valoración respecto a una determinada conducta de una persona física (la valoración

[97] *Vid.* STJUE, 20 de diciembre de 2017, asunto C-434/16, *Peter Nowak.*

positiva o negativa de la conducción de un sujeto). No es necesario que esos datos tengan que ser verídicos para considerarlos «personales».

b) *Contenido de la información.* Contiene todos aquellos datos que proporcionan información cualquiera que sea la clase de esta. Incluye la información personal considerada «datos sensibles»[98]. Los datos personales comprenden la información relativa a la vida privada y familiar, e información sobre cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El término *vida privada y familiar* tiene un concepto amplio ya definido por la jurisprudencia[99].

c) *Formato de la información contenida.* Incluye la información disponible en cualquier forma alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo (como estipula el RLOPD). Se trata de una consecuencia lógica de la inclusión en su ámbito de aplicación del tratamiento automático de datos personales. Respecto a los datos biométricos, son definidos por el CEPD en esa misma opinión como «propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad»[100]. Estos datos tienen en sí una doble vertiente: 1) se consideran contenido de la información, 2) como elemento para vincular una información a una determinada persona.

---

[98] Esos datos sensibles son recogidos en el artículo 9 del RGPD: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, 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 orientaciones sexuales de una persona física. Con estos datos, como norma general, está prohibido realizar un tratamiento.

[99] Sentencia del Tribunal Europeo de Derechos Humanos en el asunto Amann/Suiza de 16 de febrero de 2000, apartado 65: *[E]l término «vida privada» no debe interpretarse restrictivamente. En especial, el respeto por la vida privada comprende el derecho a establecer y a desarrollar relaciones con otros seres humanos; además, no hay ninguna razón de principio que justifique la exclusión de actividades de una naturaleza de profesional o empresarial de la noción de la «vida privada».*

[100] Como se ha dicho anteriormente, y como dicta el propio texto, datos biométricos proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.).

2. «*Sobre*». De modo general, se puede considerar que la información versa «sobre» una persona cuando se refiere a ella. Como norma general, es fácil establecer este tipo de relación. Por ejemplo, datos sobre los resultados de las pruebas médicas a las que se ha sometido una persona, recogidos en su historial médico, o las imágenes filmadas en video de una persona con ocasión de una entrevista. Pero hay ocasiones en las que la información no se refiere tanto a personas sino a objetos relacionados con la persona[101].

   El CEPD ya definió anteriormente qué se consideraba que una información versa «sobre» una persona. El grupo señala que «un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento, o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa»[102].

   Para considerar que un dato versa sobre una persona debe haber alguno de los siguientes elementos:

   a) *Contenido:* está presente el elemento cuando «se proporciona información sobre una persona concreta, independientemente de cualquier propósito que pueda abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el afectado».

   b) *Finalidad:* está presente el *elemento* «cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona».

   c) *Resultado:* a pesar de la ausencia de un elemento de «contenido» o de «finalidad» cabe considerar que los *datos* versan «sobre» una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto,

---

[101] Por ejemplo, 1) el valor de una vivienda propiedad de una persona cuando se utiliza como dato para el cálculo de los impuestos, o 2) un cuaderno en el que un mecánico apunta datos técnicos respecto a un vehículo, el cual está ligado a una matrícula, y a su vez, con el propietario.

[102] *Vid.* Documento n.º WP 105 del grupo de trabajo: «Documento de trabajo sobre las cuestiones relativas a la protección de datos relacionadas con la tecnología RFID», adoptado el 19 de enero de 2005, p. 8.

es probable que su uso repercuta en los derechos y los intereses de determinada persona[103].

Estos tres elementos deben considerarse como condiciones alternativas y no acumulativas. En especial, cuando exista el elemento de contenido, no hay ninguna necesidad de que también aparezcan los otros elementos para considerar que la información se refiere a una persona física.

3. *Persona física «identificada o identificable»:* se puede considerar «identificada» a una persona física *cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo.* Se considera identificable cuando sea posible hacerlo. La identificación se logra mediante datos concretos llamados «identificadores», los cuales están muy unidos a la propia persona. Identificadores pueden ser: altura, color de cabello, vestimenta, profesión, cargo, nombre, etc. En la propia definición se recoge que será «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.*

   a) *Directa:* una persona puede ser identificada directamente *mediante su nombre y apellidos.* Es el medio más común para ello, pero puede ser necesario otros datos complementarios para que no exista confusión alguna. Todos estos nuevos datos ligados al nombre y apellidos nos permiten centrarnos en un individuo concreto. Así pues, a través de los identificadores, la información original se asocia con una persona física que puede ser distinguida de otros individuos.

   b) *Indirecta:* cuando se puede identificar *mediante un número de teléfono, la matrícula de un coche, un número de Seguridad Social, un número de pasaporte o por*

[103] La puesta en funcionamiento de un sistema de geolocalización para el conocimiento por parte de una empresa de taxis con el objetivo de, mediante este tratamiento de datos, proporcionar un mejor servicio y ahorrar combustible, asignando a cada cliente que solicita un taxi el vehículo más cercano a la dirección en la que se encuentra. Los datos objetivos son los relativos a los vehículos, pero con este sistema se tiene acceso a los datos generados por los conductores, como la velocidad, itinerarios y otras conductas; por lo que pueden repercutir en las personas.

una combinación de criterios significativos (edad, empleo, domicilio, etc.), que haga posible su identificación al estrecharse el grupo al que pertenece. Nos estamos refiriendo, en general, al fenómeno de las «combinaciones únicas», sea cual sea su tamaño. Si los indicadores conocidos no permiten la individualización de una persona, la información existente combinada con otros datos permite distinguir a esa persona del resto. En este sentido, se considera como un medio indirecto que toda la información que permita identificar a una persona pertenezca a una sola[104].

Aunque la identificación a través del nombre y apellidos es, en la práctica, lo más habitual, *esa información puede no ser necesaria en todos los casos para identificar a una persona, pudiendo utilizar otros indicadores para individualizar a la persona;* por lo tanto, debe interpretarse el concepto de «dato personal» de una manera amplia[105]. En Internet existen herramientas que permiten controlar el tráfico de una determinada página realizado por un dispositivo conectado a Internet y, por lo tanto, dirigido por un usuario. Es posible recabar determinadas conductas realizadas por un usuario y clasificar a este según criterios psíquicos, económicos, sociales, culturales o de cualquier otro tipo[106]. Debido a esto, existe la capacidad de identificar a una persona sin la necesidad de llegar al conocimiento de su nombre y apellidos. Por ello, la dirección IP es considerado un dato personal[107].

Tras todo lo anterior, hay que diferenciar dos aspectos en relación con la persona identificable: 1) el hecho de no ser conocida la identidad de dicha persona por

---

[104] *Vid.* STJUE, 19 de octubre de 2016, asunto C582/14, *Breyer*.

[105] *Vid.* SERRANO CHAMORRO, María Eugenia, «Protección de datos personales: información, consentimiento y transparencia. Nuevas exigencias jurídicas comunitarias», en *Actualidad Civil,* n.º 5, Wolters Kluwer, Madrid, 2017, p. 11.

[106] Véase como ejemplo los rastros que dejamos en Internet como son los «likes» en Facebook y YouTube, o el contenido de los «tweets o retweets» generados en Twitter. Estos rastros permiten clasificar a la persona en los criterios ya comentados. STJCE, caso Lindqvist: la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento de datos personales.

[107] *Vid.* AGPD Informes 327/2003 y 0216/2008; STS, 13 de diciembre de 2014; y STJUE C-582/14 *Patrick Breyer y Bundesrepublick Deutschland*.

diversas circunstancias, y 2) que, a pesar de ello, sea posible llegar a identificar a esa persona[108].

Para determinar si una persona puede llegar a ser «identificable», debemos atenernos a lo estipulado por el considerando 26 del RGPD; ya que la propia definición no proporciona ningún criterio, salvo una alusión a los medios indirectos, que dicta que «para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos».

Esto viene a decir que *la posibilidad de individualizar a una persona no la convierte en «identificable».* Si teniendo en cuenta todos los medios disponibles para el tratamiento de datos no existe posibilidad, los costes, el tiempo necesitado y la tecnología existente, no se podrá considerar a la persona como identificable. De ahí el último inciso del artículo 5 o) del RLOPD «Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados»[109]. De ahí que la consideración de persona identificada o identificable dependa del esfuerzo dedicado para lograrlo[110].

4. «Persona física»: la protección que otorga la norma solo es aplicable a las personas físicas. En este sentido, se manifiesta los considerandos 1 y 2 del RGPD cuando

---

[108] *Vid*. ROMEO CASANOBA, Carlos María, «Definiciones: persona identificada o identificable, el afectado y el procedimiento de disociación en la protección de datos de carácter personal», en RONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, p. 230.

[109] Esta cláusula está reconocida, en su articulado, en el RLOPD; pero está recogida también en el considerando 26 de la Directiva 95/46/CE, considerando 26 del RGPD y Recommendation of the Committee of Ministers, n.º R (97) 5, en *Protection of Medical Data,* del Consejo de Europa (13 de febrero de 1997).

[110] *Vid*. DEL PESO NAVARRO, Emilio; RAMOS GONZÁLEZ, Miguel Ángel; DEL PESO RUIZ, Margarita; y DEL PESO RUIZ, Mar, *Nuevo Reglamento de Protección de Datos de Carácter Personal: Medidas de Seguridad*, Díaz de Santos, Madrid, 2012, p. 34.

afirma que: 1) «La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea ("la Carta") y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan»; 2) «Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular, el derecho a la protección de los datos de carácter personal».

III.2. CATALOGACIÓN DE DATOS

III.2.1. Datos de localización

Para esta categoría de datos, el CEPD se ha encargado en el «Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes» y en el «Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido» de solventar las dudas legales respecto a estos tipos de datos; ya que lo que no hay que negar es que el tratamiento de estos datos supone «una injerencia en la privacidad»[111].

Como hemos comentado anteriormente, los sistemas de geolocalización influyen en el negocio asegurador mediante una adecuación en la póliza en función de los valores e interpretaciones que proporcionan estos datos.

Estos datos proceden de varias fuentes:

1. *Estaciones de base.* Para conectarse a Internet, los dispositivos móviles o de comunicación 3G en adelante han de estar conectados a una antena (estación de base) que proporcione este servicio. Mientras un dispositivo esté encendido, estará en

[111] *Vid*. VELASCO NÚÑEZ, Eloy, «Tecnovigilancia, geolocalización y datos: aspectos procesales penales», en *Diario La Ley*, n.º 8338, La Ley, Madrid, p. 5.

conexión permanente con una determinada estación de base, proporcionando así un número de identificación único registrado para una ubicación concreta. La técnica usada según este método para determinar la ubicación se conoce como triangulación.

2. *Tecnología GPS.* La posición se determina mediante una serie de microprocesadores con receptores de GPS en los dispositivos. El dispositivo puede determinar su ubicación cuando la antena del GPS recibe al menos 4 de los 31 satélites que componen dicha tecnología. Esta señal es diferente de los datos de las estaciones de base porque solo viaja en un sentido. Las entidades que gestionan los satélites no tienen capacidad para establecer un registro de los dispositivos que han recibido la señal radioeléctrica. El uso de este sistema es complementado con datos de estaciones de base o puntos de acceso wifi cartografiados.

3. *Wifi.* La tecnología es similar al uso de estaciones de base. Ambas se valen de un número de identificación único (punto de acceso wifi) que puede ser detectado por un dispositivo y ser enviado a un servicio que conoce la ubicación de cada uno de estos puntos de identificación únicos. Esa identificación única se conoce como dirección MAC *(Medium Access Control).* Los puntos de acceso emiten continuamente señales, de ahí la razón de que puedan servir para geolocalizar a un usuario. Un punto de acceso wifi transmite continuamente su propio nombre de red y su dirección MAC, incluso cuando nadie esté utilizando la conexión o cuando el contenido de las comunicaciones inalámbricas esté cifrado mediante WEP, WPA o WPA2 (medidas de cifrado). La ubicación de los puntos de acceso se calcula de dos formas:

   a) *Estáticamente y una sola vez:* los propios responsables del tratamiento de datos recopilan las direcciones MAC de los puntos de acceso wifi desplazándose con vehículos equipados con antenas.

   b) *Dinámica y continuamente:* los usuarios de servicios de geolocalización recogen automáticamente las direcciones MAC captadas por sus dispositivos wifi cuando, por ejemplo, utilizan un mapa en línea para determinar su propia posición.

Los dispositivos no necesitan conectarse a puntos de acceso wifi para recoger información wifi, ya que detectan automáticamente la presencia de dichos puntos y recogen

datos sobre ellos. Aparte, esos dispositivos envían cualquier información relacionada con la localización, incluyendo los datos GPS y de estaciones de base.

Como dice el propio Dictamen 13/2011, «la geolocalización mediante el uso de puntos de acceso wifi ofrece una localización rápida y cada vez más precisa basada en mediciones continuas».

Como podemos suponer, estos datos suponen un grave riesgo para la intimidad. Esos dispositivos están estrechamente vinculados a la vida de las personas, ya que normalmente permanecen junto a ellas (como los *smartwatches* o los *smartphones*).

Estos dispositivos no suelen prestarse a otras personas debido a la gran cantidad de información privada que pueden llegar a almacenar. Debido a la gran proximidad con el usuario, permite ofrecer una imagen completa de los hábitos diarios; desde su rutina diurna hasta su periodo de inactividad nocturna. A todo esto, los patrones de comportamiento mostrados pueden incluir categorías especiales de datos, como visitas a hospitales y lugares de culto, presencia en actos políticos o en otros lugares específicos que revelen datos sobre la vida sexual. Aun más, si ese dispositivo GPS estuviera vinculado a un *smartphone* mediante *bluetooth,* sería capaz de acceder a información sobre agendas de números telefónicos e incluso tráfico de comunicaciones, a través de *logs* de llamadas efectuadas, recibidas y perdidas; y si esa tecnología se encuentra en un *smartphone* o tableta, podría se capaz de acceder a un sin fin de datos de diverso tipo[112].

La AEPD comparte este sentido en el informe 0016/2014. Sin embargo, aun observando los riesgos que comportan los datos proporcionados por la geolocalización, no se encuadran en la categoría especial de datos. Aunque una lectura detenida del artículo 9.1 RGPD demuestra que prohíbe el tratamiento de datos «que revelen [...] las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical [...] datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física».

---

[112] *Vid*. RODRÍGUEZ LAINZ, José Luis, «GPS y balizas policiales», en *Diario La Ley*, nº 8416, La Ley, Madrid, 2015, p. 5.

Si tanto el CEPD en su propio dictamen, como la AEPD en el informe anteriormente citado demuestran que esos datos pueden revelar este tipo de información, deberían estar bajo la cobertura del artículo 9 RGPD.

Los datos obtenidos mediante servicios de localización están sometidos tanto al RGPD, como a la Directiva 2002/21/CE, que será sustituida por el Reglamento sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas[113]. Cuando los datos objetos de tratamiento de las comunicaciones electrónicas se generen por la prestación y utilización de servicios de comunicaciones electrónicas, les será de aplicación la Directiva 2002/21/CE[114], en el resto de casos, será de aplicación el RGPD; ya que según los dictámenes nombrados, estos tipos de datos permiten identificar o hacer identificable a una persona. Como los dispositivos generadores de tales datos están íntimamente ligados a la persona, la identificación puede ser directa o indirecta:

a) *Directa,* mediante los datos que posee el operador del acceso GSM y el acceso móvil a Internet, como el nombre, dirección y datos bancarios de cada cliente.

b) *Indirecta,* mediante la combinación del número (o números) único del dispositivo (MAC), en combinación con una o más ubicaciones calculadas, que pueden ser transmitidas y tratadas por un servicio de geolocalización.

Respecto a estos datos, podemos distinguir tres tipos de funcionalidades:

a) *Responsables del tratamiento de datos de infraestructuras de geolocalización.* Los propietarios de bases de datos con un repertorio de puntos de acceso wifi procesan datos personales al calcular la geolocalización de un determinado dispositivo móvil inteligente. Puesto que ambos determinan los fines y medios de este tratamiento, son responsables del tratamiento con arreglo a la definición del artículo 4, apartado 7), del RGPD.

---

[113] COM (2017) 10 final.

[114] La sustitución de la directiva se prevé para el 25 de mayo de 2018, misma fecha para la entrada en vigor del RGPD.

b) *Creador del sistema operativo.* Será el responsable de tales datos cuando interactúe directamente con el usuario y recoja datos personales. Cuando ofrece una plataforma o alguna forma de venta de aplicaciones a través de la red y puede tratar los datos personales resultantes de la instalación y uso de las aplicaciones de geolocalización, con independencia de los proveedores de aplicaciones.

c) *Proveedores de aplicaciones y servicios de geolocalización.* El responsable que más nos concierne en cuanto al objeto de estudio. Estos proveedores pueden ofrecer al usuario aplicaciones en tales dispositivos y procesar los datos de localización (y otros) de un dispositivo móvil inteligente, independientemente del creador del sistema operativo o de los responsables del tratamiento de datos de la infraestructura de geolocalización. Un servicio adecuado sería el que ofrece una empresa aseguradora con el objetivo de facilitarle una serie de rutas con un menor índice de riesgo, o monitorizar su ruta con el objetivo de ofrecerle una tarificación adecuada. El proveedor de una aplicación que sea capaz de procesar datos de geolocalización es el responsable del tratamiento de datos personales resultantes de la instalación y uso de tal aplicación.

III.2.2. Datos relativos a la salud

La recolección de datos relativos a la salud es muy común en la formalización del contrato de seguro, ya que el artículo 10 de la ley de Contrato de Seguro obliga al tomador a declarar todas las circunstancias que puedan influir en la valoración del riesgo[115], y

[115] «Artículo 10 del LCS: El tomador del seguro tiene el deber, antes de la conclusión del contrato, de declarar al asegurador, de acuerdo con el cuestionario que este le someta, todas las circunstancias por él conocidas que puedan influir en la valoración del riesgo. Quedará exonerado de tal deber si el asegurador no le somete cuestionario o cuando, aun sometiéndoselo, se trate de circunstancias que puedan influir en la valoración del riesgo y que no estén comprendidas en él.

El asegurador podrá rescindir el contrato mediante declaración dirigida al tomador del seguro en el plazo de un mes, a contar del conocimiento de la reserva o inexactitud del tomador del seguro.

Corresponderán al asegurador, salvo que concurra dolo o culpa grave por su parte, las primas relativas al periiodo en curso en el momento que haga esta declaración.

Si el siniestro sobreviene antes de que el asegurador haga la declaración a la que se refiere el párrafo anterior, la prestación de eeste se reducirá proporcionalmente a la diferencia entre la prima convenida y la que se hubiese aplicado de haberse conocido la verdadera entidad del riesgo. Si medió dolo o culpa grave del tomador del seguro, quedará el asegurador liberado del pago de la prestación».

estos datos suelen revelar esas circunstancias[116], sobre todo en los seguros de salud y vida. Además, los artículos 11-13 de la misma ley suponen una habilitación legal suficiente para el tratamiento de datos pertenecientes a esta categoría, que pueden tanto una agravación como disminución del riesgo. Estas previsiones legales buscan mantener el equilibrio del contrato entre las partes, y otorgan una habilitación suficiente para que, con arreglo al artículo 7.3 de la LOPD, no sea necesario el consentimiento del afectado[117].

El contenido de los datos relativos a la salud tiene que ser estudiada desde dos ámbitos normativos[118]:

1. Desde la normativa de protección de datos

El RGPD los define en el artículo 4, apartado 15) 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».

Los datos relativos a la salud se definen en el artículo 5.1 g) del RLOPD como «las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética»[119].

Esta definición deriva de la dictada por el TJUE en el caso *Lindqvist*: «Teniendo en cuenta el objeto de la Directiva 95/46/CE, es preciso dar *una interpretación amplia a la expresión "datos relativos a la salud", empleada en su artículo 8, apartado 1, de modo que comprenderá*

---

[116] *Vid*. Informe AEPD 0452/2012.

[117] *Vid.* LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo,* Francis Lefebvre, Madrid, 2016, p. 111.

[118] *Vid*. BELTRÁN AGUIRRE, Juan Luis, «La protección de los datos personales relacionados con la salud», en *Jornada sobre Protección de Datos Personales,* Defensor del Pueblo de Navarra-INAP, Navarra, 2012, p. 12.

[119] El dato genético está definido en el artículo 3. j) de la Ley 14/2007, de Investigación Biomédica, como la información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos, como en el artículo 4. 13) RGPD: 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.

la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona».

De esa interpretación amplia hay que señalar que progresivamente se ha ido aumentando la amplitud del término, llegando a admitir a los datos genéticos y biométricos como datos sanitarios.

La definición del reglamento no se refiere solo a los datos relacionados directamente con la salud, sino que incluye datos sobre el estado de la salud, tal y como recoge el considerando 35[120]. Esto se debe a la propia delimitación del contenido por parte del CEPD sobre lo que entiende por «datos relacionados con la salud», que estaremos ante ellos cuando[121]:

1. Los datos son inherentemente / claramente datos médicos.

2. Los datos de sensores sin procesar, que pueden usarse en sí o en combinación con otros datos para derivar conclusión sobre el estado de salud actual o el riesgo para la salud de una persona.

3. Conclusiones sobre el estado de salud de una persona o riesgo para la salud (independientemente de si estas conclusiones son exactas o inexactas, legítimas o ilegítimas, o de otra manera adecuadas o inadecuadas).

---

[120] Considerando 35: 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*.

[121] *Health data in apps and devices*. Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

La inclusión de los datos psíquicos de una persona como datos relativos a la salud deriva de la doctrina que estableció la AEPD y la Audiencia Nacional[122,123].

El *Big Data* implica el uso de grandes cantidades de datos, por lo que es posible que el tratamiento de datos de salud suponga un tratamiento «a gran escala». Del considerando 91 podemos obtener el contenido de tal concepto, que se refiere al tratamiento de una cantidad considerable de datos personales en los ámbitos regional, nacional o supranacional, que podrían afectar a un gran número de interesados y que suponen un alto riesgo. El tratamiento de datos personales no debe considerarse «a gran escala» si lo realiza, respecto de datos personales de pacientes o clientes, una sola persona. Por lo tanto, deben cumplirse cuatro requisitos para que se considere un tratamiento a gran escala: 1) que los datos tratados se obtengan de fuentes regionales, nacionales o supranacionales; 2) que afecte a un gran número de personas; 3) que el riesgo se derive de la sensible categoría de los datos tratados, y 4) que los datos sean tratados por varias personas.

El tratamiento de datos relacionados con la salud a gran escala implica unas obligaciones adicionales por parte del RGPD:

a) Nombrar a un representante en el caso de responsables y encargados no establecidos en la Unión y sujetos al reglamento, independientemente de que el tratamiento sea ocasional (artículo 27.2.a) y considerando 80);

b) nombrar a un delegado de protección de datos (artículo 37);

c) llevar a cabo una evaluación de impacto relativa a la protección de datos (artículo 35.3.b), y

d) realizar una consulta previa a la autoridad de control de datos cuando no sea posible minimizar el riesgo y siga existiendo un alto riesgo ligado al tratamiento (artículo 36).

---

[122] SSAN, 12 de abril de 2002; 26 de septiembre de 2002 y 27 de abril de 2005; Resolución AEPD de 24 de enero de 2003.

[123] *Vid*. AGÚNDEZ LERÍA, Irene María, «Artículo 5. Definiciones», en ZABÍA DE LA MATA, Juan, *Protección de datos: comentarios al reglamento*, Lex Nova, Madrid, p. 116.

Es relevante destacar un componente clave a la hora de considerar los datos como «sanitarios»: los datos generados por algunas aplicaciones suelen tener un marcado componente estadístico y con la finalidad de informar al sujeto de su estado, pero esos datos pueden considerarse sanitarios cuando de la relación de dichos datos puedan extraerse consecuencias médicas[124]. Por eso, cualquier empresa que vaya a realizar valoraciones médicas a partir de datos generados por un sujeto debe saber que está tratando datos de salud que necesitan un consentimiento reforzado.

2. Desde la normativa sectorial

A estas definiciones, cabe sumarles el concepto de información clínica recogida 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 (LBAP), que se define en el artículo 3 como «todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla».

Prácticamente, se puede simplificar la definición a todo dato que haga referencia de forma directa o indirecta a la salud y se relacione con una persona concreta[125].

En el mismo sentido que los datos biométricos, la propia cláusula del artículo 9.4 RGPD es aplicable también a los datos relacionados con la salud.

III.2.3. Datos biométricos

Como hemos visto, los datos biométricos son usados fundamentalmente en los seguros de vida y salud para ofrecer un producto adecuado a sus necesidades en función del riesgo que muestran tales datos respecto del asegurado.

---

[124] Carta del CEPD, de 5 de febrero de 2015, sobre Health.

[125] Otros documentos de interés respecto a los datos relativos a la salud que podemos destacar son la memoria explicativa del Convenio 108 del Consejo de Europa, y la Recomendación del Consejo de Ministros n.º R (97) 5, sobre protección de datos médicos, del Consejo de Europa (13 de febrero de 1997).

Actualmente, los sistemas biométricos tienen una configuración simple y un precio asequible, por lo que *el mayor límite en su uso no es la tecnología, sino la ley*[126].

Para la explicación de estos datos, haremos referencia al «Documento de trabajo sobre biometría de 2003» y al «Dictamen 3/2012 sobre la evolución de las tecnologías biométricas».

Los datos biométricos son definidos por el Dictamen 4/2007 como «propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad».

Como observamos, la definición otorgada por el CEPD tiene un marcado componente pragmático, sin entrar en la creación de una definición doctrinal.

La AEPD los define como «aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.»[127].

El artículo 4, apartado 14) define los datos biométricos como «datos personales 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».

El Documento de trabajo sobre biometría de 2003 señala que ese dato puede ser:

- *universal:* el elemento biométrico existe en todas las personas;
- *único:* el elemento biométrico debe ser distintivo para cada persona;

---

[126] *Vid*. SOLER FUENSATA, Juan Ramón y GUASCH PORTAS, Vicente, «Identificación y autentificación de clientes en establecimientos hoteleros. La difícil combinación entre biometría y hotelería», en *Revista de Análisis Turístico*, Facultad de Trismo de la Universidad de Málaga, Málaga, n.º 16, 2013, p. 20.

[127] *Vid*. Informes AEPD de 28 de febrero de 2006, 7 de septiembre de 2007, 0324/2009, 0082/2010 y 0065/2015.

- *permanente:* la propiedad del elemento biométrico es permanente a lo largo del tiempo para cada persona.

El mismo documento nombra las fuentes de las cuales proceden tales datos dependiendo de la técnica utilizada:

a) *Técnicas basadas en aspectos físicos y fisiológicos,* que miden las características fisiológicas de una persona: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, pulsaciones, etc.

b) *Técnicas basadas en aspectos comportamentales,* que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, forma de caminar, de moverse, etc.

c) *Técnicas basadas en elementos psicológicos,* que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico.

El tratamiento de los datos biométricos consta de varios procesos:

1. *Registro:* es el proceso destinado a recabar los datos biométricos de una fuente y vincularlos a una persona. La cantidad de datos extraídos de una fuente biométrica durante la fase de registro ha de ser adecuada para los fines del tratamiento y el nivel de rendimiento del sistema biométrico.

2. *Almacenamiento:* los datos obtenidos durante el registro pueden almacenarse localmente en el centro de operaciones en el que haya tenido lugar el registro para su uso posterior, o en un dispositivo transportado por el individuo, o podrían ser enviados y almacenados en una base de datos centralizada accesible por uno o más sistemas biométricos.

3. *Correspondencia biométrica:* es el proceso de comparación de los datos capturados durante el registro con los datos o plantillas biométricas recogidos en una nueva muestra a efectos de identificación, verificación y autenticación o categorización.

Debido a su incidencia total en la protección de datos, debemos tener en cuenta que los datos biométricos se encuentran en la categoría de datos especiales del artículo 9 RGPD, por lo que su régimen es más estricto que el de otras categorías de datos.

1. *Propósito:* es necesaria una definición concreta de los fines para los que se usarán los datos biométricos. Como ejemplo aplicado a nuestro objeto de estudio, los datos biométricos se recaban con el fin de adaptar un seguro al riesgo que soporta el asegurado con base en los datos.

2. *Proporcionalidad:* los datos biométricos solo pueden utilizarse si son adecuados, pertinentes y no excesivos. Esto implica una evaluación estricta de la necesidad y la proporcionalidad de los datos tratados y de si la finalidad prevista podría alcanzarse de manera menos intrusiva. Al analizar la proporcionalidad del uso de un sistema biométrico, debemos valorar cuatro factores:

   a) si es esencial para satisfacer esa necesidad;
   b) la eficacia del sistema para responder a la necesidad según las características de este;
   c) si la pérdida de intimidad resultante es proporcional a los beneficios esperados;
   d) si no hay un medio menos lesivo que consiga el mismo resultado.

3. *Precisión:* los datos tratados deberán ser exactos y pertinentes en proporción a la finalidad para la que fueron recogidos, tanto en la recogida como en la vinculación con el individuo.

4. *Minimización de datos:* solo deberá tratarse, transmitirse o almacenarse la información necesaria, no toda la información disponible. El responsable del tratamiento deberá garantizar que la configuración por defecto promueva la protección de datos, sin tener que tomar medidas al efecto.

5. *Periodo de conservación:* el periodo de tenencia de los datos debe estar limitado, y no podrá ser superior al necesario para los fines por los que los datos fueron recabados.

El artículo 9.4 RGPD contiene una cláusula dispositiva para los Estados miembros que permite introducir nuevas condiciones o limitaciones en relación con esta categoría de datos, debido a la sensibilidad característica de dichos datos.

III.3. ANONIMIZACIÓN Y SEUDONIMIZACIÓN

Como señalamos anteriormente, las normas sobre protección de datos se aplican sobre datos considerados personales, por lo que si se rompe la relación entre el dato y el individuo en cuestión, no serán de aplicación dichas normas.

El *Big Data* cambia esta consideración, porque al aumentar la cantidad y diversidad de la información, aumenta el riesgo de reidentificación de los individuos. Incluso habiendo anonimizado los datos[128]. Por ello, es necesario analizar las soluciones que da la nueva normativa y el CEPD respecto a ello.

III.3.1. Anonimización

Muchos datos incluyen información privada con afecciones éticas o legales. Es un reto proporcionar una protección de la privacidad para datos sensibles usando la seguridad adecuada y la desinfección, anonimización y generalización de *Big Data,* dada la información personal cada vez más detallada unida a esta tecnología[129].

Para el estudio de este apartado, es de gran relevancia el «Dictamen 05/2014 sobre técnicas de anonimización» del CEPD, puesto que es uno de los pocos documentos que aborda los sistemas de anonimización desde una doble perspectiva jurídico-técnica.

No existe actualmente una definición legal de anonimización ni en la legislación europea ni en la española de protección de datos[130]. Lo más parecido a ello lo encontramos en el considerando 26 del RGPD: «*Los principios de la protección de datos deben*

---

[128] *Vid*. MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth, *op. cit.,* p. 35.

[129] *Vid. et al.* YANG, Chaowel, «Big Data and Cloud Computing: innovation opportunities and challenges», en *International Journal of Digital Earth*, vol. 10, n.º 1, Informa UK, 2017, p. 29.

[130] Sí lo encontramos, en cambio, en el artículo 3 de la Ley de Investigación Biomédica (LIBi); donde define: 1) la «anonimización» como proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere; 2) el «dato anónimo» como dato registrado sin un nexo con una persona identificada o identificable, y 3) «Dato anonimizado o irreversiblemente disociado» como dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados.

aplicarse a toda la información relativa a una persona física identificada o identificable [...] Para determinar si una persona física es identificable, *deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.* Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, *deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.* Por lo tanto, *los principios de protección de datos no deben aplicarse a la información anónima, es decir, información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos, de forma que el afectado no sea identificable, o deje de serlo. En consecuencia, el presente reglamento no afecta al tratamiento de dicha información anónima,* inclusive con fines estadísticos o de investigación».

Tanto la Directiva 2002/58/CE (artículo 6) como el reglamento que lo sustituirá (artículo 7)[131] reflejan la importancia de la anonimización de los datos en las comunicaciones electrónicas.

ROMERO CASABONA entiende por anonimización como «un proceso, es decir, el procedimiento de disociación de datos inicialmente identificados o identificables que desligue de forma definitiva unos y otros datos [...] El resultado de este proceso es que los datos tratados son anónimos»[132].

---

[131] «Artículo 7:

1. Sin perjuicio de lo dispuesto en el artículo 6, apartado 1, letra b), y en el artículo 6, apartado 3, letras a) y b), el proveedor del servicio de comunicaciones electrónicas suprimirá el contenido de las comunicaciones electrónicas o anonimizará esos datos una vez los hayan recibido el destinatario o destinatarios previstos. Tales datos podrán ser registrados o almacenados por los usuarios finales o por un tercero encargado por ellos de registrar, almacenar o tratar de cualquier otra forma los datos, de conformidad con el Reglamento (UE) 2016/679.
2. Sin perjuicio de lo dispuesto en el artículo 6, apartado 1, letra b), y en el artículo 6, apartado 2, letras a) y b), el proveedor del servicio de comunicaciones electrónicas suprimirá los metadatos de comunicaciones electrónicas o los anonimizará cuando ya no sean necesarios para transmitir una comunicación.
3. Cuando el tratamiento de metadatos de comunicaciones electrónicas se lleve a cabo a efectos de facturación de conformidad con el artículo 6, apartado 2, letra b), los metadatos correspondientes podrán conservarse hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse su pago con arreglo a la legislación nacional».

[132] *Vid*. ROMEO CASANOBA, Carlos María, *op. cit.,* p. 245.

Como el mismo autor señala, las expresiones «no identificable» y «anonimización» no significan que sea totalmente imposible la identificación del individuo. En este sentido, se incluyen las medidas «razonables» para identificar a la persona, excluyendo las medidas que impliquen «una cantidad de tiempo, gastos y trabajo desproporcionados»[133].

Podemos observar que el dictamen del CEPD cae en contradicciones al determinar el carácter absoluto del término «anonimización». Se destaca en la página 2 que la «anonimización» debe tener el mismo efecto que el borrado: «garantizar que es imposible tratar los datos personales»; sin embargo, en la siguiente página se niega a utilizar los términos «anonimato» o «datos anónimos» a favor de «técnicas de anonimización» para resaltar el riesgo de reidentificación que subyace después de cada proceso.

Por lo tanto, si se define que un dato anónimo es aquel por el cual no existe riesgo alguno de identificación, la anonimización solo sería posible en el papel, y sería imposible continuar con el flujo de datos actual debido a la siempre exigencia de consentimiento sobre todos los datos en circulación, con un grave efecto sobre el *Big Data*[134].

Por eso, es recomendable seguir el criterio marcado por el RGPD, en cuanto al «juicio de razonabilidad»[135] que otorga el considerando 26, y que ha sido admitida en el artículo 5.1 o) del RDLOPD.

La AEPD ha establecido los principios que deben regir el proceso de anonimización[136]:

1. *Principio proactivo:* se refiere a que la anonimización debe ser el primer objetivo y hacerse proactivamente, sin tender a garantizarla posteriormente debido a las brechas del proceso o perjuicios ocasionados. La AEPD prima el principio *privacy first,* consistente en establecer un nivel de privacidad predefinido, y crear modelos de privacidad para conseguirlo; al contrario del principio *utility first,* que busca la

---

[133] *Ibidem.*

[134] *Vid*. EL EMAM, Khaled y ÁLVAREZ, Cecilia, «A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques», en *International Data Privacy Law Journal*, vol. 5, n.º 1, Oxford University Press, Oxford, 2015, pp. 73-87.

[135] *Vid*. GIL GONZÁLEZ, Elena, *op. cit.,* p. 87.

[136] *Vid*. AEPD, Orientaciones y garantías en los procedimientos de anonimización de datos personales, AEPD, 2016, pp. 3-4.

anonimización de los datos manteniendo su utilidad, analizando el riesgo de identificación y tomando medidas en caso de que el riesgo sea alto.

Aunque parecen principios contrapuestos, son ponderables; puesto «que una mayor sofisticación en el uso de los datos anonimizados puede mejorar la utilidad de los datos, y por tanto mejorar la compensación entre privacidad-utilidad»[137]. En este principio, cabe destacar la importancia de la evaluación de impacto de datos personales que recoge el RGPD en el artículo 35.

2. *Privacidad por defecto:* consiste en tener siempre en cada sistema de información el objetivo de garantizar la privacidad. Este principio se encuentra recogido también en el artículo 25 del RGPD.

3. *Privacidad objetiva:* se basa en la absorción del riesgo por el responsable del riesgo mostrado en la evaluación de impacto, y se tomará en cuenta ese riesgo para el proceso de anonimización.

4. *Plena funcionalidad:* se tendrá en cuenta la utilidad final de los datos anonimizados, garantizando en la medida de lo posible la inexistencia de distorsión con relación a los datos no anonimizados. De esta forma, se garantizará la utilidad de los datos anonimizados, pero en casos especiales deberá añadirse elementos de distorsión para garantizar la privacidad de los individuos. En relación con el primer principio, vemos la ponderación de ambos, en el que el *utility first* tiene una importancia relativa en tanto en cuanto se establece la privacidad como objetivo.

5. *Privacidad en el ciclo de vida de la información:* las medidas que garantizan la privacidad de los afectados son aplicables durante el ciclo completo de la vida de la información al partir de la información sin anonimizar.

6. *Información y formación:* todo el personal interviniente en el proceso de anonimización debe estar informado y formado de sus obligaciones.

---

[137] *Vid*. LI, Tiancheng y LI, Ninghui, «On the Tradeoff Between Privacy and Utility in Data Publishing», en *CERIAS Tech Report 2009-2017*, Center for Education and Research Information Assurance and Security, Purdue University, West Lafayette (IN), 2009, p. 10.

El procedimiento de anonimización no debe ser excesivamente costoso. Debe estar organizado de tal manera que cualquier responsable de determinado ámbito profesional pueda supervisar, comprender y realizar. Al mismo tiempo, debe minimizar el riesgo de reidentificación[138].

La anonimización realizada se debe revisar periódicamente, además de evaluar los posibles nuevos riesgos que puedan surgir como consecuencia de diferentes factores. Las técnicas de anonimización deben preservar la utilidad de los datos en la medida de lo posible, sin perder de vista el impacto que puede tener la utilización de las mismas, especialmente en la elaboración de perfiles.

III.3.2. Seudonimización

Según el dictamen del CEPD, «consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro». Este término no se encontraba en la legislación anterior al RGPD, por lo que su creación es relativamente nueva.

El RGPD define la *seudonimización* en el artículo 4. 5) como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un afectado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».

La seudonimización se encuentra concretada en varios considerandos del RGPD, como podemos resaltar en el propio 26, cuando estipula que «los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable».

El considerando 28 dicta que «puede reducir los riesgos para los afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos».

---

[138] *Vid*. ALEXIN Zoltán, «Does fair anonymization exist?», en *International Review of Law, Computers & Technology*, vol. 18, n.º 1, Routledge, 2014, p. 23.

En nuestra legislación no encontramos su definición; encontramos su equivalencia en el artículo 5. k) de la Ley de Investigación Biomédica (LIBi) con el dato codificado o reversiblemente disociado: «dato no asociado a una persona identificada o identificable por haberse sustituido o desligado la información que identifica a esa persona utilizando un código que permita la operación inversa».

La diferencia con la anonimización se concreta en que un sujeto puede volver a ser identificable mediante un procedimiento reversible.

Como se ha dicho en este mismo apartado (y anteriormente en este trabajo), un dato seudonimizado no se considera anónimo y, por tanto, queda sujeto a las normas de protección de datos. La seudonimización es un procedimiento útil, pero no puede considerarse un método de anonimización debido a los riesgos de reidentificación[139].

Las técnicas más destacadas de seudonimización son:

1. *Cifrado con clave secreta:* el poseedor de la clave puede reidentificar al afectado con suma facilidad. Para ello, le basta con descifrar el conjunto de datos, ya que este contiene los datos personales, aunque sea en forma cifrada.

2. *Función hash:* se trata de una función matemática que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño. Esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Dentro de la función hash podemos encontrar diferentes variantes, como la función con clave almacenada, o el cifrado determinista.

3. *Descomposición en tokens (tokenización):* suele basarse en la aplicación de mecanismos de cifrado unidireccionales, o bien en la asignación, mediante una función de índice, de un número de secuencia o un número generado aleatoriamente que no derive matemáticamente de los datos originales.

---

[139] *Vid.* LOZOYA DE DIEGO, Abel; VILLALBA DE BENITO, María Teresa y ARIAS POU, María, «Análisis sobre la heterogeneidad en la legislación de protección de datos personales de carácter médico», en *Diario La Ley*, n.º 8688, La Ley, Madrid, p. 16.

III.3.3. Técnicas de anonimización

En el Dictamen 05/2014 se han propuesto una serie de medidas tendentes a conseguir este resultado mediante la reducción al mínimo de los problemas que genera la anonimización:

- *Singularización:* la posibilidad de extraer de un conjunto de datos algunos registros que identifican a una persona.

- *Vinculabilidad:* la capacidad de vincular como mínimo dos registros de un único afectado o de un grupo de afectados, ya sea en la misma base de datos o en dos bases de datos distintas.

- *Inferencia:* la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

III.3.3.1. Aleatorización

Constituyen el primer conjunto de técnicas que modifican la veracidad de los datos a fin de eliminar el estrecho vínculo existente entre los mismos y la persona. Si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta.

1. *Adición de ruido:* consiste en modificar los atributos del conjunto de datos para que sean menos exactos, conservando no obstante su distribución general.

    - *Singularización:* se pueden singularizar los registros de una persona, aunque sean menos fiables.

    - *Vinculabilidad:* se pueden vincular los registros de una misma persona, pero estos son menos fiables, por lo cual se puede vincular un registro real con uno añadido artificialmente.

    - *Inferencia:* se pueden llevar a cabo ataques por inferencia, pero la tasa de éxito será menor; además, no se descartan falsos positivos.

2. *Permutación:* consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos afectados.

    - *Singularización:* se pueden singularizar los registros de una persona, aunque sean menos fiables.

    - *Vinculabilidad:* es posible que impida una vinculación correcta si la permutación se aplica sobre los valores adecuados, pero también puede darse una vinculación incorrecta y asociar los datos a un afectado distinto.

    - *Inferencia:* aunque sea posible realizar inferencias, estas estarán basadas en hipótesis equivocadas y probabilidades.

3. *Privacidad diferencial:* es una de las nuevas técnicas de anonimización que utilizan las empresas tecnológicas, cuya base consiste en la adición de ruido, responsable del tratamiento de datos que genera vistas anonimizadas de un conjunto de datos, al mismo tiempo que conserva una copia de los datos originales. Estas vistas anonimizadas normalmente se generan mediante un subconjunto de consultas de un determinado tercero.

    - *Singularización:* si la salida está formada exclusivamente por datos estadísticos y las reglas que se aplican al conjunto se han escogido adecuadamente, no debería ser posible usar las respuestas para singularizar a una persona.

    - *Vinculabilidad:* si se lanzan varias consultas, es posible que se puedan vincular las entradas relativas a una persona determinada entre dos respuestas.

    - *Inferencia:* se puede inferir información sobre personas o grupos lanzando varias consultas.

III.3.3.2. Generalización

Constituyen el segundo conjunto de técnicas. Estas medidas generalizan o diluyen los atributos de los afectados modificando las respectivas escalas u órdenes de magnitud.

1. *Agregación y anonimato k:* tienen el objetivo de impedir que un afectado sea singularizado cuando se le agrupa junto con, al menos, un número *k* de personas.

    - *Singularización:* dado que ahora hay *k* usuarios que comparten los mismos atributos, ya no se puede singularizar a una persona entre un grupo de *k* usuarios.

    - *Vinculabilidad:* aunque la vinculabilidad es remota, aún se pueden vincular registros por grupos de *k* usuarios.

    - *Inferencia:* utilizando esta técnica, los datos quedarán desprotegidos frente a ataques de inferencia.

2. *Diversidad l, proximidad t:* la diversidad *l* extiende el anonimato *k* para garantizar que ya no se puedan realizar ataques por inferencia deterministas. Para ello, se asegura de que, en cada clase de equivalencia, todos los atributos tienen al menos *l* valores diferentes. La proximidad *t* es un perfeccionamiento de la diversidad *l*. Consiste en crear clases equivalentes que se parezcan a la distribución inicial de los atributos en la tabla.

    - *Singularización:* la diversidad *l* y la proximidad *t* garantizan que los registros relativos a una persona no se puedan singularizar en la base de datos.

    - *Vinculabilidad:* la diversidad *l* y la proximidad *t* no mejoran el anonimato *k* en lo que se refiere a la no vinculabilidad.

    - *Inferencia:* la principal mejora que ofrecen la diversidad *l* y la proximidad *t* con respecto al anonimato *k* es que ya no se pueden llevar a cabo ataques por inferencia contra una base de datos con diversidad *l* o proximidad *t* con un 100 % de confianza.

IV. TRATAMIENTO LEGAL DE LOS DATOS PERSONALES

Debemos partir de la definición de *tratamiento* realizada por el RGPD en el artículo 4. b), definido 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».

Esta definición debe tener una concepción finalista por el cual el tratamiento se refiere a utilización de datos personales de una base de datos o fichero, entendido este como un conjunto organizado de datos[140], con la consecuencia de que prácticamente cualquier actividad con datos personales quedará englobada en el concepto de *tratamiento*[141].

El concepto de tratamiento está directamente ligado al de dato personal; y ya que la mera recogida de datos considerados personales supone un «tratamiento», este acto supone causa suficiente para la aplicación de la normativa europea sobre protección de datos.

Cabe tener en cuenta el concepto de tratamiento *no automatizado* de datos personales, que aunque podamos afirmar que los tratamientos automatizados suponen los más comunes y los necesarios para hacer tratamientos relacionados para fines *Big Data,* los tratamientos no automatizados suponen graves riesgos por su cada vez menos uso y despreocupación en orden a la imposición de las sanciones.

Como concepto, debemos remitirnos al vigente artículo 5.1 n) donde define los ficheros no automatizados como «todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas,

---

[140] *Vid*. ERDOZÁIN LÓPEZ, José Carlos, «La protección de los datos de carácter personal en las telecomunicaciones», en *Revista Doctrinal Aranzadi Civil-Mercantil*, n.º 1, Aranzadi, Cizur Menor, 2007, p. 2.

[141] *Ibidem*, p. 3.

que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica».

Por ello, para considerar un tratamiento no automatizado, el criterio que la infomación en papel vaya destinada o pertenece a un fichero manual estructurado, un criterio, por ejemplo, es la organización en virtud de personas o por el Documento Nacional de Identidad; por eso los expedientes de bautizo no se consideran ficheros bajo el amparo de la LOPD al no estar estructurados de una forma que permita identificar a las personas[142].

IV.1. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

Debido a la globalización, la deslocalización, la variedad de opciones para el tratamiento de datos, *y la posibilidad de que un tratamiento realizado fuera del territorio de la Unión quede sujeto a la legislación europea*[143], conviene analizar el artículo 3 del RGPD para explicar los supuestos en los que el tratamiento de datos está sujeto al derecho de la Unión, cuyo alcance es mucho mayor por su extraterritorialidad (o *long-arm jurisdiction* en la doctrina anglosajona)[144], que la actual directiva[145], con el objetivo de evitar los problemas acaecidos por el intercambio de datos con Estados Unidos[146].

En comparación con la rúbrica estipulada en la Directiva 95/46/CE, que rezaba en su equivalente actual al complejo artículo 4 «Derecho nacional aplicable», el artículo 3 del RGPD adopta como rúbrica «Ámbito territorial», esto se debe a que el reglamento tiene

---

[142] SSTS, 19 de septiembre de 2008, 14 de octubre de 2008, octubre de 2008, 7 de noviembre de 2008, enero de 2009, febrero de 2009, 16 de febrero de 2009, 19 de febrero de 2009 y 26 de febrero de 2009.

[143] *Vid*. KUNER, Christopher, «The European Union and the Search for an International Data Protection Framework», en *Groningen Journal of International Law*, vol. 2, ed. 1, 2015, p. 61.

[144] *Vid.* MOEREL, Lokke, «The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?», en *International Data Privacy Law*, vol. 1, n.º 1, Oxford University Press, 2011, pp. 28-46.

[145] *Vid.* TAYLOR, Mistale, «Permissions and prohibitions in data protection jurisdiction», en *Brussels Privacy* Hub *working paper,* vol. 2, n.° 6, Universidad Libre de Bruselas, 2016, p. 13.

[146] *Vid.* SCHIEDERMAIR, Stephanie, «The new General Data Protection Regulation of the European Union-Will it widen the gap between Europe and the US?», en DÖRR, Dieter y WEAVER, Russell (eds.), *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries,* De Gruyter, Berlín, 2015, p. 76.

por objeto unificar la normativa en Europa, y reforzar el derecho fundamental a la protección de datos, más que concretar la ley del Estado miembro que se debe aplicar, salvo algún supuesto[147]. Por ello, las empresas se enfrentarán a un solo derecho paneuropeo de protección de datos, no a veintiocho; ignorando las posiciones que defienden que el nuevo RGPD puede provocar más diferencias entre los Estados miembros de las que existen a día de hoy por la remisión que prevé la norma a los Estados miembros para que legislen sobre determinados elementos dispositivos del RGPD, olvidando que, al ser un reglamento y no una directiva, la aplicación de esta nueva norma es directa para todos los Estados miembros[148].

El artículo 3 del RGPD se compone de tres supuestos que a continuación pasaremos a explicar a la luz del «Dictamen 8/2010 sobre el derecho aplicable», actualizado a 2015, y la doctrina establecida por el TJUE[149]. Como rasgo general, el artículo 3 presenta un doble criterio para determinar la aplicación de la normativa[150]: el principio de país de origen, que se centra en la ubicación geográfica del tratamiento y el uso de los datos, y 2) el principio de mercado, que se orienta hacia el mercado objetivo.

No nos centraremos en el supuesto del artículo 3.3 del RGPD en lo referido al tratamiento de datos realizados por responsables o encargados del tratamiento no establecidos en la Unión, pero que deba ser aplicable su derecho en virtud del derecho internacional público, puesto que no plantea problemas relevantes en relación con el objeto de estudio.

IV.1.1. En el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea

El artículo 3.1 estipula que se aplicará la legislación europea cuando ese tratamiento de datos se lleve a cabo «en el contexto de las actividades de un establecimiento del

---

[147] Como la determinación de la edad mínima del menor para otorgar su consentimiento (artículo 8 del RGPD).

[148] *Vid.* ALBERCHT, Jan Philipp, «How the GDPR Will Change the World», en *European Data Protection Law Review*, vol. 2, n.º 3, Lexxion, Berlín, 2016, pp. 287-289.

[149] SSTJUE *Google Spain*, C-131/12, *Weltimmo*, C-230/14 y *Amazon EU Sàri*, C-362/14.

[150] *Vid.* ZELL, Anne-Marie, «Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field», en *German Law Journal*, vol. 15, n.º 3, Washington & Lee University School of Law, Washington, 2014, p. 482.

responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no».

Así pues, cualquiera de esos actos realizados sobre los datos personales de cualquier individuo en el ámbito de la Unión se les aplicará la legislación europea.

En comparación con la directiva, es eliminada la restricción del responsable, ampliando también a los actos realizados por el encargado del tratamiento.

La cuestión más discutida por el TJUE ha sido la definición de *establecimiento.* Tanto la directiva en su considerando 19 como el RGPD en su considerando 22 describen que «un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto».

En este sentido, la STJUE *Weltimmo* busca establecer *un concepto flexible de establecimiento «que rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada.* Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento [...] *procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en ese otro Estado miembro, tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión*» (párrafo 29).

El TJUE establece un *criterio de ponderación sobre la base del tipo de prestación o actividad que la empresa ejerza u oferte en otro Estado miembro,* llegando a bastar un solo representante en otro Estado miembro si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios en la Unión[151].

En definitiva, que el concepto de *establecimiento* «se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable» (párrafo 31).

---

[151] *Vid*. DE MIGUEL ASENSIO, Pedro Alberto, «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia», en *La Ley Unión Europea*, La Ley, Madrid, n.º 31, 2015, p. 8.

Se utiliza esta concepción flexible de establecimiento para garantizar el derecho a la protección de datos, como reza el considerando 23 del RGPD.

A todo esto, el artículo 4. 16) del RGPD ha considerado en su definición el concepto de «establecimiento principal». *La inclusión de dicha definición aclara y delimita cuestiones altamente relevantes como la concreción de un establecimiento principal del responsable o de un encargado con varios establecimientos en la Unión mediante reglas marcadas por el principio de especialidad y jerarquía.*

1. En el supuesto de un responsable con varios establecimientos, *como norma general se considerará principal el establecimiento desde donde se lleve a cabo la administración central en la Unión. Pero como norma especial, si las decisiones sobre los fines y los medios del tratamiento se toman en otro establecimiento, y tiene el poder para hacerlas efectivas, se considerará como principal este último.*

2. En cuanto al supuesto de un encargado con varios establecimientos, se considerará principal el establecimiento *en el que se lleve a cabo la administración central en la Unión. Si careciera de ella, como norma supletoria, será el establecimiento del encargado en la Unión Europea en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado.*

Tal y como se acaba de decir, y como se dicta en reiteradas SSTJUE[152], *tal tratamiento debe llevarse a cabo «en el contexto de las actividades del establecimiento».* Para explicar tal concepto, debemos acudir al Dictamen 8/2010, que aporta una serie de elementos para valorar si ese tratamiento se desarrolla en tal contexto:

1. *Grado de implicación del establecimiento en las actividades en cuyo contexto se traten los datos personales.* Consiste en determinar qué actividades realiza cada establecimiento, y determinar que tales actividades comerciales están destinadas a cualquier Estado miembro de la Unión Europea[153].

---

[152] *Google Spain*, C-131/12 (pár. 52), *Weltimmo*, C-230/14 (pár. 35) y *Amazon EU Sàri*, C-362/14 (pár. 78).

[153] *Vid.* STJUE *Amazon EU Sàri* (pár. 76).

2. *Naturaleza de las actividades del establecimiento.* La cuestión de si una actividad entraña o no un tratamiento de datos y qué tratamiento se esté efectuando en el contexto de qué actividad depende en gran medida de la naturaleza de dichas actividades.

A todo esto, se le debe añadir la doctrina que estableció la STJUE en el caso *Google Spain,* que exige *confirmar que las actividades de un establecimiento local y las actividades de procesamiento de datos puedan estar inextricablemente vinculadas,* incluso si ese establecimiento no está asumiendo realmente ningún papel en el propio procesamiento de datos.

En resumen, *si el tratamiento de los datos se lleva a cabo por establecimientos no establecidos en la Unión, y el establecimiento en la Unión no interviene en dicho tratamiento, las actividades llevadas a cabo por ese establecimiento pueden, subsidiariamente, otorgar la protección que ofrece la legislación europea, siempre que exista esa «vinculación inextricable» entre las actividades del establecimiento en la Unión y el procesamiento de datos.* Por eso se ha incluido en el último inciso del artículo 3.1: *[I]ndependientemente de que el tratamiento tenga lugar en la Unión o no.*

La sentencia del caso *Google Spain* determinó que un establecimiento cuya actividad principal son los servicios publicitarios web mediante los motores de búsqueda puede ser suficiente como para que la legislación europea sea de aplicación, pero existen varias formas para en las que una empresa puede organizarse, sin tener que ser esta una de ellas. Cada caso es distinto, y se deben atener a los hechos del caso concreto. La sentencia no debe interpretar ni de forma totalmente expansiva, ni de forma restrictiva a las empresas con modelos de negocio relacionados con los motores de búsqueda.

CASO PRÁCTICO 3. Tratamiento de datos por establecimiento fuera de la UE y con establecimiento promocional

Una aseguradora se dedica a las ofertas de seguros con sede en Rusia. Para ello, utiliza medios electrónicos para recabar los datos y tratarlos.

A su vez, esta aseguradora cuenta con un establecimiento en Alemania dedicado a la promoción de su línea de negocio en Europa.

El establecimiento en Alemania no se dedica al tratamiento de datos, sino que cumple meras funciones propagandísticas.

Para determinar si los datos estarían sujetos a la normativa europea, es necesario determinar que las actividades que realiza el establecimiento en Alemania tienen una «vinculación inextricable» con las actividades que realiza la aseguradora. En este caso, podríamos establecer tal relación, ya que los servicios de publicidad favorecen el aumento de los ingresos de esa línea concreta de negocio. Por lo tanto, el tratamiento de esos datos está cubierto por el artículo 3.1 del RGPD.

IV.1.2. Actividades de tratamiento relacionadas con la oferta de bienes o servicios a afectados en la Unión Europea, independientemente de si a estos se les requiere su pago

Como apunte general al criterio de la situación del afectado del apartado 3.2 RGPD, facilita el sometimiento a la legislación europea de quienes no están establecidos en la Unión y tratan datos de individuos que se encuentran en ese territorio en circunstancias en las que se observa necesario aplicarlas[154]. Este criterio genera una mayor protección de los individuos al haber ampliado el alcance de la norma, sobre todo en lo que viene siendo la monitorización de su conducta[155].

---

[154] *Vid*. DE MIGUEL ASENSIO, Pedro Alberto, «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», en *Revista Española de Derecho Internacional*, vol. 69, n.º 1, Madrid, 2017, p. 14.

[155] *Vid*. HIJMANS, Hielke, *The European Union as Guardian of Internet Privacy: The Story of Artículo 16 TFEU*, Springer, Bruselas, p. 559.

El presente artículo ha de ponerse en relación con el artículo 27 y el considerando 80, los cuales obligan al responsable o encargado de nombrar a un representante establecido en la Unión en relación con las obligaciones que estipula el RGPD en el caso de que el tratamiento se refiera a afectados que se hallen en España, tal y como estipula el artículo 30 del Proyecto de LOPD de 2017.

Al estudiar el inciso a), debemos partir de la descripción que realiza el considerando 23, que determina que «si el responsable o encargado ofrece bienes o servicios a afectados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a afectados en uno o varios de los Estados miembros de la Unión *(targeting-based analysis)*»[156]. El considerando no contempla la accesibilidad web, el uso de un tercer idioma común o datos de contacto como indicios de oferta de servicios y productos en la Unión, como dicta la STJUE *Wertimmo*. Sí considera, por el contrario, el uso de la lengua, la moneda, o la mención de clientes o usuarios que residen en la Unión indicios de que el encargado o responsable dirige su oferta al territorio de la Unión.

Podemos considerar que, salvaguardando las distancias entre un caso y otro, sería de aplicación los criterios mostrados en la doctrina creada por la STJUE *Pammer y Hotel Alpenhof*[157], y consolidada en las SSTJUE *Mühlleitner*[158] y *Emrek*[159,160].

Uno de los criterios más relevantes de esa sentencia es tener en cuenta «todas las manifestaciones de voluntad de atraer a los consumidores de dicho Estado», como la oferta de tales servicios o productos en el Estado miembro, o la publicidad en distintos medios que facilitan su conocimiento por consumidores del Estado. La STJUE ha identificado un listado de indicios no exhaustivos, en los que se consideran como tal: *1) el carácter internacional de la actividad; 2) la indicación del prefijo internacional en los*

---

[156] *Vid.* GEIST, Michael, «Is There a There? Toward Greater Certainty for Internet Jurisdiction», *Berkeley Technology Law Journal*, vol. 16, n.º 3, California, 2001, pp. 1345-1406.

[157] STJUE C-585/08 *Pammer and Hotel Alpenhof;* ECLI:EU:C:2010:740.

[158] STJUE C-190/11 *Daniela Mühlleitner*; ECLI:EU:C:2012:542.

[159] STJUE C-218/12 *Emrek*; ECLI:EU:C:2013:494.

[160] El caso tratado en las SSTJUE citada no versa sobre protección de datos, sino de controversias en materia mercantil.

números de teléfono; 3) utilización de un nombre de dominio de primer nivel geográfico distinto al del Estado del vendedor; 4) descripción de un itinerario de envío desde un Estado miembro al lugar de la prestación del servicio; 5) la mención de una clientela internacional formada por clientes domiciliados en un Estado miembro, y 6) el empleo de lenguas o divisas que no se corresponden con las habituales en el Estado a partir del cual ejerce su actividad el empresario[161].

Pero podemos ver cumplidas las condiciones del artículo 3.2 a) RGPD cuando cualquier servicio o actividad es ofertada sin restricciones geográficas respecto de la UE, y son adquiridos por un número significativo de habitantes de la Unión[162].

Debemos reseñar la dicotomía literal entre la versión en inglés del reglamento con la versión en español. La versión inglesa exige que los afectados solo «estén» en la Unión Europea *(data subjects who are in the Union),* mientras que en la versión en español exige que los afectados «residan». Esto ha causado una disparidad de criterio entre artículos de escritura inglesa respecto a una posible interpretación amplia del artículo, haciendo que el RGPD pueda extralimitarse en su aplicación extraterritorial[163].

---

[161] La doctrina establecida por el TJUE deriva de la establecida por la *Supreme Court* estadounidense *Calder v. Jones* (465 U.S. 783 (1984)), en la que permite a los tribunales considerar si existe un mercado objetivo determinado mediante el uso de elementos como la lengua utilizada, la divisa o la nacionalidad. Aunque algún sector entiende que a esta doctrina se le puede achacar su fuerte componente subjetivo. *Vid*. JIMÉNEZ-BENÍTEZ, William Guillermo, «Rules for offline and online in determining Internet jurisdiction. Global overview and colombian cases», en *Revista Colombiana de Derecho Internacional*, n.° 26, Bogotá (Colombia), 2015, p. 30.

[162] *Vid*. DE MIGUEL ASENSIO, Pedro Alberto, «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *op. cit.,* nota 79, p. 16.

[163] *Vid.* BRKAN, Maja, «Data protection and conflict-of-laws: a challenging relationship», en *European Data Protection Law Review*, vol. 2, n.º 3, 2016, p. 337. SVANTESSON, Dan Jerker, *Extraterritoriality in Data Privacy Law*, Ex tuto Publishing, Copenhague, 2013, p. 107. Los autores discuten sobre la incoherencia del artículo 3.2 a) respecto al resto del RGPD, al afirmar que el artículo debe exigir la residencia.

CASO PRÁCTICO 4. Ofertas de pólizas de seguro por empresa externa a la Unión

Una aseguradora se dedica a las ofertas de seguros con sede en la India. Para ello, utiliza plataformas de Internet para ofertarlos.

La página web de la aseguradora está disponible en idiomas singulares de la Unión Europea como alemán, inglés, italiano, austriaco y español; aparte dispone de sistemas de cambio de divisas a euros, dólares estadounidenses y pesos argentinos.

Para determinar si los datos estarían sujetos a la normativa europea, es necesario observar los indicios que muestra la aseguradora en relación con la oferta de servicios a los habitantes de la Unión. Como observamos, la mayoría de idiomas mostrados son de uso casi exclusivo por los habitantes de los Estados miembros, pero el español y el inglés son idiomas de uso global, por lo que de estos dos últimos no cabe considerarlos como indicios. En cuanto a las divisas, observamos que una de las permitidas es el euro, por lo que hace una referencia directa al mercado de la Unión. Por lo tanto, el tratamiento de los datos derivados de tal actividad estará cubierto por el artículo 3.2 a) del RGPD.

IV.1.3. Actividades de tratamiento relacionadas con el control de su comportamiento, en la medida en que este tenga lugar en la Unión Europea

El artículo 3.2 b) del RGPD será de aplicación cuando el tratamiento de los datos de los afectados verse sobre la observación del comportamiento, en la medida en que este tenga lugar en la Unión y si el responsable o encargado no estuviera establecido en la Unión. Mientras la doctrina tiene asumida que este supuesto está destinado solamente al uso de archivos o programas informáticos que almacenan y permiten acceso al dispositivo de usuario *(cookies),* y excluye por tanto el ofrecimiento de productos o servicios[164]. *Considero que este artículo puede incluirse directamente en los productos ofertados mediante el uso del* Big Data *que, al fin y al cabo, no hace más que monitorizar el comportamiento del ser humano.*

---

[164] *Vid*. ALBRECHT, Jan Phillipp y JOTZO, Florian, *Das neue Datenschutzrecht der EU*, Baden-Baden, Nomos, 2017, p. 67; ERNST, Stefan, «Artículo 3», en PAAL, Boris y PAULY, Daniel (coords.), *Datenschutz-Grundverordnung,* C.H. Beck, Múnich, 2017, pp. 25-26, y DE MIGUEL ASENSIO, Pedro Alberto, *op. cit.,* p. 16.

Si entendemos el comportamiento como el conjunto de actos realizados por el ser humano producido por la interacción con el entorno en el que vive, algunas de las categorías de datos tratados por el *Big Data* revelan dichos actos[165].

El presente artículo hay que ponerlo en relación con el considerando 24, que determina que se entenderá como un control de comportamiento el seguimiento del afectado en Internet, pero a continuación estipula una referencia que resume a la perfección el objeto y la esencia del *Big Data*: «[I]nclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes».

Por las razones anteriores, *consideramos que el artículo 3.2 b) del RGPD es aplicable no solo a la motorización de los comportamientos mostrados en Internet, sino también a cualquier motorización realizada por cualquier medio destinado para ello.*

CASO PRÁCTICO 5. Uso de aplicaciones deportivas

Una aseguradora se dedica a las ofertas de seguros con sede en Estados Unidos. Para ello, utiliza plataformas de Internet para ofertarlos, sin ninguna mención concreta al mercado europeo.

La empresa pretende sacar un nuevo producto consistente en la adecuación de la póliza de un seguro de vida en función del riesgo real demostrado por el asegurado mediante el uso de una aplicación de la aseguradora que permite la medición de datos como la actividad física, la actividad nocturna y las rutas que puede seguir el individuo para, por ejemplo, salir a correr.

Estos datos revelan el comportamiento concreto de un individuo ante algunas acciones (por ejemplo, al ir a dormir), y de tales comportamientos puede emitirse una determinada acción, como el incremento o disminución del precio de la póliza. Por lo tanto, el tratamiento de los datos derivados de tal actividad estará cubierto por el artículo 3.2 b) del RGPD.

[165] P. ej., la ubicación de los individuos, los hábitos diarios relacionados con las horas de sueño o la actividad deportiva.

IV.2. CONSENTIMIENTO

El consentimiento del afectado es, por tanto, el elemento definidor del sistema de protección de datos de carácter personal. La LOPD establece el principio general de que el tratamiento de los datos personales solamente será posible con el consentimiento de sus titulares, salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento (STC 39/2016). En el RGPD se consagra el consentimiento como medio estrella para la licitud del tratamiento de datos personales, puesto que lo consagra en el artículo 6.1 a), dedica todo el artículo 7 a su desarrollo, y es una de las excepciones al tratamiento de las categorías especiales de datos del 9.1, y de las excepciones a la posibilidad de efectuar una transferencia internacional de datos a terceros países según el artículo 48.1 a).

Aunque sea la medida más importante, no es ni mucho menos la más sólida para legitimar el tratamiento de los datos. Como dice el CEPD en el Dictamen 15/2011 sobre la definición de consentimiento: «Algunas veces el consentimiento constituye una débil base para justificar el tratamiento de datos personales y pierde valor si se amplía o ajusta para adaptarlo a situaciones en las que nunca debería utilizarse».

El consentimiento permite al afectado ejercer el control sobre sus datos personales, puesto que es el propio afectado quien tiene que otorgar su consentimiento para que se pueda realizar el tratamiento de los datos[166], ya lo sostenía la STC 292/2000.

La reforma ocasionada por el RGPD ha llevado cambios en el consentimiento al haber eliminado, en un primer momento, la posibilidad de la validez del consentimiento tácito, modificación que estudiaremos a continuación.

Cabe resaltar la posición recogida en el considerando 171, que estipula que *se deberá renovar el consentimiento en los casos en los que no se haya otorgado en las condiciones que marca el RGPD,* como el haber otorgado el consentimiento de manera explícita. Por lo tanto, podemos encontrarnos ante tres diferentes situaciones:

---

[166] *Vid*. LESMES SERRANO, Carlos (coord.); BUISÁN GARCÍA, Nieves; FERNÁNDEZ GARCÍA, José Arturo; GUERRERO ZAPLANA, José; y SANZ CALVO, Lourdes, *La ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008, p. 190.

- Tratamientos de datos iniciados antes del 25 de mayo y que cumple con los requisitos del RGPD: no será necesario renovar el consentimiento si el tratamiento está destinado a los mismos fines que consintió en un primer momento. Solo sería necesario informar al afectado del cambio de la nueva normativa.

- Tratamientos de datos iniciados antes del 25 de mayo y que cumple con los requisitos del RGPD: será necesario renovar el consentimiento si los datos van a ser tratados para fines distintos a los que se consintió inicialmente, además de informar sobre la nueva normativa.

- Tratamientos de datos iniciados antes del 25 de mayo, pero que no cumple con los requisitos del RGPD (como el tratamiento basado en el consentimiento tácito): se debe renovar el consentimiento basándose en los nuevos criterios del RGPD.

Este consentimiento se caracteriza por las siguientes condiciones[167]:

1. *Causa.* Establece la posibilidad de otorgar el consentimiento en cualquier momento mediante un acto o declaración de voluntad.

2. *Irretroactividad.* La retirada del consentimiento no afectará a la licitud del tratamiento basado en el consentimiento previo a su retirada.

3. *Facilidad.* El consentimiento será tan fácil otorgarlo como retirarlo.

4. *Gratuidad.* El RGPD establece que el consentimiento podrá retirarse de un modo sencillo y gratuito, que no implique un ingreso para el responsable.

5. *Información.* La información debe consistir en la revocación del consentimiento en cualquier momento y su irretroactividad, además de los medios para poder hacerlo.

---

[167] ADSUARA VARELA, Borja, «El consentimiento», en PINAR MAÑAS, José Luis (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Editorial Reus, Madrid, 2016, pp. 161-162.

Es reseñable que el Proyecto de LOPD de 2017 en su artículo 9.1 ha establecido la prohibición de utilizar el mero consentimiento como base legitimadora del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, y que obtengan resultados discriminatorios, por lo que será necesaria otra base legitimadora adicional para posibilitar el tratamiento de los datos personales. Además, el artículo 9.2 permite 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.

IV.2.1. Definición. Elementos básicos

El RGPD define el consentimiento en el artículo 4. 11) como «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el afectado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen», en el mismo sentido que el artículo 6 del Proyecto de LOPD de 2017. A partir de esta definición, conviene explicar sus elementos centrándonos en las explicaciones que ofrece el dictamen anteriormente nombrado.

Como se ha dicho anteriormente, el consentimiento es:

1. *Toda manifestación de voluntad.* Al dejar este apartado en la ambigüedad, se permite cualquier forma de manifestación de la voluntad. Ni en la directiva en su momento ni en el RGPD aparece que el consentimiento tenga que ser «escrito». Esto se debe a razones de flexibilidad, ya que si se exigiera la necesidad de ser escrito, ralentizaría el flujo de datos existente en el mercado digital, por lo que deja abierta una interpretación amplia del concepto.

   Se presentan dudas en cuanto a la posibilidad de admitir el consentimiento tácito. La posición adoptada por la Audiencia Nacional establece límites a la posibilidad de legitimar un tratamiento de datos mediante un consentimiento tácito, ya que con ello no se demuestra que el consentimiento recibido fuera «inequívoco»[168], sin

[168] SSAN, 20 de septiembre de 2006 y 7 de marzo de 2007.

eliminar esta posibilidad[169]. Esta postura ha sido rechazada por el nuevo texto del RGPD, que estipula que para otorgar el consentimiento debe hacerse *mediante una declaración o una clara acción afirmativa*.

2. *Libre.* El consentimiento solo puede ser válido si el afectado puede escoger una opción y no existe riesgo de engaño, intimidación, coerción, o consecuencias negativas por su no consentimiento. El considerando 42 establece que «cuando el afectado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno». La AEPD viene sosteniendo que el consentimiento libre es aquel en el que no intervienen los vicios del consentimiento recogidos por el Código Civil[170]. Por ejemplo, el haber otorgado el consentimiento mediante una orden, este deja de ser «libre»[171].

   El CEPD define el consentimiento libre como «una decisión voluntaria, de un individuo en posesión de todas sus facultades, tomada sin ningún tipo de coacción, ya sea social, financiera, psicológica u otra»[172].

   El artículo 7.4 toma como indicativo sobre el consentimiento libre el hecho de si la ejecución del contrato se supedita al tratamiento de datos personales no necesarios para la ejecución del fin. Sirve como interpretación el criterio otorgado por el considerando 43 por el cual determina que no es motivo válido el consentimiento libre cuando «exista un desequilibrio claro entre el afectado y el responsable del tratamiento [...] Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento». En este sentido, cabe citar la STS 259/2014 (fundamento jurídico 3.º), en la que se señaló que aquellos datos que no fueran en absoluto necesarios e imprescindibles para el

---

[169] SAN, 20 de septiembre de 2013.

[170] *Vid.* Informes AEPD 0645/2009, 0039/2010, y 0108/2010, entre otros.

[171] STS –Sala de lo Militar–, 6 de febrero de 2015.

[172] *Vid.* «Dictamen 15/2011 sobre la definición de consentimiento», p. 14, y «Dictamen sobre los registros sanitarios electrónicos», p. 9.

mantenimiento y cumplimiento del contrato de trabajo, no pueden verse amparados por la excepción a la obligación de recabar el consentimiento.

Las directrices respecto al consentimiento del RGPD divide este criterio en otros elementos para determinar si el consentimiento se otorga libremente:

- *Desequilibrio entre las partes del tratamiento:* el consentimiento no será válido si existe dicho desequilibrio, lo que ocurre cuando el «responsable sea una autoridad pública y sea, por lo tanto, improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular». Tampoco sería una condición adecuada de legitimación del tratamiento en la relación laboral, ya que ante el temor de un riesgo real de perjuicio que pudiera tener su negativa a proporcionar su consentimiento, daría un consentimiento viciado. Aunque sí pueden darse casos en los que el empleador puede demostrar un consentimiento libre.

- *Condicionalidad:* se produce alguna situación en la que el consentimiento esté «agrupado» con la aceptación de términos y condiciones o «atado» a la provisión de un contrato o un servicio cuando los datos personales solicitados no son necesarios para el cumplimiento del contrato o la prestación de servicio. Se busca que el consentimiento no sea la contraprestación en el contrato.

- *Granularidad:* debe darse el consentimiento para los diferentes tratamientos realizados por separado. No se enterará dado libremente cuando no se ha podido autorizar por separado los diferentes fines.

- *Perjuicio:* existencia de retirar el consentimiento sin que el afectado sufra un perjuicio.

3. *Específica*. El consentimiento indiscriminado sin especificar la finalidad exacta del tratamiento no es admisible. El consentimiento debe ser comprensible; es decir, debe referirse de manera clara y precisa al alcance y las consecuencias del tratamiento de datos. No puede referirse a un conjunto indefinido de actividades de tratamiento. Por eso el consentimiento debe otorgarse en un contexto limitado.

   Uno de los principios que debe regir el tratamiento de los datos es la recogida con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con dichos fines de forma ulterior (artículo 5.1 b).

El Dictamen 03/2013 sobre limitación de finalidad viene a explicar los conceptos de este principio:

a) *Fines determinados:* el responsable debe determinar cuidadosamente los fines para los que vayan a ser destinados los datos personales y qué tipos de datos recabar. Para asegurarse si la recolección de datos cumple con la ley, es necesario identificar «ex ante» el o los propósitos. El fin o los fines de la recolección debe estar claro y específicamente identificado: debe ser suficientemente detallado para determinar qué tipo de procesamiento está y no está incluido dentro del propósito especificado. Los responsables del tratamiento deben evitar utilizar un propósito «paraguas» para incluir fines relacionados sin nombrarlos. Estos fines deben estar también explicados de forma separada.

b) *Fines explícitos:* deben ser claramente revelados, explicados o expresados de alguna forma inteligible. De lo anterior se deduce que esto debería suceder no más tarde del momento en que se produce la recogida de datos personales. La especificación de los objetivos debe expresarse, en particular, de tal manera que el responsable y los terceros encargados, así como las autoridades encargadas de la protección de datos, así lo entiendan de la misma manera que los afectados.

c) *Fines legítimos:* la legitimidad es un requisito amplio. Para que los fines sean legítimos, el procesamiento debe basarse, en todas las etapas y en todo momento, en al menos uno de los fundamentos jurídicos previstos en el artículo 6; pero la amplitud no se limita a los fundamentos que otorga este artículo. Para que el tratamiento sea legítimo deben cumplirse los principios relativos al tratamiento que dicta el artículo 5 y todos los requisitos que pueda marcar la ley, ya que si para conseguir tal fin es necesario saltarse la ley, ese fin no será legítimo.

Debemos destacar el artículo 6.2 del Proyecto del LOPD en el que estipula que cuando se funda el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste claramente dicho consentimiento para cada una de ellas.

4. *Informada.* El deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de

la necesidad de consentimiento del afectado. El deber de información sobre el uso y destino de los datos personales que exige la Ley Orgánica de Protección de Datos de carácter personal está íntimamente vinculado con el principio general de consentimiento para el tratamiento de los datos, pues si no se conoce su finalidad y destinatarios, difícilmente puede prestarse el consentimiento. Por ello, a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta, dada la estrecha vinculación entre el deber de información y el principio general de consentimiento (STC 39/2016). El consentimiento debe estar informado. Esto implica que toda la información necesaria debe suministrarse en el momento en que se solicita el consentimiento, de forma clara y comprensible, y debe abarcar todas las cuestiones pertinentes[173]. La AEPD se ha referido a este criterio en el sentido de que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce[174], además de considerar al derecho de información como contenido fundamental del derecho a la protección de datos[175]. Con esta matización el legislador ha querido destacar la necesidad de que para que se haga realidad el principio del consentimiento debe venir este precedido del de información a que se refieren los artículos 13, 14, y 7.3 RGPD, aunque puede entenderse que puede llegar a ser redundante,

---

[173] *Vid*. GIL GONZÁLEZ, Elena, *op. cit.,* p. 67.

[174] *Vid*. Informe AEPD 0081/2009.

[175] «El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele». *Vid*. Informe AEPD 02257/2010.

puesto que para tomar una decisión libre ha de tenerse la suficiente información que permita deliberar la opción. Sin la información que produce el conocimiento no puede existir auténtica libertad de decisión[176], por lo que la información constituye una circunstancia intrínseca al consentimiento[177]. El considerando 42 señala que para que el consentimiento otorgado por el afectado sea un consentimiento informado debe contener como mínimo la identidad del responsable del tratamiento y la finalidad del tratamiento. Tanto el CEPD como el TJUE[178] han determinado que esta característica estará cumplida si se ratifican dos requisitos:

I. *Calidad de la información.* La manera en que se presenta la información debe ser clara, comprensible, y ser lo menos técnica posible. La forma en la que se suministra la información variará dependiendo del contexto, pero nunca deben menoscabarse los principios de licitud y transparencia del artículo 5 del RGPD[179]. El artículo 11 del Proyecto de LOPD estipula como información mínima que debe ser otorgada al afectado:

   a) La identidad del responsable del tratamiento o de su representante, en su caso.

   b) La finalidad del tratamiento.

   c) El modo en que el afectado podrá ejercitar los derechos.

II. *Accesibilidad y visibilidad de la información.* La información debe comunicarse directamente a las personas. No basta con que la información esté «disponible» en algún lugar. La información debe ser claramente visible (tipo y tamaño de los caracteres), destacada y completa.

---

[176] *Vid*. FERNÁNDEZ LÓPEZ, Juan Manuel, «Principios de la protección de datos: consentimiento del afectado. Principio de consentimiento», en RONCOSO REIGADA, Antonio (dir.), *op. cit.,* p. 465.

[177] *Vid.* REBOLLO DELGADO, Lucrecio y SERRANO PÉREZ, María Mercedes, *Manual de protección de datos,* Dykinson, Madrid, 2014, p. 120.

[178] STJUE (Gran Sala) de 5 de octubre de 2004, *Pfeiffer Roith, Suß, Winter, Nestvogel, Zeller, Döbele*, en los asuntos acumulados C-397/01 a C-403/01.

[179] *Vid.* SERRANO CHAMORRO, María Eugenia, «Protección de datos personales: información…», *op. cit.,* p. 9.

El artículo 7.2 contempla otro criterio que viene a aclarar cuándo se puede considerar que el consentimiento es informado. En el marco de una declaración escrita en el que concurren varios asuntos, la solicitud del consentimiento deberá ir separada de tales asuntos y estar escrita en un lenguaje sencillo. Si este requisito no se cumple, no será vinculante. En cuanto a la posible efectividad de este requisito, puede darse la «paradoja de la transparencia»[180]: si se optan por criterios de simplicidad y claridad, se perderá precisión. Los textos escritos con un lenguaje sencillo no permiten otorgar toda la información posible al afectado; por ende, el consentimiento otorgado no será «informado».

5. *Inequívoca.* Para que el consentimiento se otorgue de forma inequívoca, el procedimiento de su obtención y otorgamiento no tiene que dejar ninguna duda sobre la intención del afectado al dar su consentimiento. El carácter «inequívoco» está íntimamente relacionado con la «manifestación de voluntad», puesto que, como discutimos anteriormente, se debatía por la posibilidad de considerar el consentimiento tácito como forma válida para otorgarlo; pero esta modalidad no despejaba las dudas en cuanto a la intención del afectado[181]. Como hemos visto, la Audiencia Nacional admitía esta modalidad con la máxima cautela, aunque la doctrina lo admitía también de una forma más flexible[182]; pero el RGPD viene a reforzar el concepto de «acción», al exigir una en carácter afirmativo para su consentimiento, por lo que ya no cabe la opción de otorgar el consentimiento de forma tácita. Como se dice en el considerando 32, «el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento».

6. *Mediante una declaración o clara acción afirmativa.* Es el inciso que ha introducido el RGPD. Con ello, pretende eliminar las dudas interpretativas respecto a la modalidad de consentimiento otorgado[183], como hace el Proyecto de LOPD en su exposición de

---

[180] *Vid*. BAROCCAS, Solon y NISSEBAUM, Helen, «Chapter 2: Big data's End Run Around Anonimity and Consent», en *Privacy, big data and the public good*, Cambridge University Press, 2014, p. 14; y GIL GONZÁLEZ, Elena, *op. cit.,* p. 71.

[181] *Vid*. GIL GONZÁLEZ, Elena, *op. cit.,* p. 68.

[182] *Vid*. MARTÍNEZ ROJAS, Ángela, «Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea», *Revista Aranzadi de Derecho y Nuevas Tecnologías,* n.º 42, Aranzadi, Cizur Menor, 2016, p. 6; LESMES SERRANO, Carlos (coord.); BUISÁN GARCÍA, Nieves; FERNÁNDEZ GARCÍA, José Arturo; GUERRERO ZAPLANA, José, y SANZ CALVO, Lourdes, *op. cit.,* pp. 194-196.

[183] *Vid*. MARTÍNEZ ROJAS, Ángela, «Principales aspectos...», *op. cit.,* p. 4.

motivos IV, aunque es posible que no lo haya logrado[184]. El RGPD ofrece dos alternativas para otorgar el consentimiento:

a) *Declaración.* Según la RAE, una *declaración* es «una manifestación del ánimo o de la intención», o «una manifestación formal que realiza una persona con efectos jurídicos»[185]. Por lo tanto, una manifestación y una declaración son sinónimos.

b) *Clara acción afirmativa.* Esta submodalidad lleva consigo la realización de una conducta afirmativa en tal sentido, es por esta modalidad por la que se elimina la posibilidad de otorgar el consentimiento tácito.

Pero la definición que otorga el reglamento no es lo suficientemente contundente como para eliminar cualquier duda respecto a la posibilidad de admitir el consentimiento tácito por los siguientes motivos:

a) En la definición se propone que se pueda otorgar *«ya sea» mediante una declaración o una clara acción afirmativa.* El uso de este nexo puede interpretarse tanto en el sentido de que los medios enunciados con posterioridad sean dictados de manera enunciativa, dando la posibilidad de admitir otros recursos para plasmar el consentimiento. Para haber evitado esta confusión, pudieron haber utilizado palabras con un marcado componente imperativo como «necesariamente».

b) El considerando 50 no aclara si es necesario el consentimiento del afectado cuando vaya a realizarse un tratamiento ulterior de los datos. Cuando nos referimos a un tratamiento ulterior, lo hacemos en el sentido de realizar un tratamiento con fines diferentes a los que se dedicaron cuando se recabaron. El considerando dicta que cuando el tratamiento esté destinado a otros fines, el afectado deberá estar «particularmente» informado para ejercer su derecho de oposición. En ningún momento se estipula que uno de los requisitos fundamentales sea el consentimiento «explícito»; de hecho, tal base jurídica está excluida

---

[184] *Vid*. DEL PESO RUIZ, Mar, «¿Consentimiento tácito con el Reglamento Europeo de Protección de Datos?», IEE - Informáticos Europeos Expertos, s/f. Disponible en: http://www.iee.es/pages/opinion/ventana.html.

[185] *Vid. Diccionario de la Real Academia Española (RAE).* Disponible en: http://dle.rae.es/?id=BxamUxw.

de los supuestos del 6.4 para realizar un tratamiento con fines distintos a los que se recogieron cuando no se hubiera basado en el consentimiento.

En definitiva, *a partir de la aplicación del RGPD, y de la futura LOPD, el consentimiento tendrá que ser explícito (tal y como dice el reglamento), siendo mediante una declaración la norma general a seguir para obtenerlo*[186].

Otra opción que recoge el RGPD para legitimar el tratamiento en determinadas fases del procesamiento del *Big Data* es el uso de algoritmos para descubrir correlaciones y patrones de contenido, y que muchas veces este tratamiento no es necesario para desempeñar el contrato por el cual legitima el tratamiento, por lo que una nueva base que puede legitimar el tratamiento es el conocido interés legítimo, que para aplicarlo hay que hacer una ponderación entre los intereses del responsable y la afectación al derecho fundamental.

IV.2.2. Prueba del consentimiento

El artículo 7.1 del RGPD consagra que la carga de la prueba del consentimiento obtenido recaerá sobre el responsable. No solo la ley lo ha determinado, anteriormente también la Audiencia Nacional justifica este criterio argumentando que el responsable es la persona que solicita el consentimiento[187]. La Audiencia Nacional extendió *la obligación de recabar el consentimiento a todos aquellos que traten datos personales*[188], *por lo que extiende la obligación de probar el consentimiento a todos aquellos que traten datos personales*[189].

Puesto que el RGPD ha restringido fuertemente el consentimiento tácito como medio para otorgar el consentimiento, se facilita de alguna forma la prueba de su obtención,

---

[186] *Vid*. GARCÍA NOBLIA, Analore, «¿Realmente cambiará el consentimiento el Reglamento Europeo?», en *Noticias Jurídicas*. Disponible en: http://www.abogacia.es/2016/11/15/realmente-cambiara-el-consentimiento-el-reglamento-europeo/.

[187] SSAN, 25 de octubre de 2002, 30 de junio de 2004.

[188] SAN, 10 de noviembre de 2003.

[189] SSAN, 25 de octubre de 2005 y 1 de febrero de 2006.

por lo que al solicitarlo de forma explícita, se reducen los problemas, pero no quita la obligación de demostrar que ese consentimiento fue *libre, específico, informado, inequívoco y mediante una declaración o una clara acción afirmativa*.

Debido a esta obligación, será necesario revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría[190].

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	**Contenido**
Responsabilidad activa (artículo 5.2)	El responsable debe aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD. Analizar qué datos tratan, con qué calidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, han de poder establecer qué medidas deben aplicar y cómo deben hacerlo. Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como: • Nombre y datos de contacto del responsable o corresponsable y del delegado de protección de datos si existiese. • Finalidades del tratamiento. • Descripción de categorías de interesados y categorías de datos personales tratados. • Transferencias internacionales de datos... Están exentas las organizaciones que empleen a menos de 250 trabajadores, a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados.
Licitud del tratamiento (artículo 6)	El tratamiento de datos debe hacerse bajo alguna de las siguientes bases: a) Consentimiento; b) Relación contractual; c) Intereses vitales del interesado o de otras personas; d) Obligación legal para el responsable; e) Interés público o ejercicio de poderes públicos; f) Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.

(cont.)

[190] *Vid.* SERRANO CHAMORRO, María Eugenia, «Protección de datos personales..., *op. cit.*, p. 15.

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	Contenido
Consentimiento (artículo 7)	Debe ser inequívoco libre, específico, informado y prestarse mediante una manifestación del interesado o mediante una clara acción afirmativa. Los tratamientos iniciados con anterioridad al inicio de la aplicación del RGPD sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa. Debe ser explícito en caso de: a) tratamiento de datos sensibles; b) adopción de decisiones automatizadas; c) transferencias internacionales.
Información (artículos 12 y 13)	La información a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Se deberán evitar las fórmulas especialmente farragosas y que incorporan remisiones a los textos legales. Las cláusulas informativas deberán explicar el contenido al que inmediatamente se refieren de forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia. Se establece una lista exhaustiva de la información que debe proporcionarse a los afectados y que añade: a) base jurídica del tratamiento; b) intención de realizar transferencias internacionales; c) datos del delegado de protección de datos (si lo hubiere); d) elaboración de perfiles. La información a los interesados deberá facilitarse por escrito, incluidos los medios electrónicos cuando sea apropiado.
Derechos (artículos 15-22)	Los responsables deben facilitar a los interesados el ejercicio de sus derechos, y los procedimientos y las formas para ello deben ser visibles, accesibles y sencillos. Los responsables posibilitarán la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se realiza por estos medios. El ejercicio de los derechos será gratuito para el interesado, excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas. El responsable podrá cobrar un canon que compense los costes administrativos de atender a la petición o negarse a actuar. El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (podrá extenderse dos meses más cuando se trate de solicitudes especialmente complejas y deberá notificar esta ampliación dentro del primer mes). Si el responsable decide no atender una solicitud, deberá informar de ello, motivando su negativa, dentro del plazo de un mes desde su presentación.

(cont.)

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	**Contenido**
Derecho de acceso (artículo 15)	Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento. Los responsables podrán atender a este derecho facilitando el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.
Derecho al olvido (artículo 17)	No está considerado un derecho autónomo o diferenciado de los clásicos derechos ARCO, sino la consecuencia de la aplicación del derecho al borrado de los datos personales. Es una manifestación de los derechos de cancelación u oposición en el entorno *online*. Los responsables que hayan hecho públicos los datos personales deberán adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar su información personal.
Derecho a la limitación del tratamiento (artículo 18)	La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. Se puede solicitar la limitación cuando: • El interesado ha ejercido los derechos de rectificación u oposición y el responsable está en proceso de determinar si procede atender a la solicitud. • El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello. • Los datos ya no son necesarios para el tratamiento, que también determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones. En el tiempo que dure la limitación, el responsable solo podrá tratar los datos afectados, más allá de su conservación: • Con el consentimiento del interesado. • Para la formulación, el ejercicio o la defensa de reclamaciones. • Para proteger los derechos de otra persona física o jurídica. • Por razones de interés público importante de la Unión o del Estado miembro correspondiente.

(cont.)

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	**Contenido**
Derecho a la portabilidad (artículo 20)	El derecho a la portabilidad de los datos es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Este derecho solo puede ejercerse: • Cuando el tratamiento se efectúe por medios automatizados. • Cuando el tratamiento se base en el consentimiento o en un contrato. • Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del afectado. El derecho a la portabilidad implica que los datos personales del interesado se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.
Relación responsable-encargado	El RGPD contiene obligaciones expresamente dirigidas a los encargados. La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su nulidad. Los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo: • Deben mantener un registro de actividades de tratamiento. • Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan. • Deben designar a un delegado de protección de datos en los casos previstos por el RGPD. Según el RGPD, el responsable deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD (principio de responsabilidad activa). Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD. Contratos de encargo concluidos con anterioridad a la aplicación del RGPD en mayo de 2018 deben modificarse y adaptarse para respetar este contenido, sin que sean válidas las remisiones genéricas al artículo del RGPD que los regula.

(cont.)

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	Contenido
Privacidad por diseño y por defecto (artículo 25)	Los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD. Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.
Medidas de seguridad (artículo 32)	En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo. Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta: • El coste de la técnica. • Los costes de aplicación. • La naturaleza, el alcance, el contexto y los fines del tratamiento. • Los riesgos para los derechos y libertades. En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas.
Notificaciones de violación de seguridad (artículos 33 y 34)	Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados. La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella. La notificación ha de incluir un contenido mínimo: • La naturaleza de la violación. • Categorías de datos y de interesados afectados. • Medidas adoptadas por el responsable para solventar la quiebra. • Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

(cont.)

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	**Contenido**
Notificaciones de violación de seguridad (artículos 33 y 34)	Los responsables deben documentar todas las violaciones de seguridad. En los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con una notificación dirigida a estos últimos. El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible. El RGPD añade a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.
Evaluación de impacto y consulta previa (artículos 35 y 36)	Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados. El RGPD establece un contenido mínimo de las evaluaciones de impacto sobre la protección de datos, aunque no contempla ninguna metodología específica para su realización. Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del RGPD indiquen que esos tratamientos presentan alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas necesarias para adecuar esos tratamientos a las exigencias del RGPD. En los casos en que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia evaluación de impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

(cont.)

OBLIGACIONES DEL RGPD PARA LOS RESPONSABLES	
Obligación (artículo)	**Contenido**
Delegado de protección de datos (artículo 39)	El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en: • Autoridades y organismos públicos. • Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala. • Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles. El DPD ha de ser nombrado atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, en la medida en que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea. La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados, y deberán ser comunicados a las autoridades de supervisión competentes. La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran: • Total autonomía en el ejercicio de sus funciones. • Necesidad de que se relacione con el nivel superior de la dirección. • Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.
Transferencias internacionales de datos (artículos 44-50)	Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo: • A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado. • Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino. • Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

V. TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Las transferencias internacionales de datos personales (TID) ha sido uno de los caballos de batalla que ha tenido que afrontar la Unión Europea en materia de protección de datos. Como principales hitos[191]:

1. El 30 de mayo de 2006, la Gran Sala del Tribunal de Justicia de la UE dictó una sentencia sobre los asuntos C-317/04 y C-318/04, *Parlamento contra Consejo y Comisión,* la nulidad de la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al servicio de Aduanas y Protección de Fronteras de los Estados Unidos (DO L 235, p. 11) debido a que el tratamiento de datos objeto de la decisión se excluye de lo estipulado por la Directiva 95/46, y de la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de Seguridad Nacional, Oficina de Aduanas y Protección de Fronteras de los Estados Unidos (DO L 183, p. 83, y corrección de errores en DO 2005, L 255, p. 168), puesto que no puede ser adecuado a derecho la celebración de un acuerdo cuyo objeto se encuentra excluido de la directiva mencionada.

2. En 2013, la Resolución del Parlamento Europeo de 23 de octubre de 2013, sobre la suspensión del acuerdo TFTP a raíz de la vigilancia de la NSA[192], insta a la Comisión Europea a actuar sobre la posible suspensión del acuerdo SWIFT de transmisión de datos bancaria.

---

[191] *Vid*. ORTEGA GIMÉNEZ, Alfonso, «Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield», en *Revista Lex Mercatoria, Doctrina, Praxis, Jurisprudencia y Legislación*, n.º 4, Universidad Miguel Hernández, Elche, 2016, p. 85.

[192] Texto aprobado, P7_TA(2013) 0449.

3. El último tropiezo lo encontramos en 2015 por otra STJUE de la Gran Sala sobre el asunto C-362/14, *caso Schrems,* por el cual anula la Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, porque se ha constatado que Estados Unidos no es considerado un tercer país que garantice un nivel de protección adecuada.

Los sucesivos varapalos institucionales no han hecho más que *aumentar la inseguridad jurídica dentro de los Estados miembros respecto a las TID, puesto que, y aunque ellas dependen de un derecho interno muy heterogéneo en Europa, las decisiones de adecuación vienen a traer estabilidad y uniformidad a dicha materia.*

Se ha reflejado en el RGPD la importancia de las transferencias de los flujos de datos a terceros países para la expansión del comercio[193] y de la cooperación internacional, pero las transferencias internacionales de datos no deben menoscabar el derecho a la protección de datos de los particulares[194].

Por ello, el nuevo régimen de las transferencias internacionales de datos del RGPD tiene una doble razón de ser[195]: *por un lado, el flujo transfronterizo de datos es no solo imprescindible en la actualidad, sino que aumenta día a día; y por el otro, intentar restringir sin razones tales flujos de datos en pos de la protección de datos está abocado al fracaso.*

El nuevo RGPD ha venido a subsanar este problema por la eficacia directa que disfrutan los reglamentos europeos, y refuerza también el régimen de las transferencias, aumentando las garantías que se deben asegurar para llevarlas a cabo.

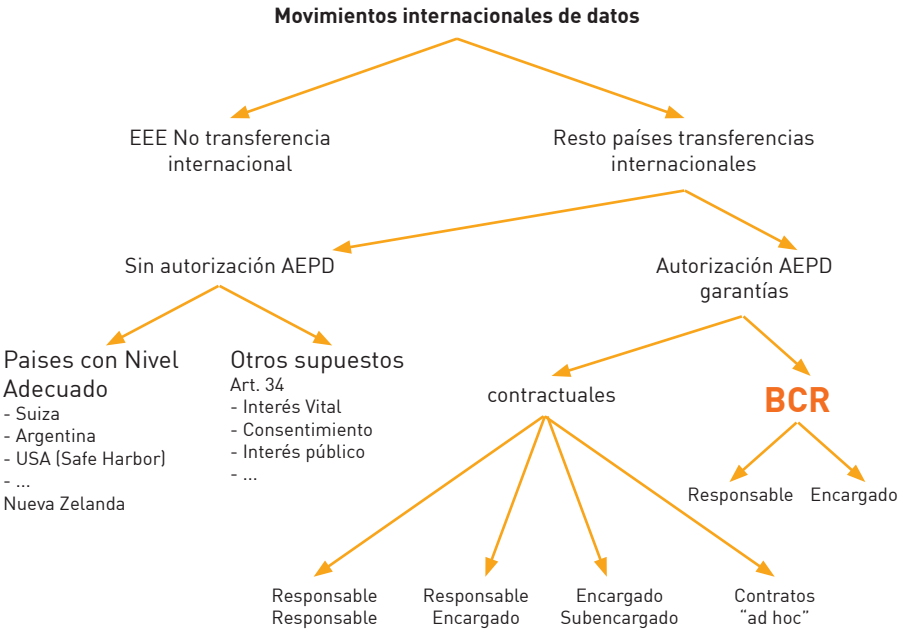
---

[193] *Vid.* OSTER, Jan, *European and International Media Law,* Cambridge University Press, Cambridge (UK), 2017, p. 351.

[194] *Vid*. Considerando 101 del RGPD.

[195] *Vid*. PINAR MAÑAS, José Luis, «Transferencias de datos personales a terceros países u organizaciones internacionales», en PINAR MAÑAS, José Luis (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Editorial Reus, Madrid, 2016, p. 430.

Figura 4. Esquema de las transferencias internacionales de datos



Fuente: AEPD.

V.1. CONCEPTO

La definición de *transferencia internacional de datos* no se encuentra en ningún instrumento legislativo comunitario[196], pero el TJUE, sin llegar a dar una definición formal, ha delimitado en sentido negativo el contenido de la definición a raíz del *Caso Lindqvist*.

El objeto principal de la cuestión planteada al TJUE era determinar si la publicación de datos personales en una página web almacenada por su proveedor de servicios de

[196] Tampoco la encontramos en las UN *Guidelines for the Regulation of Computerized Personal Data Files.* Aprobadas por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990, cuyo texto se limita a otorgar una serie de principios que los Estados deben respetar. En cambio, podemos encontrar una definición en las *OECD Privacy Guidelines of 2013,* que las define simplemente como «Movimientos de datos personales a través de las fronteras nacionales».

alojamiento domiciliado en la Unión, en la que se puede acceder desde cualquier lugar, debe ser considerada como una transferencia internacional (apartado 71), y se determinó que no debe considerarse como tal, aunque sí se considera un tratamiento de datos (apartado 27).

El tribunal basa su fallo en dos elementos:

1. *La naturaleza técnica de las operaciones efectuadas.* El acto de haber publicado en una página web los datos personales no implica «una transmisión directa entre dos sujetos, sino que se han transmitido con ayuda de una infraestructura informática» (apartado 60). Esto quiere decir que uno de los elementos constituyentes de una transferencia internacional de datos es la existencia de dos sujetos en el proceso (un exportador de datos y un importador de los mismos).

2. *El objetivo y la organización sistemática de la Directiva 95/46/CE.* El momento del desarrollo de Internet al tiempo de la publicación de la directiva influyó en lo que debe considerarse como «transferencia», y no tenía en cuenta las posibilidades que ofrecería Internet en el futuro. Por eso este tipo de operaciones no se contemplan en la directiva y, por tanto, no se consideran transferencias internacionales.

Pero en el contexto actual, este argumento *no puede ser válido: sería iluso por parte del legislador pensar que estas operaciones no han podido ser previstas por el reglamento, pero aun siendo previstas, no han sido contempladas de forma expresa en el texto.*

Por tanto, una transferencia internacional de datos deberá constar de los siguientes elementos[197]:

1. Debe tratarse de datos de carácter personal; esto es, de «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables». En definitiva, «que

[197] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita,* AEPD, Madrid, 2015, p. 23; y *Transferencias internacionales de datos de carácter personal ilícitas,* Aranzadi, Cizur Menor, 2017, p. 31.

permitan identificar o hacer identificable a una persona de manera directa o indirecta»[198].

2. Los datos de carácter personal que vayan a transmitirse vienen referidos tanto a aquellos que son tratados de forma automatizada (movimientos realizados por medios informatizados) como a los tratados de forma no automatizada (aquellos generados por medios convencionales).

3. La transferencia internacional de datos se efectúa con el objeto de realizar un tratamiento de datos de carácter personal por parte del destinatario de los mismos, ya sea tanto cesión (a otro responsable) como prestación de un servicio (encargado de tratamiento).

4. El traslado físico efectivo de los datos de carácter personal, de un lugar a otro, a través de las fronteras nacionales, ya sea dentro o fuera de la UE.

5. El lugar de destino de los datos de carácter personal debe encontrarse en un territorio distinto al de origen de estos.

6. Existirá transferencia internacional de datos personales en cualquiera de los dos casos siguientes: cuando constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable.

Aunque en la LOPD no se hubiese definido la *transferencia internacional de datos*, sí lo hizo la Instrucción 1/2000 de la Agencia Española de Protección de datos, considerándolos como «toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero» (norma primera).

Pero hay que tener en cuenta que esta instrucción fue anulada parcialmente por la SAN de 15 de marzo de 2002, y confirmada por la STS de 25 de septiembre de 2006.

---

[198] *Vid*. artículos 3.a) LOPD, 5.1.f) del RLOPD y 4.1) del RGPD.

Posteriormente, el RLOPD definió el concepto en el artículo 5.1 s) como «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español».

Tras estas definiciones, se asentó un concepto laxo sobre lo que se puede considerar como *transferencia internacional de datos* entendiéndolos como «cualquier comunicación de datos fuera del territorio español»[199]. Aunque solo deben considerarse transferencia internacional de datos en sentido estricto las transferencias a terceros países que no pertenecen al Espacio Económico Europeo (EEE)[200,201].

Pero en el contexto actual, y atendiendo al requisito mínimo al que se refiere la Instrucción 1/2000 respecto a la fluidez de los datos[202], puede ser factible reformular el concepto *transferencia internacional de datos* con el objetivo de incluir los supuestos de *acceso internacional de datos,* quedando como «todo movimiento de datos de carácter personal, provisional o definitivo, sin importar el soporte en que se encuentren los mismos, los medios utilizados ni el tipo de tratamiento que reciban, a una persona ubicada fuera del territorio español, así como el acceso a los datos por parte de una persona ubicada fuera del territorio español»[203].

La consideración de los supuestos de acceso internacional como transferencias internacionales *indudablemente reforzará el derecho del titular a la protección de datos*[204], pero, por otra parte, el flujo de datos podrá verse *drásticamente reducido debido a los estrictos procedimientos de autorización de las que son objeto las transferencias*

---

[199] *Vid*. CAZURRO BARAHONA, Víctor, «Transferencias internacionales de datos», en ÁLVAREZ HERNANDO, Javier y CAZURRO BARAHONA, Víctor, *Practicum Protección de datos 2016*, Aranzadi, Cizur Menor, 2015, p. 391.

[200] *Vid*. FERNÁNDEZ-LONGORIA, Paula y FERNÁNDEZ-SAMANIEGO, Javier, «Transferencias internacionales de datos personales», en TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley…*, *op. cit.,* p. 1779.

[201] Actualmente está compuesto por los veintiocho Estados de la UE más Liechtenstein, Islandia y Noruega.

[202] *Vid*. ERDOZÁIN LÓPEZ, José Carlos, «La protección de los…», *op. cit.,* p. 10.

[203] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular…, op. cit.,* p. 28; el mismo, *Transferencias internacionales…, op. cit.,* p. 36.

[204] *Ibidem*.

internacionales. En la misma consideración, PINAR MAÑAS aporta como argumento el nuevo artículo 49.1.g), que considera válida la transferencia cuando se realice desde un registro público que, con arreglo al derecho de la Unión o de los Estados miembros, tenga por objeto facilitar la información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés, pero solo en la medida en el que se cumplan las condiciones que establece el derecho de la Unión o de los Estados miembros para la consulta. Es decir, bastaría con la puesta a disposición de los datos[205], misma postura que mantiene el supervisor europeo de protección de datos[206].

V.2. RÉGIMEN JURÍDICO PREVISTO EN EL RGPD

El nuevo régimen del RGPD está recogido en el capítulo IV, y viene a sustituir el régimen basado en principios y excepciones de la Directiva 95/46/CE por un capítulo de siete artículos en los que se recoge el principio de prohibición general de transferencias internacionales (artículo 44), las transferencias realizadas bajo una decisión de adecuación (artículo 45), las transferencias realizadas mediante las garantías adecuadas (artículo 46), el régimen de las normas corporativas vinculantes (artículo 47), transferencias o comunicaciones no autorizadas (artículo 48), excepciones (artículo 49) y cooperación internacional (artículo 50).

La finalidad del RGPD es garantizar que sus normas ofrezcan el máximo nivel de protección de los particulares, de modo que en la práctica se impida su incumplimiento o menoscabo a través de conductas que distorsionen o desfiguren el régimen protector de las transferencias internacionales de datos.

Por eso el nuevo régimen no se limita solo a regular las transferencias con una mera decisión de adecuación, sino que también incluye normas claras para posibilitar transferencias mediante garantías adecuadas, transferencias mediante normas

---

[205] *Vid*. PINAR MAÑAS, José Luis, «Transferencias de datos personales a terceros países u organizaciones internacionales»..., *op. cit.,* p. 433.

[206] *Vid*. SEPD, *The transfer of personal data to third countries and international organizations by EU institutions and bodies,* Position paper, Bruselas, 2014, pp. 5-6.

corporativas vinculantes, además de contemplar significativas excepciones para dar viabilidad práctica a situaciones específicas[207].

V.2.1 Principio general y transferencia bajo una decisión de adecuación (artículos 44 y 45 del RGPD)

El principio negativo que contiene el RGPD determina que «solo se podrán efectuar transferencias internacionales de datos a un tercer país u organización internacional si, prácticamente, cumple todas las obligaciones que manda el reglamento; en especial, las consistentes en garantías en las ulteriores transferencias»[208].

Por lo tanto, la sociedad en cuestión no solo debe afirmar que es «segura», también debe acreditar que ha implementado las medidas de seguridad oportunas y que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también estos adoptan las garantías tecnológicas suficientes[209].

Como norma general, esa transferencia será autorizada mediante una decisión de adecuación que certifique que ese país, región u organización internacional tiene un «nivel de protección adecuado». Esta decisión se tomará sobre la base de:

a) el Estado de derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como

---

[207] *Vid*. DÍAZ DÍAZ, Efrén, «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», en *Revista Aranzadi Doctrinal*, n.º 6, Aranzadi, Cizur Menor, 2016, p. 13.

[208] «Artículo 44. Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente reglamento no se vea menoscabado».

[209] *Vid*. DÍAZ DÍAZ, Efrén, «El nuevo Reglamento General de...», *op. cit.,* p. 13.

la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los afectados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos los poderes de ejecución adecuados, de asistir y asesorar a los afectados en el ejercicio de sus derechos y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

Se prevé un mecanismo de revisión cada cuatro años con el objetivo de controlar si ese tercer Estado, región u organización internacional sigue cumpliendo con tales condiciones. Si se observa que ya no se cumple tal nivel, la Comisión derogará, suspenderá o modificará el acuerdo. Se entablarán conversaciones con ese Estado para poner remedio a la situación anterior.

Esta última previsión hace una clara referencia a la STJUE *Schrems,* por la cual se anularon los principios de puerto seguro.

Actualmente, los Estados sobre los que existe una decisión de adecuación son: Suiza[210], Canadá[211], Argentina[212], Guernsey[213], Isla de Man[214], Jersey[215], Islas Feroe[216], Andorra[217], Israel[218], Uruguay[219], Nueva Zelanda[220] y Estados Unidos de América[221].

Las decisiones de todos estos Estados –excepto la de EE. UU.– fueron modificadas por la Decisión de Ejecución 2016/2295 de la Comisión, de 16 de diciembre de 2016, en las que se añadieron mayores controles por parte de la Comisión a los países con el nivel de protección adecuado respecto a sus ordenamientos jurídicos.

V.2.2. Transferencias mediante garantías adecuadas. Cláusulas contractuales tipo (artículo 46 del RGPD)

Si no se hubiese dictado una decisión según las características anteriores, solo se podrán transferir datos personales a un tercer Estado u organización si se hubieran ofrecido las garantías adecuadas y los derechos exigibles.

Los medios por los cuales se pueden aportar esas garantías son:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

---

[210] Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.

[211] Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

[212] Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.

[213] Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.

[214] Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.

[215] Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.

[216] Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.

[217] Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.

[218] Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.

[219] Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.

[220] Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

[221] Decisión 2016/1250 de la Comisión, de 12 de julio de 2016. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE. UU.

b) normas corporativas vinculantes;

c) cláusulas tipo de protección de datos adoptadas por la Comisión o autoridad de control y aprobadas por la Comisión;

d) un código de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los afectados; o

e) un mecanismo de certificación, con los mismos compromisos que la medida anterior.

La derogación de los principios del *Safe Harbour* instauró una atmósfera de inseguridad en la Unión Europea debido a que se cuestionaban (y se siguen cuestionando) los medios proporcionados por la Unión para efectuar las transferencias internacionales de datos. A todo esto, el CEPD dictaminó que las cláusulas contractuales tipo y las normas corporativas vinculantes serían suficientes para garantizar la seguridad de los datos[222]. Sobre todo, han sido las primeras el medio más utilizado por las empresas para continuar con las transferencias internacionales de datos a terceros Estados, ya que «son una herramienta de gran utilidad que permite transferir datos personales desde todos los Estados miembros mediante un conjunto de normas comunes»[223].

Tanto la Comisión como la AEPD han adoptado diferentes cláusulas dependiendo de la calidad de los sujetos intervinientes:

a) Cuando se traten de transferencias entre responsables de tratamiento, podrán utilizarse las cláusulas recogidas en la Decisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país entre responsables[224] y la Decisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la

---

[222] *Vid.* Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems *v* Data Protection Commissioner case (C-362-14).

[223] *Vid.* GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria,* AEPD, Madrid, 2014, p. 162.

[224] DOCE L 181, 4 de julio de 2001.

transferencia de datos personales a terceros Estados[225] (versión consolidada de 1 de abril de 2005), modificada por la Decisión de Ejecución 2016/2297/CE [226].

Las cláusulas contenidas en la Decisión 2001/497/CE *contienen un régimen de responsabilidad solidaria entre ambos responsables en el caso de que el afectado haya sufrido algún tipo de perjuicio.* En cambio, el conjunto de cláusulas de la Decisión 2004/915/CE regulan un régimen de responsabilidad *basado en la debida diligencia*[227] por la cual el importador y exportador de datos responderán ante los afectados por el incumplimiento de sus obligaciones respectivas. El exportador será responsable si no realiza esfuerzos razonables para determinar si el importador es capaz de cumplir sus obligaciones legales. Se prevé una mayor intervención del exportador a la hora de la resolución de las reclamaciones de los afectados. La autoridad de control podrá prohibir o suspender con más facilidad las transferencias si el exportador rechaza tomar medidas contra el importador para hacerle cumplir sus obligaciones.

Ambos conjuntos de cláusulas tienen una composición rígida. Solo se puede elegir uno de ellos, sin que quepa utilizar cláusulas de los dos modelos en un mismo contrato, ni modificar las existentes.

b) Cuando se traten de transferencias entre encargados, podrán utilizar las recogidas en la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, modificada por la Decisión de Ejecución 2016/2297/CE.

Esta decisión contiene cláusulas específicas para la subcontratación por un encargado del tratamiento establecido en un tercer país a otros subencargados establecidos en terceros países. También añaden las condiciones que debe cumplir el subtratamiento para garantizar que los datos personales sigan protegidos con independencia de una ulterior transferencia a un subencargado del tratamiento. Ese

---

[225] DOUE L 385, 29 de diciembre de 2004.

[226] DOUE L 344/100, 17 de diciembre de 2016.

[227] *Ibidem*, nota 211.

subtratamiento no podrá exceder de las operaciones estipuladas en el contrato, por lo que deberá adecuarse al principio de finalidad. Aun si el subencargado incumple sus obligaciones, el importador de datos continuará siendo responsable. Al igual que las anteriores cláusulas, no solo son exigibles entre los importadores y exportadores, sino que también son exigibles por el afectado cuando sufra un perjuicio derivado de un incumplimiento contractual.

c) Cuando se traten de transferencias de encargado a subencargado del tratamiento, podrán utilizar las cláusulas contractuales redactadas por la AEPD en 2012.

Tal y como dicen el CEPD[228] y el considerando 23 de la Decisión 2010/87/UE[229], las cláusulas recogidas en la mencionada decisión solo son de aplicación a las transferencias entre encargados del tratamiento a subencargados del tratamiento que se encuentren ambos en terceros países, por lo que no se aplican a transferencias realizadas de un encargado establecido en el Espacio Económico Europeo a un subencargado establecido en un tercer país. El CEPD otorgó tres soluciones:

1. Un contrato directo entre el encargado del tratamiento en el EEE y el subencargado del tratamiento en aquel tercer país según la Decisión 2010/87/UE.

2. Un mandato expreso en el que el responsable da al encargado establecido en el EEE el poder de utilizar las cláusulas tipo de la Decisión 2010/87/UE por su cuenta.

3. Un contrato *ad hoc* del cual hace mención la Decisión 2010/87/UE.

---

[228] *Vid.* WP 176. «Lista de preguntas más frecuentes planteadas por la entrada en vigor de la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo».

[229] Solo se aplica a la subcontratación por un encargado del tratamiento establecido en un tercer país de sus servicios de tratamiento a un subencargado establecido en un tercer país, por lo que no se aplicará a la situación en la que un encargado del tratamiento establecido en la Unión Europea y que realice el tratamiento de datos personales en nombre de un responsable del tratamiento establecido en la Unión Europea subcontrate sus operaciones de tratamiento a un subencargado del tratamiento establecido en un tercer país. En tales situaciones, los Estados miembros son libres de tener en cuenta el hecho de que los principios y las garantías de las cláusulas contractuales tipo establecidas en la presente decisión se hayan utilizado para subcontratar a un subencargado establecido en un tercer país con la intención de prestar la adecuada protección de los derechos de aquellos afectados cuyos datos personales se estén transfiriendo para operaciones de subtratamiento.

Esta última solución es la que ha adoptado la AEPD. El conjunto de cláusulas prevé que la solicitud de autorización de transferencia internacional sea efectuada por el encargado. Por este modelo, el responsable deberá autorizar con anterioridad al encargado la posterior subcontratación a un subencargado importador. En el contrato marco entre responsable-encargado regulado en el artículo 12 del LOPD y en los artículos 20-22 del RLOPD debe estar especificado la autorización para la subcontratación y para la transferencia internacional de datos.

La habilitación para el uso de estos instrumentos se encuentra en el artículo 70.2 RLOPD. Para solicitar la autorización se deberá aportar:

1. Escrito de solicitud con identificación de los ficheros objeto de la transferencia con indicación del código con el que el fichero figura inscrito en el Registro General de Protección de Datos.

2. Contrato basado en las cláusulas contractuales tipo firmado por las partes (copia original o fotocopia compulsada).

3. Poderes suficientes de los firmantes.

4. La inscripción de los ficheros deberá encontrarse completamente actualizada.

5. Para cualquiera de los documentos se deberá aportar, en su caso, traducción al español por intérprete jurado.

6. Las cláusulas contractuales tipo que, para las TID, establecen las decisiones de la Comisión Europea dan cumplimiento, a su vez, a lo establecido en el artículo 46 del RGPD (en el momento en el que este sea de aplicación).

En el artículo 41.1 del Proyecto de LOPD de 2017 se recoge la potestad de la AEPD de crear cláusulas contractuales tipo sometidas al dictamen del Comité Europeo de Protección de Datos según el artículo 64 del RGPD.

Las cláusulas contractuales adoptadas por las decisiones de la Comisión Europea se encuentran en entredicho a raíz de la STJUE *Schrems*. Actualmente, hay un

procedimiento abierto en la *High Court* irlandesa[230] en el que vuelven a intervenir Facebook y Max Schrems con el objetivo de buscar el pronunciamiento del Tribunal de Justicia de la Unión Europea. El DPC irlandés argumentó en el caso que las cláusulas no otorguen protección suficiente a los ciudadanos europeos cuando sus datos personales se transfieren fuera del EEE, y dichos datos pueden estar en riesgo de ser accedidos y procesados por agencias estatales de EE. UU. por razones de seguridad nacional de una manera incompatible con los artículos 7 y 8 de la Carta de los Derechos Fundamentales, que otorgan derechos al respeto de la vida privada y familiar y a la protección de los datos personales, respectivamente. Al considerar el caso, el Tribunal Superior de Irlanda declaró que «el derecho de la Unión Europea garantiza un alto nivel de protección a los ciudadanos de la UE». Las inquietudes suscitadas por el caso *Schrems*[231] y el procedimiento abierto en Irlanda han sido a lo que ha llevado a la Comisión Europea a adoptar la Decisión de Ejecución 2016/2297/CE con el objetivo de aumentar el flujo de información entre las autoridades de control y la Comisión[232].

Aunque las decisiones se encuentren en tela de juicio, el mismo artículo 46 permite adoptar unas garantías adecuadas mediante otros instrumentos contractuales adoptados por las partes, siempre que sean validados por la correspondiente autoridad de control. Este nuevo clausulado debe tener la estructura de un contrato de encargado recogido en el artículo 26 del RGPD:

1. Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal

---

[230] «Data Protection Commissioner *v.* Facebook Ireland Limited & Maximilian Schrems». The Court Record Number: 2016/4809P.

[231] *Vid*. los considerandos 1, 6 y 7 de la Decisión de Ejecución 2016/2297/CE.

[232] Modificación de sendos artículos 4 de la Decisión 2001/497/CE y de la Decisión 2004/915/CE: Cuando las autoridades competentes de los Estados miembros ejerzan sus facultades con arreglo al artículo 28, apartado 3, de la Directiva 95/46/CE, y ello dé lugar a la suspensión o la prohibición definitiva de los flujos de datos hacia terceros países con el fin de proteger a las personas en lo que respecta al tratamiento de sus datos personales, el Estado miembro afectado informará inmediatamente a la Comisión, que remitirá la información a los demás Estados miembros.

previa al tratamiento, salvo que tal derecho lo prohíba por razones importantes de interés público;

2. la garantía de que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

3. la adopción de todas las medidas necesarias de seguridad;

4. el cumplimiento de las pautas para la designación de subencargados;

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

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

7. suprimir o devolver todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimir las copias existentes a menos que se requiera la conservación de los datos personales en virtud del derecho de la Unión o de los Estados miembros;

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

V.2.3. Normas corporativas vinculantes (artículo 47 del RGPD)

Cuando se trate de transferencias internacionales de datos entre empresas del mismo grupo, el RGPD ha previsto un régimen «a medida» para aquellas entidades, conocidas como Normas Corporativas Vinculantes (NCV), o *Binding Corporate Rules* (BCR's).

El considerando 110 otorga la posibilidad de que un grupo empresarial pueda invocar unas NCV autorizadas para efectuar transferencias internacionales de datos a otras entidades del grupo situadas en terceros países, siempre que tales normas incluyan las garantías necesarias[233].

Al contrario que las cláusulas contractuales tipo, en la elaboración de las NCV no ha intervenido la Comisión para elaborar unas normas tipo. Ha sido el CEPD mediante numerosos *papers* quien ha ido perfilando el contenido de las NCV hasta la entrada en vigor del reglamento. Sobre la base de todos esos documentos de trabajo, el RGPD incluye en el artículo 47 el contenido que deben tener las NCV, además de establecer un mecanismo por el cual la Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control mediante decisiones de ejecución.

El nuevo régimen (más institucionalizado que el anterior al reglamento) se debe al objetivo principal del reglamento de homogenizar la legislación europea sobre protección de datos y añadir coherencia a los actos de las autoridades de protección de datos europeas.

La legitimación de estos instrumentos en la normativa española se encuentra en el artículo 137 del RLOPD, y el uso de las NCV es combinable con las cláusulas contractuales tipo.

V.2.3.1. Concepto y contenido

Son normas internas adoptadas por un grupo multinacional de empresas que definen su política global con respecto a las transferencias internacionales de datos personales dentro de un mismo grupo empresarial a entidades situadas en países que no ofrecen un nivel adecuado de protección. Están destinadas únicamente a los grupos empresariales.

---

[233] Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

Actualmente, el artículo 4. 20) del RGPD los define como «las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta».

Si anteriormente existían dudas sobre su carácter vinculante «legal»[234], el RGPD consagra que tales normas serán exigibles jurídicamente «tanto en el ámbito interno como externo», estipulado en artículo 47.1.

El *contenido mínimo* de las normas se encuentra en el artículo 47.2 del RGPD:

a) La estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros.

b) Las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de afectados y el nombre del tercer o los terceros países en cuestión.

c) Su carácter jurídicamente vinculante, tanto a nivel interno como externo.

d) La aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y, por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes.

---

[234] Debido a que el régimen legal anterior a ello era ínfimo, se dudaba de que la adopción de tales reglas entre las sociedades pudiera llegar a ser exigible legalmente entre las partes. *Vid*. ÁLVAREZ RIGAUDAS, Cecilia, «Movimiento internacional de datos: las transferencias internacionales de datos personales», en TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley..., op. cit.,* p. 1827; y CERVERA NAVAS, Luis, «Primera aproximación a las "Binding Corporate Rules" para la transferencia de datos personales a terceros países», en *Revista datospersonales.org*, n.º 4, septiembre de 2003.

e) Los derechos de los afectados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros, y el derecho a obtener una reparación y, cuando proceda, una indemnización por violación de estas normas.

f) La aceptación por parte del responsable o del encargado del tratamiento establecido en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro.

g) La forma en que se facilita a los afectados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f), y en cuanto al derecho de información.

h) Las funciones de todo delegado de protección de datos, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las NCV dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta.

i) Los procedimientos de reclamación.

j) Los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas para garantizar la verificación del cumplimiento de las NCV, como auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del afectado. Los resultados de dicha verificación deberían comunicarse al delegado de protección de datos o similar, y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas, y ponerse a disposición de la autoridad de control competente que lo solicite.

k) Los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control.

l) El mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j).

m) Los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un tercer país a un miembro del grupo empresarial o de la unión de empresas, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes.

n) La formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

Como complemento a estos requisitos, debemos tener en cuenta los siguientes documentos de trabajo del CEPD: WP 74[235], WP 107[236], WP 108[237], WP 153[238], WP 154[239] y WP 155[240].

El uso de estas normas por los responsables del tratamiento de los grupos multinacionales ha aumentado rápidamente con el paso de los años debido a la flexibilidad que estas otorgan[241]. Para adaptarse a los nuevos modelos de negocios, el CEPD ha

---

[235] «Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers». Adoptado el 3 de junio de 2003.

[236] «Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"». Adoptado el 14 de abril de 2005.

[237] «Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules». Adoptado el 14 de abril de 2005.

[238] «Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules». Adoptado el 24 de junio de 2008.

[239] «Working Document Setting up a framework for the structure of Binding Corporate Rules». Adoptado el 24 de junio de 2008.

[240] «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules». Adoptado el 24 de junio de 2008, y modificado el 7 de febrero de 2017.

[241] *Vid*. GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón, «*Cloud Computing,* cláusulas contractuales y reglas corporativas vinculantes», en *Revista de Derecho UNED*, n.º 14, Madrid, 2014, p. 266.

elaborado unas nuevas RCV destinadas a los encargados del tratamiento, cuyo régimen se encuentra en los WP 195[242], 195a[243] y WP 204[244].

El WP 204 considera que las RCV para los encargados del tratamiento «se conciben originariamente como un instrumento de ayuda para estructurar las transferencias internacionales de datos personales inicialmente tratados por un encargado del tratamiento, en nombre de un responsable del tratamiento de la UE y según sus instrucciones, y subtratados dentro de la organización del encargado del tratamiento».

V.2.3.2. Procedimiento de elaboración y aprobación

El procedimiento para adoptar estas reglas deriva de los anteriores documentos:

a) *Primer paso:* la empresa designará a *la autoridad principal,* es decir, *la autoridad que se encargará del procedimiento de cooperación de la UE entre las demás APD europeas mediante el formulario del WP 133,* que sirve también para solicitar la aprobación de las RCV ante la autoridad. El WP 244 establece las guías para identificar a esa autoridad líder. La identificación de esta figura solo es necesaria cuando se produce un tratamiento transfronterizo de datos.

    1. El artículo 4. 23) del RGPD entiende por *tratamiento transfronterizo:* a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a afectados en más de un Estado miembro.

---

[242] «Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules». Adoptado el 6 de junio de 2012.

[243] «Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities». Adoptado el 17 de septiembre de 2012.

[244] «Explanatory Document on the Processor Binding Corporate Rules». Adoptado el 19 de abril de 2013, y modificado el 22 de mayo de 2015.

2. El RGPD no define el significado «afecta sustancialmente», y ha sido el WP 244 que nos indica que este término debe interpretarse caso por caso, y sobre la base de distintos criterios como el contexto del tratamiento, el tipo de datos tratados, el objeto del proceso y otro tipo de factores como si dicho tratamiento es susceptible de provocar daños a las personas, si puede limitar el derecho de las personas, o si puede afectar a la salud, calidad de vida o tranquilidad de las mismas. La prueba de «efecto sustancial» tiene por objeto garantizar que las autoridades de supervisión solo están obligadas a cooperar formalmente mediante el mecanismo de coherencia del artículo 63 del RGPD «cuando una autoridad de supervisión tenga la intención de adoptar una medida destinada a producir efectos jurídicos en operaciones de tratamiento que afectan a un número significativo de sujetos de datos en varios Estados miembros»[245].

b) *Segundo paso:* la empresa redacta el BCR cumpliendo con los requisitos establecidos en los documentos de trabajo adoptados por el Comité Europeo de Protección de Datos. Este proyecto se presenta a la autoridad principal que lo revisa y proporciona comentarios a la empresa para asegurar que el documento cumpla con los requisitos establecidos en el documento WP 153.

c) *Tercer paso:* la autoridad responsable inicia el procedimiento de cooperación de la UE mediante la circulación del BCR a la DPA pertinente, es decir, de aquellos países desde donde las entidades del grupo transfieren datos personales a entidades situadas en países que no garantizan un nivel adecuado de protección.

d) *Cuarto paso:* el procedimiento de cooperación de la UE se cierra después de que los países de reconocimiento mutuo hayan reconocido la recepción del BCR y los que no estén reconocidos mutuamente han considerado que el NCV cumple con los requisitos establecidos en el WP29 (en el plazo de un mes)[246].

e) *Quinto paso:* el RGPD exige en el artículo 64.1.f) que el futuro comité emita un dictamen previo a la aprobación de las reglas, que deberá ser seguido por la autoridad

---

[245] *Vid.* Considerando 135 del RGPD.

[246] *Vid*. artículos 47.1, 57.1.s), y 58.3.j) RGPD.

de control. Si esta no lo siguiese, el comité emitirá un dictamen vinculante según el art 65.1.c).

f) *Sexto paso:* una vez que el BCR haya sido considerado como definitivo por todos los DPA, la compañía solicitará autorización de transferencias sobre la base del BCR adoptado por cada DPA nacional.

El artículo 70.1.i) estipula que el comité emitirá directrices, recomendaciones y buenas prácticas con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos basadas en las NCV a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados, y otros requisitos adicionales para garantizar la protección de los afectados.

El Proyecto de LOPD de 2017 recoge la potestad de la AEPD de permitir a este órgano la creación de NCV. El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de un año. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del RGPD y se reiniciará tras su notificación a la AEPD.

V.3. SUPUESTOS SOMETIDOS A AUTORIZACIÓN O INFORMACIÓN PREVIA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

En el caso de que una transferencia internacional no se ampare en ninguno de los medios anteriormente estudiados, la AEPD o las autoridades autonómicas autorizarán previamente cuando se apoyen en cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control.

La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refiere el artículo 64 del RGPD. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la AEPD o, por conducto de la misma, a la autoridad de control competente.

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquellos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del RGPD:

1. que la transferencia no sea repetitiva;

2. que afecte a un número limitado de personas;

3. que los intereses del responsable no prevalezcan sobre intereses o derechos y libertades del afectado, y

4. que se hayan ofrecido garantías apropiadas con respecto a la protección de datos personales.

V.4. *PRIVACY SHIELD*

En 2015, *la STJUE de la Gran Sala sobre el asunto C-362/14, caso Schrems, anula la decisión de la Comisión de 26 de julio de 2000 (conocida como Safe Harbour) porque constató que Estados Unidos no es considerado un tercer país que garantice un nivel de protección adecuada.* El puerto seguro era una institución jurídica que permitía a las empresas la transmisión de datos hacia sociedades en EE. UU., cumpliendo una serie de principios referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son complementados con las «preguntas más frecuentes», básicamente referidas a tipos específicos de datos o tratamientos.

El Privacy Shield *es un mecanismo de autocertificación de empresas estadounidenses en el que se permite la transferencia de datos a las empresas que hayan sido certificadas mediante el cumplimiento de unos requisitos de seguridad y de unos principios avalados*

por el Departamento Federal de Comercio. Las empresas certificadas se incluirán en una lista publicada por las autoridades estadounidenses en las que se muestran a todas las empresas que han superado el proceso de autocertificación. Esas empresas deberán renovar anualmente su autocertificación. Del mismo modo, deberán tomar medidas para verificar que las políticas de privacidad que han publicado se ajustan a los principios y se aplican.

Fue aprobada la Decisión de Ejecución 2016/1250 el 12 de julio y de aplicación el 1 de agosto[247]. La estructura de la nueva decisión consta de solo seis artículos, pero de 155 considerandos y siete anexos donde se recogen los compromisos adquiridos por los organismos estadounidenses.

El Privacy Shield *se aplica tanto a los responsables como a los encargados del tratamiento,* si bien estos deben estar obligados, por contrato, a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la Unión Europea y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los siguientes principios[248]:

1. *Principio de notificación/derecho a ser informado*

Las empresas estadounidenses estarán obligadas a informar a los titulares de los datos sobre los aspectos clave en el procesamiento de sus datos de carácter personal (tipos de datos recopilados, propósito del procesamiento de los datos, derechos de acceso a la información y condiciones de transmisión o cesión de dichos datos a un tercero, medios de contacto con la empresa, órgano de resolución de controversias, APD de EE. UU.). Además de diversas obligaciones formales [a) su adhesión al *Privacy Shield* y la indicación del enlace a la lista de entidades adheridas al mismo; b) los tipos de datos que se han recogido; c) el compromiso que tiene la entidad de cumplir con dichos principios; d) la finalidad para la cual se recogen los datos; e) el procedimiento para contactar con la entidad para presentar reclamaciones y quejas].

---

[247] DO L 207/1, de 1 de agosto de 2016.

[248] *Vid.* PÉREZ CAMBERO, Raúl, «Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de Privacidad UE-EE. UU.», en *Actualidad Administrativa,* n.º 4, Wolters Kluwer, Madrid, 2017, p. 3.

2. *Principio de elección/derecho de elección*

Las empresas estadounidenses deberán obtener el consentimiento formal por parte de los ciudadanos antes de ceder sus datos personales sensibles a entidades terceras o se utiliza para un fin distinto por el que se recabaron los datos en un principio.

3. *Principio de seguridad*

Las empresas estadounidenses deberán evaluar los riesgos de seguridad en el tratamiento de la información de carácter personal y deberán implantar medidas de seguridad que mitiguen al máximo riesgos como pérdidas, mal uso, acceso no autorizado, revelación, alteración o destrucción de estos datos. En el caso de que la entidad subcontrate a un tercero de un servicio determinado, se le deberá exigir un nivel de seguridad equivalente al requerido por la entidad para la protección de la información de carácter personal tratada.

4. *Principio de integridad y limitación de la finalidad*

Las empresas estadounidenses deberán garantizar la integridad de los datos personales obtenidos. El titular de los datos soolo deberá ser revelado en los casos en que esto sea imprescindible. La limitación de la finalidad de los datos implica que los datos de carácter personal recabados deben ser relevantes para los fines del tratamiento. Únicamente se permite guardar los datos personales en tanto resulten necesarios para el propósito del tratamiento. A dichas empresas se les permitirá conservar datos durante periodos más prolongados exclusivamente en caso de que los necesite para determinados fines en particular, tales como archivo por interés público, periodismo, literatura y arte, investigación científica o histórica, o para análisis estadístico (los mismos que se recogen en el RGPD).

Si el nuevo fin es sustancialmente distinto, la empresa sujeta al Escudo de Privacidad solo podrá usar sus datos si no se pone ninguna objeción o, en caso de tratarse de datos sensibles, si da su consentimiento. Si el nuevo fin está bastante relacionado con el original, su uso es permisible. Existe el derecho a elegir si los datos enviados a una empresa sujeta al Escudo pueden transferirse a otra empresa, sea de EE. UU. o no. Si los datos son enviados a otra empresa para tratarlos en su nombre, esta deberá suscribir

un contrato con la segunda empresa con las mismas garantías que ofrece el Escudo. La responsabilidad de la empresa receptora es extensible a la empresa sujeta al Escudo.

5. *Principio de acceso/derecho de acceso y rectificación de sus datos*

Las empresas estadounidenses deberán informar a los titulares de los datos sobre el contenido que obran en su poder y deberá facilitarles el acceso a dichos datos en un plazo de tiempo razonable, salvo que suponga un esfuerzo desproporcionado. Se podrá solicitar a la empresa que los corrija, los cambie o los elimine si no son exactos, están desfasados o han sido procesados infringiendo las normas del Escudo de Privacidad. La empresa deberá también confirmar si guarda y procesa o no sus datos personales. Las peticiones de acceso a su información personal podrán ser efectuadas por los ciudadanos en cualquier momento. Por lo general, no se obliga a dar ninguna razón acerca de los motivos por los que desea acceder a sus datos; no obstante; la empresa podrá pedirle que lo haga si su solicitud es demasiado genérica o vaga.

6. *Principio de responsabilidad para transmisiones lícitas*

Como elemento común, se pueden transmitir datos a terceros de manera lícita solo si existe justificación expresa.

Si se va a transferir los datos a un tercero responsable de los datos, deberán cumplir los principios de notificación y opción. Las entidades deberán requerir, a través de un acuerdo por escrito, que las terceras partes que reciban los datos personales otorguen el mismo nivel de protección que el que proporciona el *Privacy Shield*.

Si se realiza a un tercero que actúe como encargado del tratamiento, la entidad deberá asegurarse, entre otras, de que este tratará los datos únicamente para los fines para los que fueron recabados.

7. *Principio de responsabilidad, aplicación y responsabilidad/derecho a reclamar y ser indemnizado*

Las empresas estadounidenses deberán implantar sistemas de verificación del cumplimiento de los principios del *Privacy Shield* y deberán informar de su cumplimiento

de manera anual por medio de la renovación de su autocertificación, donde deberán acreditar las acciones que han adoptado para ceñirse a los principios del *Privacy Shield*. En el caso de que las empresas afectadas no demuestren el cumplimiento de dichos requerimientos, saldrán de la lista de empresas adheridas al *Privacy Shield* y estarán sujetas a sanciones económicas.

Si se considera que se han vulnerado los derechos y ha recibido un perjuicio, se tiene derecho a reclamar:

a) Ante la propia empresa estadounidense sujeta al Escudo de Privacidad. La empresa debe responder en un plazo de 45 días desde la recepción de la reclamación. La respuesta deberá establecer si la reclamación tiene o no fundamento y, en caso afirmativo, qué recurso aplicará la empresa como solución.

b) Mediante un mecanismo de recurso independiente, como la RAL o ante la APD. La RAL es un procedimiento privado de resolución alternativa de litigios que debe ofrecer la empresa sujeta al Escudo. Puede ejercerse en la UE o en EE. UU. También se puede optar por una APD europea.

c) Ante el Departamento de Comercio de EE. UU. (aunque únicamente a través de la APD). Este examinará su reclamación y responderá a su APD en un plazo de 90 días. El Departamento de Comercio también podrá remitir las reclamaciones a la Comisión Federal de Comercio (o al Departamento de Transportes).

d) Ante la Comisión Federal de Comercio de EE. UU. (o el Departamento de Transportes de EE. UU. si la reclamación se refiere a una compañía aérea o una agencia de viajes).

e) Ante el Panel del Escudo de Privacidad, solo después de que hayan fracasado las demás opciones de reparación. Es un «mecanismo de arbitraje» compuesto por tres árbitros neutrales. Sus decisiones son vinculantes y ejecutables ante los tribunales estadounidenses. El recurso al arbitraje podrá invocarse únicamente a través del Panel del Escudo de Privacidad, y con arreglo a determinadas condiciones. Solo el consumidor puede ejercer esta medida. Para iniciar el procedimiento, hay que notificar formalmente a la empresa su intención de hacerlo. La notificación

deberá incluir un resumen de los pasos previos para resolver su reclamación y una descripción de la supuesta infracción. El arbitraje tendrá lugar en EE. UU., pero el consumidor tendrá diversos derechos:

- Solicitar la asistencia de su APD para preparar su reclamación.

- Posibilidad de tomar parte en los procedimientos por teléfono o videoconferencia, por lo que no se requiere estar presente físicamente en Estados Unidos.

- Posibilidad de obtener interpretación y traducción de documentos sin ningún coste del inglés a otro idioma.

Los costes arbitrales correrán a cargo de un fondo constituido para ello. El procedimiento terminará en el plazo de 90 días, y si se declara a favor del consumidor, ofrece medidas de reparación como acceso, corrección, eliminación o devolución de los datos personales. El Panel no puede resarcir económicamente, por lo que habrá que acudir a los tribunales estadounidenses para ello. Si no se está de acuerdo con el resultado del arbitraje, puede recurrirse ante los tribunales. Si la reclamación se efectuara contra una autoridad pública estadounidense, se activa el mecanismo del Ombudsperson, un alto funcionario de EE. UU. independiente receptor de reclamaciones. La reclamación se efectuará en colaboración con la APD del Estado miembro.

8. *Se prevén otros principios accesorios en casos especiales*

Como los datos sensibles, periodísticos, responsabilidad subsidiaria, auditorías, información sobre viajes, productos médicos y farmacéuticos, información de registros públicos e información accesible al público, o solicitudes de acceso de las autoridades públicas.

Por la otra parte, el Congreso de Estados Unidos adoptó la ley de Recurso Judicial que permite salvaguardar la protección de los derechos y datos provenientes de la Unión[249].

[249] Public Law No: 114-126 (24 de febrero de 2016).

Tras la publicación y entrada en vigor de la decisión, el CEPD dictó las WP 245 y 246 con una serie de indicaciones para las empresas y los individuos, donde aparece la información para solicitar el proceso de certificación para el *Privacy Shield,* así como indicaciones previas a la transferencia de datos. Además, se ha acordado que las autoridades nacionales sean consideradas órganos centralizados de la UE en el que se tramitan solicitudes de reclamación relativas a los accesos por razones de seguridad nacional a datos transferidos a EE. UU. con fines comerciales.

Pero no todo es positivo en esta nueva decisión. La poca rigidez en las obligaciones impuestas a Estados Unidos[250], el lenguaje ambiguo, poco claro y difícil de entender en algunos aspectos, debido a que muchos términos se interpretan de manera diferente en la Unión Europea y en Estados Unidos[251], y las nuevas reformas emprendidas por el nuevo Gobierno de Estados Unidos han supuesto una pérdida de protección de la privacidad, como la *Executive Order on Public Safety*[252], que excluye la aplicación de la ley de Protección de Datos estadounidense a las personas extranjeras en Estados Unidos, o la derogación de la *rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"*[253]; aunque recientemente *se ha nombrado al nuevo* ombudsperson, *cargo designado a dirimir las reclamaciones relacionados con el* Privacy Shield, *cuya independencia se pone en entredicho.*

Todas estas medidas dirigidas a mermar la privacidad en Estados Unidos afectan directamente a los datos personales exportados a las empresas estadounidenses. Por ello, el Parlamento Europeo ha dictado una resolución[254] donde ha lamentado las nuevas reformas estadounidenses y pide a la Comisión Europea medidas destinadas a asegurar los principios estipulados en la decisión.

---

[250] *Vid.* Wolters Kluvier, «El "Escudo de Privacidad" entre la UE y EE. UU. necesita mejorar», en *Diario La Ley*, n.º 8760, Wolters Kluvier, Madrid, 2016.

[251] *Vid.* BU-PASHA, Shakila, «Cross-border issues under EU data protection lawwith regards to personal data protection», en *Information & Communications Technology Law,* Taylor & Francis, 2017, p. 12.

[252] Executive Order 13768, 27 de enero de 2017.

[253] Public Law No: 115-22 (4 de marzo de 2017).

[254] (2016/3018(RSP)).

En septiembre de 2017 la Comisión Europea realizó la primera revisión anual conjunta entre EE. UU. y la Comisión Europea[255] donde se ha concluido que Estados Unidos, hasta la fecha, *continúa asegurando un nivel adecuado a los datos personales transferidos bajo el* Privacy Shield *a las organizaciones adheridas.* Aun así, la Comisión recomienda algunas medidas destinadas a asentar el propio mecanismo en un tono muy laxo.

En cambio, el CEPD en el WP 255 ha sido más contundente respecto a la revisión conjunta, donde destaca las deficiencias de esta decisión de adecuación. El dictamen del CEPD se ha basado en el a) ámbito privado como en la b) *sumisión del* Privacy shield *ante las leyes que permiten el acceso de datos personales a instituciones públicas con razón de cumplimiento de la ley y seguridad nacional.*

Respecto a las deficiencias en los aspectos que atañen a las empresas, el CEPD destaca:

a) La falta de documentos de apoyo por parte del Departamento de Comercio.

b) La concepción de datos laborales por parte de las organizaciones estadounidenses, que difiere respecto al de la Unión Europea.

c) Falta de supervisión en el cumplimiento de los principios.

d) La aplicación del *Privacy Shield* a los encargados establecidos en EE. UU.

e) La inexistencia de reglas especiales para los supuestos de *profiling.*

En cuanto a las excepciones por seguridad nacional y cumplimiento:

a) La recopilación de datos indiscriminada a las agencias de inteligencia y seguridad.

b) La supervisión de los programas de vigilancia, ejecutada por la Privacy and Civil Liberties Oversight Board.

---

[255] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield (COM(2017) 611 final).

c) Las dificultades de un ciudadano europeo de solicitar una indemnización en procesos penales en casos de vigilancia.

d) La ausencia de *ombudsperson* como órgano independiente que se prometió por parte del Gobierno estadounidense.

Como declaración, el CEPD pretende que estos problemas sean corregidos un año. Si no se consigue, *planteará una cuestión prejudicial* para que el TJUE se pronuncie sobre la legalidad de la Decisión 2016/1250 conforme al artículo 7 de Carta Europea de Derechos Humanos si EE. UU. no adaptase su legislación a las recomendaciones antes de septiembre, puesto que fundamentos no le faltan para pedirlo. Esta opinión se suma a la *Resolución del Parlamento Europeo sobre la adecuación de la protección otorgada por el Escudo de Privacidad UE-EE. UU.*[256] El Parlamento Europeo mantiene una postura similar a la presentada por el CEPD, *instando a la Comisión Europea a suspender el* Privacy Shield *a partir del 1 de septiembre si no se aplicasen las recomendaciones.* Ya ha pasado la fecha límite, y aún se permiten las transferencias a Estados Unidos, por lo que habrá que estar atentos a los siguientes movimientos entre ambos bloques.

[256] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0315+0+DOC+XML+V0//EN.

VI. TRATAMIENTO ILÍCITO DE LOS DATOS: RECLAMACIONES DE LOS AFECTADOS DESDE EL DERECHO INTERNACIONAL PRIVADO

Los tratamientos de datos nominativos generan una serie de responsabilidades de índole administrativo, civil y, en su caso, penal, que obligan, por un lado, a hacer frente a las sanciones administrativas o penales impuestas ante la Comisión, por acción o incumplimiento, de determinados actos considerados ilícitos, y, por otro, a resarcir de los daños causados generados por dichos tratamientos. Estas responsabilidades recaerán, en forma individual o colectiva, según los casos, sobre el titular del fichero, el responsable del mismo, el encargado del tratamiento, el responsable de seguridad, o sobre aquellas otras personas relacionadas directa o indirectamente con el fichero a quienes, por sus facultades o actos, pudieran serles atribuidas.

En lo que respecta a las responsabilidades civiles, el responsable y, en su caso, el encargado del tratamiento, junto con el titular del fichero que responderá con ellos en forma solidaria, asumirán aquellas derivadas de los actos propios u omisiones, contemplados en las normas civiles.

Estas responsabilidades, en función de su origen, pueden dividirse en responsabilidades contractuales, que nacen del incumplimiento de aquellas obligaciones estipuladas contractualmente, y responsabilidades extracontractuales, que nacen de actos dañosos generados al margen de una relación contractual.

Respecto a las responsabilidades contractuales, los marcos normativos de referencia establecen que, cuando no sea posible obtener el cumplimiento de cualquier obligación, previamente pactada, relacionada con la protección de los datos, se sustituirá dicho cumplimiento por una indemnización a la persona concernida que deberá cubrir la totalidad de daños y perjuicios ocasionados por el incumplimiento.

Como excepciones a la regla general de responsabilidad por incumplimiento contractual, establecida en la teoría general del contrato, se suelen indicar en el cuerpo del

mismo, por un lado, mediante cláusulas de limitación de responsabilidad, un tope a la cuantía máxima de indemnización, y por otro, mediante las denominadas *cláusulas de limitación de responsabilidad,* un tope a la cuantía máxima de indemnización; además, mediante las denominadas cláusulas penales, la fijación de una cuantía que, como compensación de los presuntos daños causados, se establece como cobertura de la responsabilidad derivada del incumplimiento, evitando los problemas que suelen surgir con la prueba de cuantificación de los daños ocasionados.

En cuanto a las responsabilidades extracontractuales, estas se establecen, en lo que respecta a la protección de datos, como protección de la persona afectada ante los daños que pueda sufrir derivados del riesgo generado por el tratamiento de sus datos nominativos.

Así, pues, el primer elemento a considerar, en lo que respecta a la responsabilidad civil, es la generación de un daño consumado cierto, personal, directo y que afecte a intereses legítimos de la víctima, elementos todos ellos imprescindibles para exigir esta responsabilidad.

El daño causado puede afectar tanto a la esfera patrimonial, que abarcará tanto la pérdida efectiva como el lucro cesante, como a la esfera moral, que abarcará cualquier tipo de perjuicio susceptible de incidir en el ámbito espiritual de la víctima y, en especial, dados los riesgos habitualmente generados por los tratamientos de datos, en la vulneración de sus derechos al honor, intimidad o propia imagen.

En cuanto a la posibilidad de imputación del deber de reparar el daño causado a terceros, hay que recordar que la concepción de la responsabilidad civil ha evolucionado desde una perspectiva meramente subjetiva (responsabilidad civil subjetiva), que vinculaba la obligación de resarcimiento a la existencia de una culpa o negligencia, a otra perspectiva objetiva (responsabilidad objetiva), que contempla el resarcimiento del daño en sí mismo considerado[257].

A partir de estas consideraciones, debemos resaltar que la acción de responsabilidad contemplada en el RGPD se refiere a una responsabilidad extracontractual como

---

[257] *Vid.* PÁEZ MAÑÁ, Jorge, «Responsabilidades derivadas del tratamiento nominativo de datos», en *Informáticos Europeos Expertos*, s/f. Disponible en: http://www.iee.es/pages/bases/articulos/derint026.html.

explicaremos con más detenimiento posteriormente, puesto que se resuelve fuera de un hipotético marco contractual. Aunque debemos destacar la existencia de una eventual responsabilidad contractual, en el caso de que la entidad aseguradora se haya comprometido a custodiar los datos conforme a la legislación vigente y a los fines que se determinen en el propio contrato.

Este doble régimen es de gran relevancia en supuestos internacionales, ya que el régimen jurídico aplicable desde el derecho internacional privado varía en las cuestiones fundamentales objeto de esta materia, tales como la competencia judicial internacional y la ley aplicable.

VI.1. DERECHO A INDEMNIZACIÓN DEL RGPD

El RGPD regula *por primera vez el derecho a la indemnización derivado de los daños causados por el tratamiento ilegal de los datos de carácter personal en el artículo 82*[258]; al contrario que la directiva, que se dedicaba en el artículo 23 a obligar a los Estados a

---

[258] «Artículo 82. Derecho a indemnización y responsabilidad:

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.
2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.
3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.
4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del afectado.
5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.
6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al derecho del Estado miembro que se indica en el artículo 79, apartado 2».

configurar el derecho a la indemnización en sus ordenamientos internos. En España, la transposición se realizó en el artículo 19 de la LOPD.

El artículo 82 establece la responsabilidad del responsable del tratamiento: «el responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente reglamento». Se establece la responsabilidad del responsable cuando participe en una operación y no cumpla, tanto por acción como por omisión, las normas del RGPD dirigidas a los encargados, o cuando el encargado obvie las indicaciones del responsable.

El RGPD establece un *sistema de responsabilidad directa* del responsable del tratamiento por los daños causados a una persona física tanto si el tratamiento se llevase a cabo en un establecimiento del responsable como si se externalizase a un tercer encargado. La responsabilidad de este último es limitada, puesto que solo responderá cuando el daño y perjuicio deriven de un incumplimiento de las obligaciones legales del RGPD y de sus normas derivadas. Podemos entender como lógica esta limitación, puesto que el encargado del tratamiento actúa por mandato del responsable[259].

Cuando nos referimos al incumplimiento de lo dispuesto en el RGPD, incluimos un tratamiento que infrinja también los actos delegados y de ejecución de conformidad con el RGPD, así como las normas de desarrollo aportadas por los Estados miembros en cumplimiento del RGPD[260].

En este punto, cabe distinguir *una doble esfera de responsabilidad*[261]:

1. La que se deriva del incumplimiento de las disposiciones del RGPD y sus normas de desarrollo, que conlleva automáticamente a indemnizar el daño.

---

[259] *Vid.* RECIO GAYO, Miguel, «Acerca de la evolución de la figura del encargado del tratamiento», en *Revista de Privacidad y Derecho Digital,* n.º 0, 2015.

[260] *Vid.* Considerando 146 del RGPD.

[261] LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales*..., *op. cit.,* p. 176.

2. Demostrar la ausencia de responsabilidad en el hecho de que haya causado el daño y que va junto con la adopción de las medidas técnicas y organizativas que impone el artículo 24 del RGPD. Se debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta[262]. La anterior afirmación hace que nos situemos en el supuesto del artículo 1902 del CC[263], pero es un mero espejismo, puesto que el mismo considerando debe demostrar, además, la conformidad de las actividades del tratamiento con el RGPD. Esto conlleva a invertir la carga de la prueba y demostrar que no se actuó con la debida diligencia.

Como hemos dicho anteriormente, podemos encontrarnos una responsabilidad subjetiva, aquella que se genera con el incumplimiento de cualesquiera obligaciones civiles legales o contractuales y, asimismo, de los actos u omisiones ilícitos, siempre y cuando intervenga culpa o negligencia y se produzca un daño; y una responsabilidad objetiva, aquella que se genera con la mera producción de un determinado daño concreto, sin que la causa del mismo provenga de una determinada infracción del ordenamiento jurídico, o de culpa o negligencia (ya sea directa o indirecta) del imputado[264].

El sistema introducido por el RGPD es un sistema de responsabilidad subjetiva. En este sentido, el párrafo tercero del artículo 82 del RGPD exonera de responsabilidad por los daños causados en la operación de tratamiento al responsable y encargado si se demuestra que no es responsable en modo alguno del hecho que haya causado los daños y perjuicios.

Respecto al objeto que se debe indemnizar, *son indemnizables los daños y perjuicios materiales o inmateriales; es decir, se cubren tanto los daños físicos como morales,* interpretándose el concepto de «daños y perjuicios» que dicta el TJUE[265], por lo que se viene a buscar una reparación integral del daño sufrido. En cuanto a los daños morales,

---

[262] *Vid.* Considerando 74.

[263] «El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado».

[264] *Vid.* PÁEZ MAÑÁ, Jorge, «Responsabilidades derivadas del...», *op. cit.*

[265] *Vid.* Considerando 146 del RGPD. En cuanto a la doctrina del TJUE, *vid.* STJUE *Liffers* (Asunto C-99/15).

destacamos la reciente STS 261/2017, de 26 de abril, en la que estipula los criterios para evaluar el daño moral por el incumplimiento de los requisitos de la LOPD.

En ella, el Tribunal considera como relevantes:

- El tiempo de permanencia de los datos.
- El alcance de la divulgación de los datos personales a terceros.
- La inacción del responsable del tratamiento (fichero).

El tribunal considera irrelevantes para la cuantía de indemnización:

- El mero incumplimiento de la LOPD;
- la naturaleza de las personas consultantes de los ficheros, y
- que el afectado no haya podido acceder a servicios ofrecidos por las empresas consultantes.

El RGPD regula la responsabilidad solidaria del responsable y el encargado, permitiendo al afectado demandar una indemnización total y efectiva tanto al responsable como al encargado, pudiendo repetir el sujeto que abonó la indemnización contra el resto de sujetos intervinientes por la parte que les correspondería pagar. El Proyecto de LOPD de 2017 en su artículo 30.2 extiende la responsabilidad solidaria al representante establecido en la Unión Europea.

A todo esto, hay que diferenciar esta acción civil de la reclamación por vía administrativa, y que, eventualmente, puede desencadenar en un recurso contencioso-administrativo, puesto que esta última vía no está destinada a la reparación económica del daño, sino en la imposición de sanciones respecto a las infracciones estipuladas tanto en la LOPD como en el RGPD. Aunque también cabe la posibilidad de dirimir determinadas infracciones a través de un proceso civil como, por ejemplo, la imposición al responsable de una limitación o prohibición al tratamiento, tal y como expresa la STS (Sala de lo Civil) de 15 de octubre de 2015.

Actualmente, existe una divergencia entre una reclamación realizada por la vía civil y la vía administrativa, siendo posible efectuar acciones indistintamente sin que una excluya a la otra derivada de las sentencias relacionadas con el derecho de supresión en la contradicción entre las SSTS 574/2016 y 210/2016. Ambas sentencias discuten sobre quién es el responsable del tratamiento de los datos, a lo que las salas dan respuestas contradictorias[266].

1. La STS 574/2016 estipula que el responsable del tratamiento de esos datos es quien gestiona técnica y administrativamente los medios para la indexación de la información, como es, en este caso, el motor de búsqueda. Y es la empresa matriz quien destina los medios para gestionarlo. La empresa filial no sería responsable si entre sus actividades principales no consta ninguna orientada a la indexación o almacenamiento de datos. No existiría tampoco corresponsabilidad al no existir unidad de negocio, ya que sus actividades están diferenciadas. Aunque sean representantes de la empresa matriz, es una sociedad con personalidad jurídica diferenciada y con objetivos diferenciados. Esta consideración se reduce en la jurisdicción C-A, cuyo objeto pueden ser las reclamaciones de los afectados por el medio indexador, así como las resoluciones de la AEPD en procedimientos de tutela de derechos en materia de protección de datos. Estas incidencias no pueden dirigirse contra la entidad filial, sino contra la matriz.

2. Por el contrario, la STS 210/2016 considera que el responsable del tratamiento es, en la mayoría de los casos, la filial, ya que según el TJUE, al interpretar la Directiva 95/46, no se exige para la aplicación del derecho nacional que el tratamiento de los datos sea efectuado directamente por el propio establecimiento (la matriz), sino que se halle en las actividades de este. Considera que las actividades de la matriz y de la filial están ligadas, porque la filial, aun no dedicándose directamente a la indexación de la información, realiza actividades de promoción del medio de indexación (motor de búsqueda), además de ofrecerle los recursos económicos, sin importar la forma jurídica de la filial. Por lo tanto, la filial y la matriz son corresponsables del tratamiento de datos, y está legitimada pasivamente para ser parte demandada en los

---

[266] *Vid.* DE MIGUEL ASENSIO, Pedro Alberto, «La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google», en *Diario La Ley*, n.º 8773, La Ley, Madrid, 2016, pp. 1-6.

litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición.

Resumiendo los problemas procesales y de competencia internacional, la sentencia de la sala primera explica que las sentencias no son contradictorias, ya que ambos casos están regidos por normas y principios totalmente diferentes, por lo que son complementarios en el siguiente sentido: para los casos respecto a procedimientos de tutela de derechos en materia de protección de datos, el responsable será la matriz extranjera; para el ejercicio en un proceso civil de sus derechos, lo será también la filial nacional. La postura adoptada por el TS está fundamentada en el alto coste que supondría litigar contra una persona jurídica en el extranjero; aparte, esta postura tiene el objetivo de favorecer a la parte débil (consumidor) en las transacciones internacionales de flujos de datos, permitiendo al afectado litigar en su lugar de residencia y sobre la base de su derecho nacional[267].

VI.2. RESPONSABILIDAD CONTRACTUAL DERIVADA DEL INCUMPLIMIENTO DE UN CONTRATO DE SEGURO

Tal y como hemos hablado a lo largo de este trabajo, un contrato de seguro implica el tratamiento de datos personales, tanto ordinarios como sensibles –podemos ver la habilitación en los artículos 10 y 11 de la LCS–, para los que la entidad aseguradora debe proteger obligatoriamente según las disposiciones legales nacionales e internacionales.

Pero eso no impide que se pueda acordar contractualmente el compromiso de la entidad aseguradora de proteger los datos personales según la legislación vigente. Es más, en el propio contrato deberá constar los fines destinados a tal tratamiento; y en el caso de que el tratamiento se realice para fines diferentes a los plasmados en contrato, estos deberán ser compatibles con los iniciales. En el caso de que no lo sean, el responsable del tratamiento podrá incurrir en responsabilidad contractual[268]. Incluso

[267] Idea recogida en la STJUE de 25 de octubre de 2011, *eDate Advertising y Martinez*, C-509/09 y C-161/10, y plasmada en el artículo 79.2 RGPD.

[268] Como ejemplo, SAP de Islas Baleares (sección 4.ª). Sentencia n.º 181/2007, de 23 de abril.

se ha llegado a afirmar que la acción de responsabilidad del artículo 19.1 de la LOPD (sin equivalente en el Proyecto de LOPD de 2017, remitiéndose a la regulación del RGPD) se ejercita en el marco de una responsabilidad contractual «por cuanto surge del incumplimiento de obligaciones legales previas que recaen sobre el responsable del tratamiento de datos personales, sin perjuicio de la aplicación preferente de las previsiones contenidas en la Ley Orgánica 1/1982, cuando haya sido infringido uno de los derechos fundamentales a cuya tutela se preordena esta ley, respecto de la que aquella es subsidiaria»[269]. Además, «la naturaleza contractual o no de la acción ejercitada con fundamento en el precepto que nos ocupa dependerá de la existencia o no de una relación contractual con fundamento en la cual se hayan cedido los datos personales al responsable del fichero»[270]. Por lo tanto, «las obligaciones del responsable del fichero o del encargado del tratamiento han de integrarse, además, y exartículo 1258 del CC, con las obligaciones legales y reglamentarias previstas»[271].

VI.3. CLÁUSULAS DE EXONERACIÓN O LIMITACIÓN DE RESPONSABILIDAD

Es común por los proveedores de tecnología *Big Data* que incluyan cláusulas de limitación o exoneración de responsabilidad, alegando que estos suministradores no tratan los datos personales, o que puede llegar a ser imposible conseguir una completa anonimización, requisito que no es necesario, como hemos estudiado en apartados anteriores de este trabajo, o porque tales proveedores no tratan los datos personales. Por ello, la estipulación de dichas cláusulas puede considerarse abusiva y nula según la legislación nacional y comunitaria.

En las relaciones comerciales, podemos encontrarnos, como es habitual, una relación «profesional-consumidor persona física», en la que claramente podemos observar una parte jurídicamente débil en la relación, y una relación «profesional-profesional»,

---

[269] *Vid.* GARCÍA RUBIO, María Pilar, «Bases de datos y confidencialidad en Internet», en ECHEBARRÍA SÁENZ, Joseba Aitor (coord.), *El comercio electrónico,* EDISOFER, Madrid, 2001, p. 487.

[270] *Vid.* BUTTARELLI, Giovanni, *Banche dati e tutela della riservatezza (La* privacy *nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997, pp. 351-352.

[271] *Vid.* BUSTO LAGO, José Manuel, «La responsabilidad civil de los servidores y operadores de datos», en *Seminario sobre Protección de Datos*, UCLM, Ciudad Real, 2005, p. 18.

en la que puede existir una parte débil si se cumplen determinadas condiciones[272]. Partiendo de esta base, debemos decir que la empresa contratante de tecnología *Big Data* no puede considerar consumidores a efecto de las Directivas 93/13/CEE[273] y 2011/83/UE[274], ni tampoco de la STJUE *Costea,* en la que permite a los profesionales ser consumidores ante comerciantes si el contrato no tiene relación con la actividad profesional. Por lo tanto, desde la perspectiva española, no es aplicable la Ley General para la Defensa de los Consumidores y Usuarios[275], sino la Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación[276], tal y como estipula la STS 57/2017, de 30 de enero.

Tal y como dice en el preámbulo de la exposición de motivos I de esta última ley, *las cláusulas generales de contratación pueden darse entre profesionales, y en tal relación pueden existir cláusulas abusivas, pero tal régimen debe atenerse a las reglas de nulidad contractual y no la lista de cláusulas abusivas recogidas en los artículos 82-85 de la Ley General para la Defensa de los Consumidores y Usuarios.* Para ello, es ilustrativa la STS 227/2015, de 30 de abril, en la que recuerda que: «[e]n nuestro ordenamiento jurídico, la nulidad de las cláusulas abusivas no se concibe como una técnica de protección del adherente en general, sino como una técnica de protección del adherente que tiene la condición legal de consumidor o usuario, esto es, cuando este se ha obligado con base en cláusulas no negociadas individualmente» [...] «las condiciones generales insertas en contratos en los que el adherente no tiene la condición legal de consumidor o usuario, cuando reúnen los requisitos de incorporación, tienen, en cuanto al control de contenido, el mismo régimen legal que las cláusulas negociadas, por lo que solo operan como límites externos de las condiciones generales los mismos que operan para las cláusulas negociadas, fundamentalmente los previstos en el art. 1255 del CC y en especial las normas imperativas, como recuerda el art. 8.1 LCGC».

---

[272] *Vid.* PASTOR VITA, Francisco Javier, «Las condiciones generales y cláusulas abusivas en los contratos celebrados entre empresarios», en *Diario La Ley*, n.º 6367, La Ley, Madrid, 2005.

[273] DO L 95, 21 de abril de 1993.

[274] DO L 304, 22 de noviembre de 2011.

[275] BOE n.º 287, de 30 de noviembre de 2007.

[276] BOE n.º 89, de 14 de abril de 1998.

Pero en esa exposición reconoce también que pueda existir un abuso de una posición contractual dominante, y existir una condición general que sea abusiva cuando sea contraria a la buena fe[277] y cause un desequilibrio importante entre los derechos y obligaciones de las partes, incluso aunque se trate de contratos entre profesionales o empresarios. Pero habrá de tener en cuenta en cada caso las características específicas de la contratación entre empresas.

Como dictó la STS 241/2013, de 9 de mayo, rechazó expresamente en su fundamento jurídico 233 c) que el control de abusividad pueda extenderse a cláusulas perjudiciales para el profesional o empresario. Pero igualmente en el fundamento jurídico 201 recordó que el control de incorporación de las condiciones generales se extiende a cualquier cláusula contractual que tenga dicha naturaleza, con independencia de que el adherente sea consumidor o no[278].

Pero en la ya citada STS 57/2017, se admite la relación entre los artículos 8.1 de la LCGC y 1258 del CC, con el 82.1 del TRLGCU. Las SSTS 367/2016 y 57/2017 admiten la usabilidad del artículo 1258 del CC para cláusulas que suponen un desequilibrio de la posición contractual del adherente, es decir, aquellas que modifican subrepticiamente el contenido que el adherente había podido representarse como pactado conforme a la propia naturaleza y funcionalidad del contrato, en el sentido de que puede resultar contrario a la buena fe intentar sacar ventaja de la predisposición, imposición y falta de negociación de cláusulas que perjudican al adherente, y puede postularse la nulidad de determinadas cláusulas que comportan una regulación contraria a la legítima expectativa

---

[277] STS 367/2016, de 3 de junio: «la virtualidad del principio general de buena fe como norma modeladora del contenido contractual, capaz de expulsar determinadas cláusulas del contrato, es defendible, al menos, para las cláusulas que suponen un desequilibrio de la posición contractual del adherente, es decir, aquellas que modifican subrepticiamente el contenido que el adherente había podido representarse como pactado conforme a la propia naturaleza y funcionalidad del contrato; [...]. [...] puede postularse la nulidad de determinadas cláusulas que comportan una regulación contraria a la legítima expectativa que, según el contrato suscrito, pudo tener el adherente [...]. Conclusión que es acorde con las previsiones de los principios de derecho europeo de los contratos, formulados por la Comisión de Derecho Europeo de los Contratos [...]».

[278] «En el derecho nacional, tanto si el contrato se suscribe entre empresarios y profesionales como si se celebra con consumidores, las condiciones generales pueden ser objeto de control por la vía de su incorporación a tenor de lo dispuesto en los artículos 5.5 LCGC "[l]a redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez", 7 LCGC "[n]o quedarán incorporadas al contrato las siguientes condiciones generales: a) Las que el adherente no haya tenido oportunidad real de conocer de manera completa al tiempo de la celebración del contrato [...]; b) Las que sean ilegibles, ambiguas, oscuras e incomprensibles [...]"».

que, según el contrato suscrito, pudo tener el adherente (sentencias 849/1996, de 22 de octubre; 1141/2006, de 15 de noviembre; y 273/2016, de 23 de abril).

Para obtener tal nulidad, debe tenerse en cuenta el nivel de información presentado por el empresario no adherido y la diligencia del empresario no adherente para conocer tales consecuencias jurídicas, que dependerá, en gran medida, de sus circunstancias subjetivas, como personalidad jurídico-mercantil, volumen de negocio, estructura societaria, experiencia, conocimientos financieros, asesoramiento, etc.

Y puesto que el adherente no es consumidor, operan las reglas generales de la carga de la prueba, por lo que habrá de ser el prestatario que pretende la nulidad de una condición general desde el punto de vista de la buena fe, alegando la introducción de una estipulación sorprendente que desnaturaliza el contrato y frustra sus legítimas expectativas, quien acredite la inexistencia o insuficiencia de la información y quien, ya desde la demanda, indique cuáles son sus circunstancias personales que pueden haber influido en la negociación y en qué medida la cláusula le fue impuesta abusivamente.

Vista la inaplicación de la TRLGCU, debemos atenernos al régimen presentado por el derecho común. Si pasamos al régimen concreto de una cláusula de exoneración de responsabilidad, cabe recordar que si el incumplimiento contractual fuera doloso, el artículo 1102 del CC estipula que siempre es exigible toda responsabilidad (no cabe tampoco limitación) derivada del dolo, y toda renuncia de la acción es nula. Es indiferente que tales pactos se hayan estipulado en el momento de la celebración del contrato, esto es, incluyéndose en él como una de sus cláusulas o, por el contrario, hayan sido estipulados con posterioridad a la celebración del mismo en un documento separado[279].

En cambio, se discute la posibilidad de admitir cláusulas de limitación o exoneración de la responsabilidad si el hecho fuera negligente. En el derecho español no existe ninguna disposición como la que se recoge en el artículo 1102 del CC, por lo que se argumenta su admisibilidad sobre la base del artículo 1003 del CC[280], por la no estipulación de

---

[279] *Vid.* DE VERDA Y BEAMONTE, José Ramón, «Las cláusulas de exoneración y limitación de responsabilidad en el derecho español», en *Revista Chilena de Derecho Privado*, n.º 4, Universidad Diego Portales, Santiago, 2005, p, 37.

[280] «La responsabilidad que procede de negligencia es igualmente exigible en el cumplimiento de toda clase de obligaciones».

nulidad, en relación con el artículo 1104[281]. Se ha afirmado así que, dado que el precepto permite a los contratantes pactar el grado de diligencia exigible en el cumplimiento de las obligaciones, estas pueden pactar que no les sea exigible ningún grado de diligencia en dicho cumplimiento, admitiéndose, en consecuencia, la validez general de las cláusulas de exoneración de responsabilidad procedente de culpa[282]; pero ello no significa que todas las cláusulas sean válidas, puesto que no deben ser contrarias a la buena fe del artículo 1255 del CC.

Es estos casos, hay que distinguir entre la culpa grave y la leve:

1. En caso de *negligencia grave,* las cláusulas de *exoneración de responsabilidad* pueden ser declaradas nulas por ser contrarias al orden público, por ser tal culpa casi equiparable al dolo[283] y, por tanto, siendo aplicable el artículo 1102 del CC (SSTS, 18 de junio de 1990 y 3 de julio de 1992). En cuanto a las cláusulas de limitación, se consideran nulas cuando la responsabilidad se derive por negligencia grave.

2. *Se puede admitir cuando sea por culpa leve* en virtud del artículo 1103 del CC, que permite a los tribunales moderar la responsabilidad en caso de negligencia, pero tales cláusulas no deben sobrepasar los límites del artículo 1255 del CC. Además, *deben ser inválidas las cláusulas de limitación* de responsabilidad por daños ocasionados a las personas (muerte o lesiones), y las cláusulas de limitación por culpa leve que, encubiertamente, causan una exoneración completa. Respecto a las cláusulas de limitación, caben distinguir y analizar las siguientes variantes:

   a) *Cláusula limitativa de la cuantía del resarcimiento:* es admitible por nuestro derecho la existencia de cláusulas limitativas que absorban la indemnización por daños y perjuicios (artículo 1152 del CC y STS, 16 de julio de 1982), pero serán nulas si la cuantía es irrisoria o desproporcionada al daño producido.

---

[281] «Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se exigirá la que corresponda a un buen padre de familia».

[282] *Vid.* ÁLVAREZ LATA, Natalia, *Cláusulas restrictivas de responsabilidad civil*, Comares, Granada, 1998, p. 84.

[283] *Ibidem*, nota 264, p. 49.

b) *Las cláusulas limitativas de la garantía patrimonial universal:* son admitibles las cláusulas limitativas de la responsabilidad efectiva sobre ciertos bienes, modificando el principio de garantía universal del artículo 1911 del CC. Esta tesis puede sostenerse mediante la disposición del artículo 1807 del CC[284] y el artículo 140 de la Ley Hipotecaria[285], además de la STS, 21 de mayo de 1963.

c) *Las cláusulas que acortan los plazos de prescripción de la acción:* son válidas las cláusulas que limitan la responsabilidad del deudor, acortando el largo plazo de prescripción de la acción para exigir indemnización de daños por incumplimiento, que es de cinco años, según resulta del artículo 1964 del Código Civil. No obstante, los pactos de acortamiento del plazo de prescripción serán nulos, cuando el plazo señalado fuera tan breve que, en la práctica, hiciera inviable el ejercicio de la acción.

---

[284] «El que constituye a título oneroso una renta sobre sus bienes puede disponer al tiempo del otorgamiento que no estará sujeta dicha renta a embargo por obligaciones del pensionista».

[285] «La obligación garantizada se haga solamente efectiva sobre los bienes hipotecados», precisando que: «en este caso la responsabilidad del deudor y la acción del acreedor por virtud del préstamo hipotecario quedarán limitadas al importe de los bienes hipotecados, y no alcanzarán a los demás bienes del patrimonio del deudor».

VII. PROTECCIÓN DE DATOS, CONTRATOS DE SEGURO Y DERECHO INTERNACIONAL PRIVADO

VII.1. COMPETENCIA JUDICIAL INTERNACIONAL DEL RGPD

El artículo 82 del RGPD remite al artículo 79.2, el lugar donde debe dirigirse el afectado derivado de un supuesto de responsabilidad del artículo 82. En este sentido, el artículo 82.6 nos remite al artículo 79.2, que dispone que las acciones dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro donde estos tengan un establecimiento.

Alternativamente, podrán ejercitarse tales acciones en los tribunales competentes del Estado miembro donde el reclamante tenga su domicilio, en concordancia con lo estipulado en el considerando 145[286].

Como hemos visto, *las acciones objeto del artículo 82 tienen un carácter «civil-mercantil» que, a su vez, se encuadran dentro del ámbito de aplicación del artículo 1.1 del Reglamento (UE) 1215/2012 «Bruselas I Bis»*[287]*, y cuya materia no está en los supuestos de exclusión del artículo 1.2.*

Aunque se dé por hecha la adecuación de esta acción a los supuestos de responsabilidad extracontractual cuando exista un perjuicio relacionado con un tratamiento de datos ilícito según el artículo 82.6 del RGPD, *pero es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del reglamento «Bruselas I Bis» si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales*

---

[286] Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el afectado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

[287] DOUE L 351/1, 20 de diciembre de 2012.

cuando se estudie caso por caso el objeto del contrato[288]. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente, aunque *la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual.*

Concretando más en el fuero del establecimiento del responsable, el artículo 79.2 permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento. Como hemos estudiado en el apartado III del presente trabajo, *debe tenerse un concepto flexible de «establecimiento»;* tal y como se indica en la STJUE *Weltimmo,* debe extenderse «a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable»[289]. Para ello, debe valorarse también el «grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión». En la STJUE *Amazon EU Sàri* considera posible tener en cuenta la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado[290], *siendo posible considerar como «establecimiento» un representante de la sociedad si actúa con un grado de estabilidad suficiente*[291].

De esta consideración se desprende que *cualquier establecimiento del encargado o del responsable permite atribuir la competencia a los tribunales del Estado miembro en el que esté sito.* Tampoco será necesario que la acción esté dirigida a las actividades de ese concreto establecimiento, sino que *la existencia de cualquier establecimiento extiende el daño causado.*

El foro alternativo que prevé el RGPD *permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual.* Para su consideración, será necesario que el afectado *tenga un grado de permanencia que revele una situación de estabilidad*[292].

---

[288] *Vid*. SSTJUE, 13 de marzo de 2014, *Brogsitter,* C-548/12, 14 de julio de 2016; *Granarolo*, C-196/15.

[289] *Vid.* Apartados 31 de la STJUE *Weltimmo* y 75 de la STJUE *Amazon EU Sàri*.

[290] *Vid.* Apartados 76 y 77.

[291] *Vid.* Apartado 30 de la STJUE *Weltimmo*.

[292] *Vid*. STJUE, 22 de diciembre de 2010, C-497/10, Mercredi ECLI:EU:C:2010:829.

La residencia habitual no es un concepto sinónimo al de «centro de intereses de la víctima» que promulga la STJUE eDate Advertising[293], que aunque en principio *suele coincidir con la «residencia habitual», podemos encontrarlo en otro Estado cuando exista un vínculo particularmente estrecho con ese otro Estado que resulte de otros indicios, como el ejercicio de una actividad profesional.* La consideración de este foro de competencia *no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño*[294]. Por lo que se puede dar el caso, por ejemplo, de que una persona, conocida en Islandia, que resida en España sin que sea conocida, sufra una difamación en España utilizando para ello la lengua islandesa. En este supuesto, el nacional islandés podrá demandar ante los tribunales españoles, aunque no se haya producido efectivamente el daño[295], en el caso de que el centro de intereses del afectado no se encuentre en el Estado de residencia, sino en el Estado con vínculos profesionales. Volviendo al ejemplo anterior, supongamos que este nacional trabaja como tertuliano en una televisión española, y sufre una difamación que atenta contra sus derechos a la personalidad, pero tal publicación está escrita en islandés, por lo que no tiene efecto «real» en España[296]. *En este sentido, creemos que hubiera sido mejor el criterio del abogado general del asunto estudiado, que proponía como criterio para determinar la competencia –el cual rechazó seguir el TJUE– el «centro de gravedad del conflicto»*[297]. Este criterio bebe del asimilado por el TJUE, que lo consagra como el lugar

---

[293] STJUE C-509/09 y C-161/10 eDate Advertising ECLI:EU:C:2011:685.

[294] *Vid.* OREJUDO PRIETO DE LOS MOZOS, Patricia, «La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia», en *La Ley Unión Europea*, n.º 4, 2013, p. 23.

[295] Sentencia del Tribunal Federal Supremo alemán *(Bundesgerichtshof)* BGH NJW 2011, 2059: El demandante y el acusado eran de Rusia y habían asistido a la escuela secundaria juntos en Moscú. Habiendo terminado la escuela, el demandante llegó a residir habitualmente en Alemania, el demandado en los Estados Unidos. Se reunieron de nuevo en septiembre de 2006 para una reunión de clases en Moscú. Después de este acontecimiento, el demandado fijó una entrada en la página www.womanineurope.com, que fue funcionado por una compañía alemana. En este post, el demandado describió las condiciones de vida y el aspecto del demandante en términos bastante desfavorables. El post fue escrito en lengua rusa y en letras cirílicas. El BGH denegó la jurisdicción porque la publicación carecía de una conexión suficiente con Alemania.

[296] *Ibidem*, nota 250.

[297] El criterio del «centro de gravedad del conflicto» no es un descubrimiento reciente. Los tribunales estadounidenses, por ejemplo, aplican un análisis de intereses al determinar la ley aplicable que también se denomina enfoque de «contactos más significativos», o «centro de gravedad» (p. ej. *Tooker v Lopez*, 24 N.Y.2d 569, 301 N.Y.S.2d 519, 249 N.E.2d 394 (1969), o *Neumeier v Kuehner*, 31 N.Y.2d 121, 335 (1972)). Esto incluye, junto con apreciaciones tradicionales como el lugar de contratación, lugar de ejecución o lugar del hecho dañoso, la consideración de qué jurisdicción mantiene la relación

donde el afectado «desarrolla esencialmente su proyecto vital» (59 de las Conclusiones), pero que tiene en cuenta dos criterios más:

1. *El contenido de la información*: esto es, si la información tiene interés en el territorio.

2. *La conexión que pueda tener con el territorio,* a la luz de indicios que derivan de la propia web, tales como el nombre de dominio de primer nivel, el idioma empleado, la publicidad que esta contenga o las palabras clave que se han suministrado a motores de búsqueda para identificar la página, o incluso de indicios exteriores, tales como los registros de la página.

La compatibilidad entre los foros del artículo 79.2 y los del reglamento «Bruselas I bis» deriva del artículo 67 de este último reglamento, al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares, como es el caso del artículo 79.2 del RGPD. En cuanto a los argumentos presentados por el RGPD, encontramos *el considerando 147, que afirma que las normas generales de competencia judicial del reglamento «Bruselas I bis» «deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD».* El considerando 145 estipula que el demandante «deberá tener la opción» de ejercitar las acciones en los tribunales de los Estados miembros.

Al observar lo anterior, revela que *el RGPD pone a disposición de los afectados la posibilidad de que puedan utilizar los foros de competencia del artículo 79.2, en contra del inciso imperativo que recoge ese mismo párrafo. Por lo tanto, cabe afirmar que los foros*

---

más significativa o los contactos con el objeto de la controversia. Estos principios están recogidos en la Section 145 of the Restatement (Second), Conflict of Laws, aprobado por el American Law Institute en 1971. El artículo 145 (1) establece que «los derechos y responsabilidades de las partes con respecto a una cuestión extracontractual son determinados por la ley del Estado que, con respecto a esa cuestión, tenga la relación más significativa con el hecho y las partes [...]». El párrafo 2 identifica entonces los contactos que deben tenerse en cuenta en un caso de responsabilidad civil para determinar la ley aplicable a una cuestión como a) el lugar donde ocurrió la lesión, b) el lugar donde ocurrió la conducta que causó la lesión, c) el domicilio, residencia, etc., de las partes en la acción, y d) el lugar donde se centra la relación, si la hay, entre las partes, estos contactos deben evaluarse en función de su importancia relativa con respecto al asunto en cuestión. Vid. OSTER, Jan, «Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights», en *International Review of Law, Computers & Technology*, vol. 26, n.º 2-3, Routledge, 2012, p. 120.

recogidos en el RGPD son complementarios a los recogidos por el reglamento «Bruselas I bis»[298] que explicamos a continuación:

1. *Sumisión expresa* (artículo 25 «Bruselas I bis»): es lo que se conoce como «una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional»[299]. El artículo 25 dicta que «si las partes, con independencia de su domicilio, han acordado que un órgano jurisdiccional o los órganos jurisdiccionales de un Estado miembro sean competentes para conocer de cualquier litigio que haya surgido o que pueda surgir con ocasión de una determinada relación jurídica, tal órgano jurisdiccional o tales órganos jurisdiccionales serán competentes». *El propio artículo pone como límite material a este mismo precepto la adecuación de la cláusula al derecho material de dicho Estado miembro, siendo esta una norma de conflicto uniforme para resolver todos estos casos e independiente del resto de un hipotético contrato.* En cuanto a los límites formales, el acuerdo atributivo de competencia *deberá celebrarse a) por escrito, o verbalmente con confirmación escrita, o b) en una forma que se ajuste a los hábitos que las partes tengan establecido entre ellas, permitiéndose en cualquiera de las formas anteriores materializarse mediante instrumentos electrónicos que permitan un registro duradero.*

2. *Sumisión t*ácita (artículo 26 «Bruselas I bis»). La siguiente conducta procesal de las partes significará que estamos ante una sumisión tácita: *cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial*[300]*; es decir, entra a discutir sobre el fondo del asunto.* Aunque en el caso de que, por razón de la materia, o por existir un acuerdo de sumisión expresa anterior al litigio, el demandado puede declinar la competencia mediante una declinatoria, dependiente del derecho procesal de cada Estado miembro. En España, *la declinatoria se regula en el artículo 39 de la LEC.*

---

[298] *Vid.* ALBRECHT, Jan Phillipp y JOTZO, Florian, *op. cit.,* pp. 127-128. Aunque se ha entendido que los fueros del RGPD plantean conflictos con las competencias exclusivas del reglamento «Bruselas I bis». *Cfr.* BRKAN, Maja, «Data Protection and European Private International Law», julio de 2015, *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, p. 23.

[299] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional de datos», en *Revista Boliviana de Derecho*, n.º 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013, p. 138.

[300] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional...», *op. cit.,* p. 139.

3. *Foro del domicilio del demandado* (artículo 4 «Bruselas I bis».) Este foro de competencia es un clásico de los instrumentos normativos de atribución de competencia. *A falta de pacto expreso o tácito, el criterio atributivo de competencia es el del domicilio del demandado, que hace competentes a los tribunales del domicilio del demandado.* El propio reglamento «Bruselas I bis» nos da una definición de domicilio en el artículo 63, que se entenderá que una *persona jurídica está domiciliada en el Estado en el que se encuentra: a) su sede estatutaria; b) su administración central; o c) su centro de actividad principal.* En cuanto a la residencia habitual de una persona física, *el artículo 62 nos remite a la ley interna del propio Estado*[301], puesto que el reglamento «Bruselas I bis» no nos aporta una noción autónoma del concepto. Aunque debemos resaltar la nula practicidad de este foro, puesto que genera muchos más perjuicios al propio demandante que al propio demandado, como el desconocimiento del idioma, los costes y las diferentes normas procesales aplicables.

4. *Foro especial en materia de obligaciones extracontractuales: el «lugar donde se hubiere producido o pudiere producirse el hecho dañoso»* (artículo 7.3 «Bruselas I bis»). Consiste en un foro especial regido por el principio de ubicuidad que en el caso de efectuar una acción por daños y perjuicios, el demandante tiene derecho a elegir entre los tribunales del lugar dónde se produjo el hecho dañoso (ya sea donde se haya producido el hecho generador del daño o donde se padezca el daño). Constituye la solución tradicional –y no siempre muy acertada– en esta materia[302]:

   a) El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej., el Estado donde se recaban los datos).

   b) O el del lugar en que se verifica el resultado dañoso (p. ej., el Estado donde se acceden a los datos).

---

[301] En el caso de España, el artículo 40 CC señala que «para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y en su caso, el que determine la Ley de Enjuiciamiento Civil».

[302] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional...», *op. cit.,* p. 142.

Estas situaciones dificultan la determinación del lugar donde se ha producido el hecho dañoso, que se manifiesta en dos preguntas:

1. ¿Cuál es el lugar donde *se produce el evento generador del daño?* Debemos responder esta pregunta en el sentido de será el Estado en que se ha difundido o tratado ilícitamente los datos.

2. ¿Cuál es el lugar donde se concreta el resultado lesivo? Aquí no hay una respuesta concreta, sino una multitud de posibilidades:

   a) el país desde donde se han introducido los datos;

   b) en el marco de Internet, el lugar donde está ubicado el servidor que los alberga;

   c) el país desde donde se puede tener acceso a los datos; o

   d) el país donde reside el titular del derecho infringido, que es, en definitiva, donde se ha producido el hecho dañoso;

   e) el país donde radique el fichero de datos.

Como hemos observado, este artículo se caracteriza *por una gran «dispersión competencial» que ataca directamente a la protección del titular del derecho a la protección de datos*. A este artículo contribuyó a esclarecer la competencia judicial relacionada con litigios derivados de ilícitos contra los derechos de la personalidad la STJUE *eDate Advertising,* derivada de la doctrina instaurada por la STJCE *Fiona Shevill*[303], que interpretaba el antiguo artículo 5.3 del reglamento «Bruselas I». La STJCE *Fiona Shevill* permitía –y sigue permitiendo– a la víctima de la vulneración del derecho a la intimidad por la difamación de datos personales publicados y accesibles en varios Estados miembros ejercer una acción resarcitoria contra el promotor de la acción que causa el hecho dañoso ante los tribunales del domicilio de tal persona para reclamar una indemnización íntegra, o bien demandar ante los tribunales de cada Estado miembro

[303] *Vid.* STJCE, 7 de marzo de 1995, Asunto C-68/03, *Ixora Trading Inc; Chequepoint SARL, Chequepoint International Ld. C Press Alliance SA* ECLI:EU:C:1995:61.

el que la publicación sea difundida, y en el que la víctima alegue haber sufrido un ataque contra su reputación. *La STJUE* eDate Advertising *viene a concretar y reducir esta «dispersión competencial» permitiendo que el afectado que alegue un daño o perjuicio en un Estado miembro exija una indemnización integral por todo el daño sufrido ante los tribunales del Estado promotor de la acción, y el Estado donde la víctima tenga su centro de intereses* (cuestión discutida anteriormente).

Visto esta disposición de foros otorgados por diferentes instrumentos normativos, algún autor ha sostenido que sería más apropiado regular las reglas de competencia judicial internacional en el reglamento «Bruselas I bis» en vez del propio RGPD para evitar así está complicada compatibilidad de foros disponibles establecida tanto por el reglamento «Bruselas I bis» como por el RGPD, y los problemas de litispendencia y conexidad del artículo 81 del RGPD para, a su vez, mantener coherencia entre ambos reglamentos[304].

Mientras que la jurisdicción general es «neutral», la jurisdicción específica al menos indica que ya hay algún tipo de conexión significativa entre el foro y la cuestión jurídica a decidir[305]. Podemos observarlo en los foros especiales del artículo 79.2 del RGPD en los que se permite demandar ante los tribunales del Estado en el que esté domiciliado algún establecimiento tanto del responsable como del encargado, o ante los tribunales del Estado de la residencia habitual del afectado por un supuesto tratamiento ilícito de los datos personales que genera una responsabilidad extracontractual. Estos foros estipulados por el RGPD están redactados para adecuarse al supuesto concreto. En cambio, los foros del reglamento «Bruselas I bis» tienen como objeto cubrir supuestos generales (p. ej., accidentes de circulación).

Debemos destacar que podemos encontrarnos, además de los supuestos del artículo 79 del RGPD y los propios de «Bruselas I bis», que tal perjuicio se materialice en el marco de una relación contractual, por lo que debemos atenernos a los foros concretos en materia contractual del reglamento «Bruselas I bis» (competencia especial en materia contractual del artículo 7.1); foros especiales de protección en materia de seguros de los

---

[304] *Vid*. BRKAN, Maja, «Data protection and European private international law: observing a bull in a China shop», en *International Data Privacy Law,* vol. 5, n.º 4, 2015, p. 275.

[305] *Vid.* VON HEIN, Jan, «Social Media and the Protection of Privacy», en *European Data Science Conference*, Luxemburgo, 2016, p. 24.

artículos 10-16; foros especiales de protección en materia de contratos celebrados por los consumidores de los artículos 17-19; y foros especiales de protección en materia de contratos individuales de trabajo de los artículos 20-23), y que pueden actuar con una doble función: *por un lado, establecer un foro de protección especial para la parte que ha sufrido el daño y perjuicio, en casos en los que una parte de una relación contractual es la parte débil, como en los contratos de seguro o celebrados por los consumidores; y por el otro, suplir la ausencia de unos foros especiales para los responsables del tratamiento cuando estos pretendan ejercitar alguna acción contra los afectados.*

CASO PRÁCTICO 6. Competencia judicial internacional del RGPD

El afectado, residente en Austria, pero con intereses económicos relevantes en Chequia, busca emprender la acción de responsabilidad del artículo 82 del RGPD por una difamación de datos personales que ha alcanzado a los países centroeuropeos ante el responsable del tratamiento, con domicilio en Polonia, y con establecimientos en Alemania, Países Bajos, Luxemburgo, Hungría y Francia. Partiendo de este supuesto, pueden darse varias situaciones:

a) Que las partes, ya habiendo nacido el conflicto, acuerdan someter el litigio ante los tribunales de un Estado miembro concreto *(Sumisión expresa. Artículo 25 del reglamento* «*Bruselas I bis*»).

b) Que el afectado demande en primer lugar en cualquier Estado miembro, y que el responsable decida discutir sobre el fondo del asunto *(Sumisión t*ácita. Artículo 26 *del reglamento «Bruselas I bis»).*

c) Que decida demandar en los Estados en los que el responsable posea un establecimiento *(Foro del establecimiento del responsable. Artículo 79.2 del RGPD).*

d) Que demande en su Estado de residencia *(Foro de la residencia habitual del demandante. Artículo 79.2 del RGPD).*

e) Que demande en los Estados donde se haya producido un daño efectivo: indistintamente en el Estado el promotor del daño (Polonia), en el lugar del centro de intereses (Chequia), o en tantos Estados donde se haya efectuado un daño *(Foro especial en materia de obligaciones extracontractuales: el «lugar donde se hubiere producido o pudiere producirse el hecho dañoso». Artículo 7.3 del reglamento* «*Bruselas I bis*» */ STJUE* eDate Advertising*).*

VII.2. COMPETENCIA JUDICIAL INTERNACIONAL DE OTROS INSTRUMENTOS NORMATIVOS DERIVADA DE LA CONSIDERACIÓN DE CONTRATO INTERNACIONAL DE SEGURO

El aumento de la internacionalización de las relaciones jurídicas ha conllevado también el incremento de la dimensión transfronteriza del sector asegurador. Por eso el legislador europeo ha realizado un proceso de armonización y unificación legislativa[306].

A la hora de enfrentarnos al estudio del contrato internacional de seguro, cabe tener en cuenta los siguientes elementos[307]:

a) Podemos encontrar varios elementos subjetivos en los que suele haber una parte más fuerte que la otra, como es el asegurador, frente a una parte más débil, como pueden ser el tomador, asegurado y beneficiario, y

b) Encontramos contratos de seguro en los que no existe parte débil, como los relativos a los grandes riesgos, por lo que se asemejan al resto de contratos internacionales.

En cuanto a las normas aplicables al contrato de seguro, son aplicables, respecto a la competencia judicial internacional: *1) el reglamento «Bruselas I bis» en el ámbito institucional; 2) el Convenio de Lugano de 2007 en el ámbito convencional, y 3) la LOPJ, cuando ninguna de las normas anteriores encaje en el ámbito de aplicación*[308].

El reglamento «Bruselas I bis» tiene como uno de sus objetivos principales la protección de la parte débil de los contratos de seguro mediante la disposición de normas más beneficiosas[309], puesto que no goza de la facultad de negociar las cláusulas del

---

[306] *Vid.* ESPLUGUES MOTA, Carlos (dir.), *Derecho del comercio internacional*, 7.ª edición, Tirant lo Blanc, 2016, p. 265.

[307] *Vid.* CARRASCOSA GONZÁLEZ, Javier y CALVO CARAVACA, Alfonso-Luis (dirs.), *Derecho internacional privado*, vol. II, 16.ª ed., Comares, Granada, 2016, p. 1058.

[308] No será de aplicación el Convenio de la Haya de 2005 sobre elección de foro, puesto que la Unión Europea efectuó una reserva respecto a la aplicación del Convenio a los contratos de seguro debido a que quiere preservar las normas recogidas en el reglamento «Bruselas I bis».

[309] *Vid.* Considerando 8.

contrato al ser económicamente más débil[310]. Partiendo de esta premisa, serán de aplicación los foros de la sección 3 del reglamento «Bruselas I bis», aparte de los foros contenidos en los artículos 6 y 7.5, en los que cabe encontrar: sumisión tácita, sumisión expresa y foros alternativos. Cabe decir que la aplicación de este reglamento solo será posible si las partes están domiciliadas en un Estado miembro. Esta posición ha sido criticada debido a la exclusión que ha realizado el legislador en el contrato de seguro en cuanto a la exigencia de que el asegurador esté establecido en la Unión, cuando los contratos de trabajo y de consumidores disfrutan de tal excepción[311]. Esta exclusión supone una incoherencia difícil de justificar, y que no hace más que mitigar la función protectora que busca el reglamento «Bruselas I bis» sobre la parte débil del contrato de seguro.

1. *Sumisión tácita (artículo 26.1).* Es destacable la existencia de la posibilidad de aplicar la sumisión tácita del artículo 26.1 a partir de la STJUE *Bilas,* C-111/09. Por lo que un tribunal de un Estado miembro, *a priori* incompetente, podrá obtener la competencia si 1) el demandado comparece ante el tribunal sin impugnar la competencia, 2) el tribunal pertenece a un Estado miembro y 3) en caso de que el demandado sea el tomador, asegurado o beneficiario, deberá ser informado de las consecuencias de su comparecencia o incomparecencia ante el órgano jurisdiccional. En el caso de que no exista la sumisión tácita, la competencia podrá ser atribuida por una cláusula expresa. La sumisión expresa se encuentra regulada, como norma general, en el artículo 25 del reglamento «Bruselas I bis», pero en materia de seguros, se aplicará el artículo 15, cuyos acuerdos no podrán ser contrarios a las disposiciones del artículo 25. Existen cinco supuestos de sumisión expresa válidas, constituyendo así una «autonomía limitada para elegir el tribunal competente»[312].

---

[310] *Vid.* STJCE C-201/82 *Gerling* vs. *Amministrazione del Tesoro dello Stato*, apartado 17.

[311] *Vid.* AGUILAR GRIEDER, Hilda, «Alcance de la regulación europea relativa a la competencia judicial internacional en materia civil y mercantil en el marco del nuevo reglamento "Bruselas I Bis" (1215/2012): una apuesta parcialmente frustrada», en *Revista Aranzadi doctrinal*, n.º 9, Aranzadi, Cizur Menor, 2015, pp. 13-15.

[312] *Vid.* CARRASCOSA GONZÁLEZ, Javier y CALVO CARAVACA, Alfonso-Luis (dirs.), *Derecho…*, *op. cit.*, p. 1062.

CASO PRÁCTICO 7. Supuesto de sumisión tácita

El afectado, también tomador del seguro, residente en Italia, busca emprender acciones legales ante el asegurador, con domicilio en Polonia, y sin ningún establecimiento en Italia. En el contrato de seguro rige una cláusula de sumisión expresa en el que acuerdan resolver las controversias en Alemania. El afectado decide demandar en Italia, pero pueden surgir determinados escenarios:

a) El asegurador decide comparecer en Italia y discutir sobre el fondo del asunto, lo cual significaría que la cláusula de sumisión desistiría a favor de la nueva atribución de competencia a los tribunales italianos.

b) El asegurador comparece en Italia, pero para declinar la competencia de los tribunales italianos a favor de los alemanes.

Si el demandado fuera el tomador, asegurado o beneficiario, solo valdría la sumisión tácita cuando el tribual informe al demandado de las consecuencias de la atribución de la competencia a este nuevo órgano.

2. *Sumisión expresa posterior al nacimiento del litigio (artículo. 15.1).* Esta situación se admite puesto que, como la controversia ya ha surgido, la parte débil es consciente de los riesgos de tal sumisión.

3. *Sumisión expresa anterior al nacimiento del litigio (artículo 15.2-15.5).*

   a) *Sumisión expresa mediante la oferta de foros adicionales a la parte débil demandante (artículo 15.2)*. Se admiten los acuerdos «que permitan al tomador del seguro, al asegurado o al beneficiario formular demandas ante órganos judiciales distintos de los indicados en la presente sección». Deben cumplirse determinadas condiciones:

      - El demandante debe ser tomador, asegurado o beneficiario.

      - La decisión de la parte débil, en relación con la ampliación de foros que estos disponen.

CASO PRÁCTICO 8. Sumisión expresa mediante la oferta de foros adicionales a la parte débil demandante

El afectado, también tomador del seguro, residente en Austria, busca emprender acciones legales ante el asegurador, con domicilio en Polonia, y sin ningún establecimiento en Austria. En el contrato de seguro rige una cláusula de sumisión expresa en la que estipula que, además de los foros del Estado de la residencia habitual del tomador (Austria), y del foro del Estado en el que está domiciliado el asegurador (Polonia), permite litigar en España, por lo que esto supone un aumento de los foros disponibles.

b) *Sumisión expresa a los tribunales del Estado miembro del domicilio o residencia común del tomador y asegurador (artículo 15.3)*. Se admitirán como válidas las sumisiones expresas «que, habiéndose celebrado entre el tomador y el asegurador, ambos domiciliados, o con residencia habitual en el mismo Estado miembro en el momento de la celebración del contrato, atribuyan, aunque el hecho dañoso se haya producido en el extranjero, competencia a los órganos jurisdiccionales de dicho Estado miembro, a no ser que la ley de este prohíba tales acuerdos». Las condiciones necesarias para acordar tal acuerdo son:

- Tanto tomador como asegurador deben estar domiciliados o tener la residencia habitual en el mismo Estado miembro.

- El tribunal del Estado miembro ha de ser común al domicilio o residencia habitual del tomador y asegurador.

- El acuerdo de sumisión expresa solo resulta vinculante para las dos partes, sin que pueda oponerse al asegurado-beneficiario que no haya aceptado la cláusula y tenga un domicilio en un Estado miembro diferente al de los anteriores[313].

[313] *Vid*. STJCE *Société financière et industrielle du Peloux* v *Axa Belgium*, C-112/03, apartado 43.

CASO PRÁCTICO 9. Sumisión expresa a los tribunales del Estado miembro del domicilio o residencia común del tomador y asegurador

El afectado, también tomador del seguro, residente en España, busca emprender acciones legales ante el asegurador, con domicilio en Reino Unido, y sin ningún establecimiento en España. En el momento de creación del contrato, ambas partes se encontraban residiendo en Reino Unido. En el contrato de seguro rige una cláusula de sumisión expresa en la que estipula que ambas partes podrán resolver sus competencias en el Estado en el que ambos residieron en el momento de la formación del contrato, en este caso, Reino Unido.

c) *Sumisión expresa celebrada con un tomador no domiciliado en un Estado miembro (artículo 15.4)*. El tomador no ha de estar domiciliado en un Estado miembro. Significa también que no existen vínculos fuertes con los tribunales de los Estados miembros. En esta situación, a un tomador le perjudicaría gravemente cualquier litigio en la Unión, pero el tomador es considerado parte débil y se le vincula al reglamento. Esta sumisión no puede referirse ni a un seguro obligatorio ni al de un inmueble sito en la Unión.

CASO PRÁCTICO 10. Sumisión expresa celebrada con un tomador no domiciliado en un Estado miembro

El afectado, también tomador del seguro, residente en Marruecos, busca emprender acciones legales ante el asegurador, domiciliado en Irlanda. Debido a esta situación, se acuerda que las controversias se resuelvan en territorio de la Unión, incluso si el daño está focalizado fuera de la Unión. Concretamente, el Estado miembro designado es Francia.

d) *Sumisión expresa en un contrato de seguro que cubre uno o varios riesgos del artículo 16 (artículo 15.5)*. Esos supuestos son los referidos a los grandes riesgos, como los daños a buques de navegación marítima, instalaciones costeras y en altamar o aeronaves, causados por hechos sobrevenidos en relación con su utilización para fines comerciales (artículo 16.1.a).

4. *Demandas del tomador, asegurado, o beneficiario contra el asegurador*. Cuando los sujetos débiles en esta relación jurídica buscan emprender determinadas acciones, el reglamento pone a su disposición dos foros aplicables, con independencia de la materia del propio seguro, y otros foros adicionales según la materia del seguro.

   a) *Foro del Estado miembro del domicilio del asegurador (artículo 11.1.a)*. Este foro opera cuando el demandado es el asegurador, y el tribunal competente será el del Estado miembro en el que se encuentre domiciliado el asegurador. Puede darse el caso de que el asegurador no esté domiciliado en un Estado miembro, según el artículo 63. El artículo 11.2 permite demandar a las sucursales, agencias, o cualquier tipo de establecimiento, con el mismo efecto que si el asegurador estuviera domiciliado en la Unión. Se mantiene así el mismo concepto flexible de «establecimiento» que hemos estudiado.

CASO PRÁCTICO 11. Foro del Estado miembro del domicilio del asegurado

El afectado, también tomador del seguro, residente en Rumanía, busca emprender acciones legales ante el asegurador, con domicilio en Bélgica. El asegurador tiene su sede principal en Bélgica, pero tiene varios establecimientos en España, Reino Unido, Francia y Portugal. Puesto que esos establecimientos se adaptan a los supuestos del artículo 63, el afectado podrá demandar en todos aquellos Estados en los que el asegurador tenga un establecimiento (Bélgica, España, Reino Unido, Francia y Portugal).

b) *Foro del lugar del domicilio del tomador, asegurado o beneficiario (artículo 11.1.b)*. Si estos sujetos se encuentran domiciliados en Estados miembros diferentes al del asegurador, pueden usar su propio domicilio como foro. Para delimitar el domicilio del tomador, asegurado o beneficiario se estará a los criterios de los artículos 62 (persona física)[314] y 63 (persona jurídica)[315].

5. *Demandas del asegurador contra el tomador, asegurado o beneficiario.* En estos supuestos, y al contrario de lo visto anteriormente, cuando el asegurador pretenda ejercer alguna acción contra ellos, los foros disponibles se reducen al foro del Estado miembro del domicilio del demandado, sea el tomador, asegurado o beneficiario del artículo 14.1, que será determinado según las normas de los artículos 62 y 63, en su caso.

CASO PRÁCTICO 12. Demandas del asegurador contra el tomador, asegurado o beneficiario

El asegurador, con domicilio en Luxemburgo, pretende ejercer acciones legales ante el asegurado, residente en Francia. El asegurador posee varios establecimientos repartidos por los Estados miembros, uno de ellos en Francia, que cumple el requisito del artículo 63. Por lo que el asegurador puede demandar en el Estado miembro en el que posea un establecimiento. En este sentido, puede demandar en Francia mediante su establecimiento en ese Estado.

---

[314] «Artículo 62:
1. Para determinar si una parte está domiciliada en el Estado miembro cuyos órganos jurisdiccionales conozcan del asunto, el órgano jurisdiccional aplicará su ley interna.
2. Cuando una parte no esté domiciliada en el Estado miembro cuyos órganos jurisdiccionales conozcan el asunto, el órgano jurisdiccional, para determinar si dicha parte lo está en otro Estado miembro, aplicará la ley de dicho Estado miembro».

[315] «Artículo 63:
1. A efectos del presente reglamento, se entenderá que una sociedad u otra persona jurídica está domiciliada en el lugar en que se encuentra:
a) su sede estatutaria;
b) su administración central; o
c) su centro de actividad principal.
2. Para Irlanda, Chipre y el Reino Unido, la expresión «sede estatutaria» se equiparará a la *registered office* y, en caso de que en ningún lugar exista una *registered office,* al *place of incorporation* (lugar de constitución) o, a falta de tal lugar, el lugar conforme a cuya legislación se haya efectuado la *formation* (creación) de la sociedad o persona jurídica».

6. *El foro para los casos de reconvención (artículo 14.2).* En el caso de una reconvención, el artículo 14 no establece ningún foro especial para ello, por lo que hay que acudir al artículo 8.3), que el tribunal que deberá reconocer de la demanda reconvertida será el tribunal del Estado miembro que conoce la demanda inicial, por lo que es posible que el tomador, asegurado o beneficiario sean demandados en Estados miembros en los que no tengan su domicilio.

CASO PRÁCTICO 13. Foro para los casos de reconvención

El afectado, también tomador del seguro, residente en los Países Bajos, busca emprender acciones legales ante el asegurador, con domicilio en Bélgica. Una vez ejercidas las acciones en el Estado en el que se encuentra domiciliado el asegurador (Bélgica), este decide reconvertir la demanda, por lo que efectuará esta acción ante los tribunales que conocieron inicialmente la demanda (Bélgica).

7. *Foro del artículo 7.5.* Este artículo permite demandar en otro Estado miembro si el litigio versa sobre la explotación de sucursales, agencias o cualquier otro establecimiento ante el órgano jurisdiccional en el que se hallen sitos. Este foro opera tanto para el asegurador, como para el tomador, asegurado o beneficiario.

8. *Contratos internacionales de seguro en el Convenio de Lugano de 2007.* Los foros establecidos en el Convenio de Lugano son los mismos que los establecidos en el reglamento «Bruselas I bis», que podemos resumir de forma esquemática para su mejor entendimiento en:

   a) *Foros de sumisión expresa* (artículo 13).

      - Sumisión expresa posterior al nacimiento del litigio (artículo. 13.1).

      - Sumisión expresa mediante la oferta de foros adicionales a la parte débil demandante (artículo 13.2).

      - Sumisión expresa a los tribunales del Estado miembro del domicilio o residencia común del tomador y asegurador (artículo 13.3).

- Sumisión expresa celebrada con un tomador no domiciliado en un Estado miembro, salvo si se tratase de un seguro obligatorio o se refiera a un inmueble sito en un Estado miembro (artículo 13.4).

- Sumisión expresa en un contrato de seguro que cubre uno o varios riesgos del artículo 14 (artículo 13.5).

b) *Demandas del tomador, asegurado o beneficiario contra el asegurador* (artículos 9 y 10).

- Foro del tribunal del Estado miembro donde el asegurador tuviera su domicilio (artículo 9.1.a).

- Foro del tribunal del Estado miembro donde el tomador, asegurado o beneficiario tuviera su domicilio (artículo 9.1.b).

- Foro del Estado miembro del domicilio del asegurado cuando tuviera establecimientos en los Estados miembros (artículo 9.2).

c) *Demandas del asegurador contra el tomador, asegurado o beneficiario* (artículo 12).

- Foro del Estado miembro del domicilio del demandado, sea el tomador, asegurado o beneficiario (artículo 12.1).

d) *Demandas formuladas indistintamente por el sujeto entre las partes*.

- Foro para los casos de reconvención (artículo 12.2).

- Foro especial para litigios sobre la explotación de establecimientos (artículo 5.5).

CASO PRÁCTICO 14. Contratos internacionales de seguro en el Convenio de Lugano de 2007

El afectado, también tomador del seguro, residente en Islandia, busca emprender acciones legales ante el asegurador, con domicilio en Noruega, además de disponer de establecimientos en el resto de Estados miembros de la Convención (Liechtenstein y los 28 Estados miembros de la Unión). Atendiendo a los foros alternativos que dispone el Convenio de Lugano de 2007, puede litigar en:

a) Foro del tribunal del Estado miembro donde el asegurador tuviera su domicilio (Noruega).

b) Foro del tribunal del Estado miembro donde el tomador, asegurado o beneficiario tuviera su domicilio (Islandia).

c) Foro del Estado miembro del domicilio del asegurado cuando tuviera establecimientos en los Estados miembros (Liechtenstein y los 28 Estados miembros de la Unión).

9. *Contratos internacionales de seguro en la LOPJ.* Las normas autónomas se limitan a otorgar la competencia a los tribunales propios de ese Estado, en concreto, se limita a atribuir la competencia a los tribunales españoles[316]; además, funcionan a modo subsidiario cuando ninguna norma tanto institucional como convencional sirven para resolver la competencia judicial internacional. El artículo 22 quinquies e) establece que «en materia de seguros, cuando el asegurado, tomador o beneficiario del seguro tuviera su domicilio en España, también podrá el asegurador ser demandado ante los tribunales españoles si el hecho dañoso se produjere en territorio español y se tratara de un contrato de seguro de responsabilidad o de seguro relativo a inmuebles, o, tratándose de un seguro de responsabilidad civil, si los tribunales españoles fueran competentes para conocer de la acción entablada por el perjudicado contra el asegurado en virtud de lo dispuesto en la letra b) de este artículo». La letra b) hace competentes a los tribunales españoles en material

[316] Tanto el reglamento «Bruselas I bis» como el Convenio de Lugano de 2007 determinan en sus artículos 6 y 4 respectivamente que si el demandado no se encuentra domiciliado en un Estado miembro, será la legislación interna quien determine la competencia.

de obligaciones extracontractuales si el hecho dañoso se ha producido en territorio español. En el último inciso del artículo señala que serán competentes los tribunales españoles cuando el tomador o asegurado sea demandante y la sumisión sea posterior al nacimiento de la controversia; y si fuera una sumisión expresa anterior al nacimiento, cuando ambas partes tuvieran ya su domicilio en España en el momento de celebración del contrato o el demandante fuera el asegurado o tomador del seguro.

CASO PRÁCTICO 15. Contratos internacionales de seguro en la LOPJ

El afectado, también tomador del seguro, residente en España, busca emprender acciones legales ante el asegurador, con domicilio en Argentina. Debido a que un ilícito en protección de datos el lugar donde se origina el daño suele coincidir con la residencia habitual del afectado, y el demandado no se encuentra vinculado por ningún instrumento internacional sobre competencia, los tribunales españoles serán competentes por el artículo 22 quinquies e).

VII.3. LEY APLICABLE A LA CONTROVERSIA

VII.3.1. Determinación de la ley aplicable a la acción de responsabilidad extracontractual del RGPD

La primacía de la legislación de protección de datos se manifiesta en «una limitada autonomía de la ley aplicable en una cláusula contractual, que siempre deberá atenerse a los criterios del RGPD en los casos de obligaciones contractuales, cuyas cláusulas pueden estar sujetas a las leyes de otro Estado según el Reglamento (CE) 594/2008 "Roma I"»[317]. Podemos tomar como ejemplo la STJUE *Amazon EU Sàrl*, que *determinó como abusivas cláusulas sobre ley aplicable cuando no se cumplían los requisitos del artículo 6.2 del reglamento «Roma II»*[318].

[317] DOCE L 177/6, 4 de julio de 2008.

[318] En este sentido se pronuncia la STJUE *Amazon EU Sàrl* (párrafo 71).

Pero hay supuestos de responsabilidad extracontractual –como es el caso de las transferencias internacionales de datos– *que plantean importantes problemas en cuanto al derecho aplicable. La ley que resuelve esta controversia es el Reglamento (CE) 864/2007 «Roma II»*[319].

El reglamento «Roma II» es un texto legal con *carácter universal*[320]; es decir, *la ley designada por el reglamento se aplica aunque no sea de un Estado miembro, la cual permite una mayor y mejor unificación del mercado anterior*[321], pero que excluye de su aplicación en su artículo 1.2.g) «las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación», por tanto, las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia del tratamiento de sus datos personales por un responsable o encargado están excluidas de la norma, exclusión muy criticada por la doctrina[322]. Debemos destacar que *actualmente existe una propuesta de reforma del reglamento «Roma II» en el que pretende incluir estos supuestos motivada por la STJUE* eDate Advertising[323], tendente a *unificar la norma de conflicto y desplazar a la legislación interna.*

Esto, a su vez, se traduce en una serie de *consecuencias positivas*[324]:

1. Las partes en un litigio privado internacional derivado de la vulneración del derecho fundamental a la protección de datos *no tendrán que conocer las normas de conflicto de los Estados miembros de la UE y su aplicación jurisprudencial, sino que podrán acudir a un régimen único.*

---

[319] DOCE L 199/40, 31 de julio de 2007.

[320] *Vid*. artículo 3.

[321] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos..., op. cit.,* p. 138.

[322] *Vid.* DICKINSON, Andrew, *The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008, p. 240; SANCHO VILLA, Diana, *Negocios internacionales de tratamiento de datos personales,* Navarra, Civitas, 2010, pp. 97-98; ORTEGA GIMÉNEZ, Alfonso, «La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español», en *Diario La Ley,* n.º 8661, La Ley, Madrid, 2015, p. 8; BRKAN, Maja, «Data Protection...», *op. cit.,* pp. 27-28, y DE MIGUEL ASENSIO, Pedro Alberto, «Competencia...», *op. cit.,* pp. 41-42.

[323] P7_TA-PROV(2012)0200.

[324] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Propuestas ante un futuro incierto para la protección en la Unión Europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto *vs.* armonización a través de unos principios comunes?», en *Revista Aranzadi Unión Europea*, n.º 10, Aranzadi, Cizur Menor, 2016, p. 9.

2. *Reducción de costes* para la persona perjudicada.

3. *Seguridad jurídica.* Se eliminaría un sistema donde los interesados utilicen la norma de conflicto para buscar la ley que les resulte más favorable *(lex shopping).*

4. *Se evitarían las desigualdades* entre el causante del daño y la persona perjudicada.

La reforma del reglamento «Roma II» incluye un nuevo artículo 5 bis en el que introduce dos nuevos supuestos: «la ley del país en el que se produzca o sea más probable que se produzca el elemento o los elementos más significativos del daño o perjuicio» o «la ley del país de residencia habitual del demandado, en su defecto, si el demandado no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país»[325].

El supuesto del primer inciso adopta los criterios de la *lex loci damni* (la ley del país en el que se produzca o sea más probable que se produzca el elemento o los elementos más significativos del daño) o *lex loci delicti commissi* (la ley del país en el que se produzca o sea más probable que se produzca el elemento o los elementos más significativos del hecho lesivo).

El segundo supuesto resulta más confuso, en el sentido de que, más que proteger al posible afectado, favorece a la parte fuerte del litigio[326]. Permite aplicar la ley del país de residencia del demandado cuando: a) resulte imposible determinar el elemento o los elementos más significativos del daño o perjuicio (elemento objetivo); y b) que el causante del daño no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país (elemento subjetivo).

---

[325] Una redacción similar la encontramos en el artículo 99 § 2. 1º del *Code de droit international privé* belga [C – 2004/09511] en los supuestos de daños contra los derechos de la personalidad, salvo que en este artículo permite la elección entre las dos opciones de la ley aplicable si el demandado no podía predecir que el daño se produciría en ese Estado: «en cas de diffamation ou d'atteinte à la vie privée ou aux droits de la personnalité, par le droit de l'Etat sur le territoire duquel le fait générateur ou le dommage est survenu ou menace de survenir, au choix du demandeur, à moins que la personne responsable n'établisse qu'elle ne pouvait pas prévoir que le dommage surviendrait dans cet Etat».

[326] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «La (des)protección...», *op. cit.,* p. 8.

La adición de este doble criterio a la hora de la determinación de la ley aplicable puede llegar a prejuzgar el caso en una fase muy temprana del proceso, además de favorecer al presunto responsable del daño con la opción de litigar con la ley del país de residencia.

La inclusión del futuro artículo 5 bis (que esperemos que se aplique con una debida reforma del texto) *debe ponerse en relación con el artículo 14 del reglamento «Roma II», que ofrece al perjudicado y al causante del daño la posibilidad de poder elegir la ley aplicable, en virtud del principio de autonomía de la voluntad. Aunque en la práctica es difícilmente aplicable, puesto que el acuerdo debe hacerse con posterioridad al hecho generador del daño,* en esos momentos es complicado que ambas partes se pongan de acuerdo. Pero la consecuencia de la no regulación conlleva a *la aplicación de normas autónomas como el artículo 10.9 del Código Civil,* que hace que apliquemos la ley del lugar donde se ha cometido el hecho *(lex loci delicti commissi)*[327]. La *lex loci delicti commissi* es una conexión de carácter territorial cuya aplicación en los supuestos ilícitos en los elementos constitutivos (acto y resultado) se encontraban en un mismo Estado[328]. Pero en este ámbito, la precisión del lugar en el que se produce el daño puede resultar controvertida en situaciones en las que las consecuencias lesivas del hecho dañoso no son de carácter material, y esta norma no precisa cuál es el lugar del daño en las situaciones en las que el hecho causal y el resultado lesivo se producen en distintos países[329].

El artículo 10.9 del CC nos otorga dos opciones para determinar la ley aplicable: *1) la aplicación de la* lex loci actus *(ley del Estado en el que se produce el hecho del que deriva la responsabilidad); o 2) la aplicación de la* lex loci damni *(aplicación de la ley del lugar donde se materializa el daño para las víctimas).* Esta doble interpretación –o ambigüedad– puede ser solventada mediante la separación de ambos criterios en la ley, como hacen algunos países de nuestro entorno[330].

---

[327] «Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven».

[328] *Vid.* VINAIXA MIQUEL, Mónica, *La responsabilidad civil por contaminación transfronteriza derivada de residuos*, Universidad de Santiago de Compostela, 2006, p. 147.

[329] *Vid.* DE MIGUEL ASENSIO, Pedro Alberto, *Derecho privado de Internet,* 4.ª ed., Civitas, Madrid, 2011, p. 201.

[330] P. ej., el artículo 62.1 de la LEGGE 31 maggio 1995, n.º 218. *Riforma del sistema italiano di diritto internazionale privato*, que estipula que las obligaciones extracontractuales se regirán por la ley del Estado en el que se haya producido el evento *(lex loci actus);* aunque el segundo inciso habilita al demandante a solicitar la aplicación de la ley del Estado en el que se haya producido el daño *(lex loci damni):* «1. La

En la primera opción *(lex loci actus),* el mayor problema que encontramos es *determinar cuál es el Estado en el que se ha realizado el hecho dañoso,* puesto que el hecho ilícito deriva de una cadena de hechos ilícitos que se suelen desarrollar en otros Estados, que debemos verificar el Estado donde refleja sus efectos lesivos; esto es, *el tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño*[331,332]. Entonces, para poder aplicar la legislación española, el responsable del fichero tuviera su domicilio fuera de la UE y el tratamiento de datos se hubiera realizado en España.

En cuanto a la segunda opción *(lex loci damni),* y en concreto en los supuestos de mero acceso, debe rechazarse que cualquier lugar de recepción de los contenidos o la información transmitidos por Internet sea por esa simple circunstancia de lugar del daño debido a 1) que muchas veces ese acto no genera un daño «real» al titular, y 2) la aplicación de la ley de cada uno de los múltiples lugares de manifestación del daño puede conducir a una excesiva fragmentación normativa[333]. Por eso se afirma que *el lugar donde se manifiesta la consecuencia directa para la víctima se corresponde con el lugar de su residencia habitual como el centro de las relaciones sociales, personales y económicas susceptibles de verse afectadas por un atentado contra la intimidad u otros derechos de la personalidad.* Como ya comentamos a raíz de la STJUE *eDate Advertising,* no solo se materializa el perjuicio en el Estado de residencia habitual, sino también en aquel Estado en el que existan un vínculo estrecho con ese otro Estado.

---

responsabilitá per fatto illecito é regolata dalla legge dello Stato in cui si é verificato l'evento. Tuttavia il danneggiato puó chiedere l'applicazione della legge dello Stato in cui si é verificato il fatto che ha causato il danno». Otros países con este mismo sistema son: Alemania (artículo 40 del *Einführungsgesetz zum Bürgerlichen Gesetzbuche*); Portugal (artículo 45 del *Código Civil*, que permite la aplicación de la ley del lugar donde se hay producido el daño, siempre y cuando: a) el autor del daño haya podido prever que su acto podría causar daños en ese Estado; y b) que la ley del Estado donde transcurre la actividad principal causante del daño no considere responsable al autor de ese daño); Países Bajos (artículo 3 de la *wet conflictenrecht onrechtmatige daad,* permitiendo aplicar la ley de un Estado en el que se manifiesten las consecuencias de un acto ilícito distinto al del que se hubiese producido el acto, siempre que el demandado no previese razonablemente la acción).

[331] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos..., op. cit.,* p. 143.

[332] Respecto al caso BGH NJW 2011, 2059 comentado anteriormente, el *Bundesgerichtshof* señaló explícitamente que la aceptación de la jurisdicción también conduciría a la aplicación del derecho alemán (artículo 40 (1) del EGBGB).

[333] *Vid.* DE MIGUEL ASENSIO, Pedro Alberto, *Derecho privado..., op. cit.*, p. 203.

Debido a los ya resaltados problemas, conviene que ahondemos en *una crítica al precepto*[334]:

1. La generalidad del precepto priva de visibilidad al problema de la desprotección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional.

2. Adolece de una rigidez relevante, puesto que solo ofrece al juzgador una opción meramente localizadora entre la aplicación de la ley del lugar donde se ha producido el hecho causal (país de origen) o la ley del lugar donde se manifiesta la acción (país o países de resultado), con la ambigüedad que ello supone.

3. La neutralidad de la norma. Cuando se arranca de una situación en la que una de las partes está en manifiesta inferioridad; la neutralidad, lejos de ser una virtud, se convierte en una potencial fuente de injusticia.

A todo esto, debemos resaltar las precisiones del RGPD, ya que *la tendencia que genera el artículo 79.2 de dicho reglamento invita a aplicar «la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado»*[335]. Su postura se basa en el *objetivo que tiene la norma de proteger al afectado, el cual una de las maneras de plasmarlo es la aplicación de un derecho que sea familiar al afectado que se corresponda con el del Estado de la residencia habitual (o del centro de intereses del afectado);* y que entendemos que esta deba ser la opción que mejor puede llegar a proteger los intereses del afectado en función del principio de *favor laesi*[336]. *Y en la práctica podemos prever que el demandante inicie las acciones en el Estado donde tenga su residencia habitual o su centro de intereses; de forma que se aplicará la ley del Estado que, entonces, asumió la competencia* (lex fori).

La aplicación de la *lex fori* conlleva una serie de beneficios[337]:

- *Reducir el tiempo y los costes de los litigios.*

- *Mejorar la calidad de los juicios.*

---

[334] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «La (des)protección...», *op. cit.,* p. 7.

[335] *Vid.* DE MIGUEL ASENSIO, Pedro Alberto, «Competencia...», *op. cit.,* p. 42.

[336] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Propuestas ante un futuro incierto para...», *op. cit.,* p. 6.

[337] *Vid.* VON HEIN, Jan, «Social Media and the Protection...», *op. cit.,* p. 23.

- *Tener en cuenta las preocupaciones de política pública del foro,* porque los derechos de la personalidad, la privacidad, la protección de datos, etc., están arraigados en los valores constitucionales.

El principal problema lo encontraríamos en el arraigo del *forum shopping,* siempre y cuando el reglamento «Roma II» no cubra los derechos de la personalidad.

CASO PRÁCTICO 16. Determinación de la ley aplicable

El afectado, residente en España, y con su centro de intereses en ese mismo país, busca emprender la acción de responsabilidad del artículo 82 del RGPD por una difamación de datos personales que ha alcanzado a países como Italia, Francia y Portugal, debido a la utilización del idioma de tales países para la difamación, ante el responsable del tratamiento, con domicilio en Austria, y con establecimientos en Alemania, Países Bajos, Luxemburgo, Hungría y Francia. El demandante ha decidido aplicar el foro de competencia del artículo 79.2 del RGPD en lo que respecta a la residencia del afectado, por lo que litigará en España. Puesto que no existe una norma ni institucional ni convencional, será de aplicación el artículo 10.9 del CC. 1) Si entendemos la *lex loci delicti commissi* como «la ley del lugar donde se materializa el daño para las víctimas» *(lex loci damni);* 2) nos atenemos a la tendencia generada por el RGPD de aplicar la «ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado», y vemos que el afectado no tiene intereses más allá de España, se aplicaría el derecho sustantivo español a la controversia.

VII.3.2. Determinación de la ley aplicable a la acción de responsabilidad contractual por el incumplimiento del contrato internacional de seguro

Respecto a la ley aplicable a los contratos de seguro, debido a su gran internacionalidad y dispersión normativa, supone uno de los elementos más complejos desde el punto de vista del derecho internacional privado[338]. Como adelantamos en el apartado

[338] *Vid*. AGUILAR GRIEDER, Hida, «Problemas de derecho internacional privado en la contratación de seguros: especial referencia a la reciente Directiva (UE) 2016/97 sobre la distribución de seguros», *Cuadernos de Derecho Transnacional*, vol. 9, n.º 2, Área de Derecho Internacional Privado UC3M, Madrid, 2017, p. 42.

anterior, las obligaciones contractuales tienen una regulación paralela. En cuanto a la ley aplicable, el instrumento de referencia es el Reglamento (CE) 593/2008 Roma I[339], y la Directiva (UE) 2016, centrándonos en la ley aplicable a los contratos internacionales de seguro que cubren otros riesgos distintos a los «grandes riesgos», que estén localizados en la Unión Europea.

El ámbito de aplicación de la ley reguladora del contrato, que resulta de lo dispuesto en los artículos 10.1, 12 y 18.1 del reglamento, se refiere en particular a[340]:

- la formación y la validez sustancial (artículo 10.1);
- la interpretación (artículo 12.1 a);
- el cumplimiento de las obligaciones derivadas de él (artículo 12.1 b);
- dentro de los límites de las competencias atribuidas al tribunal por la respectiva ley de procedimiento, las consecuencias del incumplimiento total o parcial de dichas obligaciones, incluida la evaluación del daño, en la medida en que esta evaluación esté regulada por la ley (artículo 12.1 c);
- las diversas causas de extinción de las obligaciones (artículo 12.1 d);
- las consecuencias de la invalidez del contrato (artículo 12.1 e);
- las presunciones legales y el reparto de la carga de la prueba (artículo 18.1).

En cuanto a la localización del riesgo, la ubicación del riesgo cubierto por el seguro asume una doble importancia en el reglamento. En primer lugar, delimita, en relación con los seguros de «riesgos de masa», el ámbito de aplicación del artículo 7. Segundo, es un elemento de conexión para la determinación del derecho aplicable a los seguros

---

[339] DOUE L 177/6, 4 de julio de 2008.

[340] DE LIMA PINHEIRO, Luis, «Sobre a lei aplicável ao contrato de seguro perante o Regulamento Roma I», *Cuadernos de Derecho Transnacional*, vol. 4, n.º 2, Área de Derecho Internacional Privado UC3M, Madrid, 2012, p. 204.

que cubren riesgos de masa situados en el territorio de los Estados miembros a falta de elección válida por las partes. Por lo tanto, se debe empezar por referirse a las normas aplicables a la localización del riesgo. La situación del riesgo no es un concepto fáctico, sino un concepto técnico-jurídico que debe interpretarse con normas jurídicas que expresan una valoración[341]. La finalidad que subyace de este artículo 7 es tuitiva respecto al asegurado, ya que el mismo responde claramente a un interés de protección del asegurado, tal como pone de manifiesto el considerando 32 del reglamento «Roma I». Otros intereses que subyacen son[342]:

1. Reducir la dispersión normativa existente en el marco del Convenio de Roma.

2. No modificar sustancialmente el régimen previsto en las directivas comunitarias sobre seguros, ya que, *de facto,* el contenido de tales directivas ha sido incorporado en el propio articulado del reglamento, en concreto, en su artículo 7.

Las normas que determinan la localización del riesgo se encuentran en los artículos 13 y 14 de la Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, sobre el seguro de vida, el acceso a la actividad de seguro y de reaseguro y su ejercicio (Solvencia II), remitidos por el artículo 7.6 del reglamento «Roma II»:

a) Si se trata de un seguro de vida, el riesgo se localiza en el país de compromiso, que se define como el país de residencia habitual del tomador (artículo 14).

b) En caso de seguros distintos al de vida, podemos encontrar cuatro reglas diferentes del tipo de seguro.

   - Si se trata de un seguro relativo a bienes inmuebles y su contenido, siempre que se encuentren cubiertos por la misma póliza de seguro, se considerará localizado en el Estado en el que estén sitos los bienes.

---

[341] *Ibidem*, p. 291.

[342] *Vid*. AGUILAR GRIEDER, Hida, «Problemas de derecho internacional privado en la contratación de seguros», *op. cit.,* p. 53.

- Si se trata de un seguro relativo a vehículos, el riesgo se considerará en el Estado de matriculación del vehículo.

- Si se trata de un seguro de duración igual o inferior a cuatro meses, que cubra riesgos sobrevenidos durante un viaje o vacaciones, el riesgo se situará en el Estado donde se suscribió la póliza.

- Si se trata de un seguro no enmarcable en los anteriores, el riesgo se situará en el Estado en el que resida el tomador.

El artículo 7.3. I regula un conjunto de normas de manera alternativa que las partes pueden elegir, existiendo así una «autonomía de la voluntad limitada»:

a) *La ley del Estado miembro en que se localice el riesgo en el momento del contrato (artículo 7.3.1.a).* Para localizar el riesgo, aplicamos la remisión del 7.6. Se debe atender a la localización del riesgo en el momento de celebración del contrato, por lo que un cambio posterior de la localización del riesgo no permite modificar la ley elegida.

CASO PRÁCTICO 17. Ley del Estado miembro en que se localice el riesgo en el momento del contrato

El tomador del seguro, residente en Irlanda en el momento del contrato, y actualmente residiendo en Bélgica, contrata un seguro de vehículo matriculado en Irlanda del Norte (RU) con un asegurador domiciliado en Alemania. Debido a que el riesgo se encuentra localizado en Reino Unido por haber sido matriculado el vehículo allí, la ley que regirá el contrato será la británica, en concreto, la de Irlanda del Norte.

b) *La ley del país donde el tomador del seguro tenga su residencia habitual (artículo 7.3.1.b).* Al referirse de forma genérica a la ley del país de la residencia del tomador, puede ser la de un tercer Estado (artículo 3). La residencia habitual se determina mediante el artículo 19, y aunque no se concrete el artículo 7.3.1.b) si se ha de tener en cuenta la residencia habitual del tomador en el momento de celebración del contrato, debemos considerar que sí por 1) la analogía 7.3.1.a) y 2) por el artículo 19.3. Un cambio posterior de residencia no modificará la ley aplicable.

CASO PRÁCTICO 18. Ley del país donde el tomador del seguro tenga su residencia habitual

El tomador del seguro, residente en Gales (RU), residiendo en el momento del contrato en Argentina, contrata un seguro de vehículo matriculado en España con un asegurador domiciliado en Italia. Debido a que la nacionalidad del tomador es la argentina, la ley que regirá el contrato será la argentina.

c) *En el caso de un seguro de vida, la ley del Estado miembro del que sea nacional el tomador del seguro (artículo 7.3.1.c).* Se caracteriza por ser un precepto muy ambiguo. Es necesario que el tomador posea la nacionalidad de algún Estado miembro. Al igual con la postura anterior, un cambio de nacionalidad no conllevaría a un cambio de la ley aplicable. En el caso de un tomador con múltiple nacionalidad, el reglamento «Roma I» no resuelve el problema. Podemos discutir entre tomar en cuenta la nacionalidad del Estado con vínculos más estrechos (criterio recogido en varios reglamentos europeos, y avalado por el STJUE)[343], o permitir que las partes pacten la ley aplicable, opción avalada por el principio de la autonomía de la voluntad.

CASO PRÁCTICO 19. Ley del Estado miembro del que sea nacional el tomador del seguro en un seguro de vida

El tomador del seguro, residente en Francia, con nacionalidad alemana, residiendo en el momento del contrato en España, contrata un seguro vida en España con un asegurador domiciliado en Croacia. Debido a que se cumplen los requisitos de ser un seguro de vida y tener la nacionalidad de un Estado miembro, la ley que regirá el contrato será la alemana.

d) *Por lo que respecta a los contratos de seguro que cubran riesgos limitados a siniestros que ocurran en un Estado miembro distinto del Estado miembro en que se sitúe el*

[343] Esta cláusula se suele aplicar como última opción para determinar la competencia judicial internacional. Por ejemplo, en el artículo 11 del Reglamento (UE) 650/2012, y en la STJUE *eDate Advertising* para permitir demandar en lugar diferente a la residencia habitual cuando el daño provocado se haya efectuado en un Estado miembro con estrecha vinculación con el afectado.

riesgo, la ley de dicho Estado miembro (artículo 7.3.1.d). Puesto que este supuesto se encuentra fuera del objeto de estudio, nos limitaremos a decir que será aplicable la ley del Estado miembro donde se produzca el siniestro.

e) *Cuando el tomador de un contrato de seguro cubierto por el presente apartado ejerza una actividad comercial o industrial o una profesión liberal y el contrato de seguro cubra dos o más riesgos que estén relacionados con dichas actividades y estén situados en Estados miembros diferentes, la ley de cualquiera de los Estados miembros en cuestión o la ley del país en el que el tomador del seguro tenga su residencia habitual (artículo 7.3.1.e).* En el mismo sentido que el anterior, nos limitamos a decir que existe una alternatividad de ley aplicable entre *la ley de cualquiera de los Estados miembros en cuestión* y *la ley del país en el que el tomador del seguro tenga su residencia habitual.*

El reglamento «Roma I» determina que «en los supuestos previstos en las letras a), b) o e), si los Estados miembros a los que dichos apartados se refieren conceden mayor libertad de elección en cuanto a la ley aplicable al contrato de seguro, las partes podrán hacer uso de tal libertad». Significa que el artículo 7.3.II admite un reenvío que opera en caso de que la ley a la que remiten las letras a), b) o e) conceda una mayor autonomía conflictual. Para que opere, deben darse las siguientes condiciones[344]:

- La norma de conflicto de la ley a la que remiten las letras a), b) o e) ha de permitir la elección de otras leyes.

- El reenvío solo se aplica a los supuestos de las letras a), b) o e).

- La ley a la que remiten debe ser de un Estado miembro.

Si en un caso concreto se consigue mayor autonomía mediante las opciones presentadas, el tribunal deberá escoger las leyes que exijan menos requisitos a la hora de permitir mayor libertad de elección de ley aplicable.

---

[344] *Vid.* CARRASCOSA GONZÁLEZ, Javier y CALVO CARAVACA, Alfonso-Luis (dirs.), *Derecho…*, *op. cit.*, p. 1080.

En defecto de ley aplicable, el artículo 7.3.III, el contrato se regirá por la ley del Estado miembro donde esté localizado el riesgo. Para ello, volvemos a hacer mención de la remisión del artículo 7.6.

Cabe decir que nuestra LCS dispone de un régimen propio de ley aplicable cuando no sea posible determinar la ley aplicable mediante instrumentos institucionales o convencionales en los artículos 107 y 108 de la LCS. El primero trata sobre la ley aplicable a los contratos de seguro de daños. Se aplicará la ley española:

a) Cuando se refiera a riesgos que estén localizados en territorio español y el tomador del seguro tenga en él su residencia habitual, si se trata de persona física, o su domicilio social o sede de gestión administrativa y dirección de los negocios, si se trata de persona jurídica.

b) Cuando el contrato se concluya en cumplimiento de una obligación de asegurarse impuesta por la ley española.

Fuera de los casos anteriores, regirán las siguientes normas para determinar la ley aplicable al contrato de seguro contra daños:

a) Cuando se refiera a riesgos que estén localizados en territorio español y el tomador del seguro no tenga en él su residencia habitual, domicilio social o sede de gestión administrativa y dirección de los negocios, las partes podrán elegir entre la aplicación de la ley española o la ley del Estado en que el tomador del seguro tenga dicha residencia, domicilio social o dirección efectiva.

b) Cuando el tomador del seguro sea un empresario o un profesional y el contrato cubra riesgos relativos a sus actividades realizadas en distintos Estados del Espacio Económico Europeo, las partes podrán elegir entre la ley de cualquiera de los Estados en que los riesgos estén localizados o la de aquel en que el tomador tenga su residencia, domicilio social o sede de gestión administrativa y dirección de sus negocios.

c) Cuando la garantía de los riesgos que estén localizados en territorio español se limite a los siniestros que puedan ocurrir en un Estado miembro del Espacio Económico Europeo distinto de España, las partes pueden elegir la ley de dicho Estado.

En cuanto a la localización del riesgo, el artículo 107.4 nos remite al artículo 1.3 d), de la ley de Ordenación y Supervisión de los Seguros Privados, que son:

1.º Aquel en que se hallen los bienes, cuando el seguro se refiera a inmuebles, o bien a estos y a su contenido, si este último está cubierto por la misma póliza de seguro. Cuando el seguro se refiera a bienes muebles que se encuentren en un inmueble, y a efectos de los tributos y recargos legalmente exigibles, el Estado miembro en el que se encuentre situado el inmueble, incluso si este y su contenido no estuvieran cubiertos por la misma póliza de seguro, con excepción de los bienes en tránsito comercial.

2.º El Estado miembro de matriculación, cuando el seguro se refiera a vehículos de cualquier naturaleza.

3.º Aquel en que el tomador del seguro haya firmado el contrato, si su duración es inferior o igual a cuatro meses y se refiere a riesgos que sobrevengan durante un viaje o fuera del domicilio habitual del tomador del seguro, cualquiera que sea el ramo afectado.

4.º Aquel en que el tomador del seguro tenga su residencia habitual o, si fuera una persona jurídica, aquel en el que se encuentre su domicilio social o sucursal a que se refiere el contrato, en todos los casos no explícitamente contemplados en los apartados anteriores.

La ley debe pactarse en el contrato, a falta de elección, se regirá por la ley del Estado que presente un vínculo más estrecho en función de los supuestos del párrafo 3. Sin embargo, si una parte del contrato fuera separable del resto del mismo y presentara una relación más estrecha con algún otro Estado de los referidos en este número, podrá, excepcionalmente, aplicarse a esta parte del contrato la ley de ese Estado. Se presumirá que existe relación más estrecha con el Estado miembro del Espacio Económico Europeo en que esté localizado el riesgo.

En cuanto a los seguros de vida, la ley aplicable se regula por el artículo 108 de la LCS, que se aplicará cuando:

a) El tomador del seguro sea una persona física y tenga su domicilio o su residencia habitual en territorio español. No obstante, si es nacional de otro Estado miembro del Espacio Económico Europeo distinto de España, podrá acordar con el asegurador aplicar la ley de su nacionalidad.

b) El tomador del seguro sea una persona jurídica y tenga su domicilio, su efectiva administración y dirección o su principal establecimiento o explotación en territorio español.

c) El tomador del seguro sea una persona física de nacionalidad española con residencia habitual en otro Estado y así lo acuerde con el asegurador.

d) El contrato de seguro de grupo se celebre en cumplimiento o como consecuencia de un contrato de trabajo sometido a la ley española.

CONCLUSIONES

Primera. El Big Data, *en tanto en cuanto se nutre de los datos personales, presenta serios retos en cuanto a protección de datos se refiere.* El uso constante de categorías especiales de datos en estos servicios pone en grave peligro la privacidad de los sujetos. Pero el *Big Data* no solo afecta jurídicamente a la protección de datos. A lo largo del trabajo hemos constatado que las implicaciones legales afectan, por un lado, a los mecanismos aplicados a los datos que permiten obtener un resultado (algoritmo), en cuanto a las posibilidades jurídicas de defensa del algoritmo, que se ha mostrado el secreto comercial como mejor medio para su defensa, en detrimento de la propiedad industrial y propiedad intelectual, y por el otro, a las bases de datos creadas por las empresas aseguradoras, que hemos visto que su defensa jurídica se basa en el derecho de propiedad intelectual.

Segunda. El Big Data *no es una herramienta de futuro, lo es también de presente.* El uso de los datos permite a las aseguradoras crear coberturas a medida para adaptarse a un mercado cada vez más personalista y heterogéneo, además de otorgar los medios necesarios para la prevención del fraude. Pero esta «personalización del producto» es una hoja de doble filo, puesto que el *Big Data* es característico por la elaboración de perfiles de sus usuarios, que puede traer graves efectos colaterales para otros posibles clientes, ya que la elaboración de perfiles prejuzga las características personales de un individuo con el fin de tomar una decisión sobre si llevar a cabo tal negocio jurídico.

Tercera. Se sigue sin considerar como «sensibles» los datos sobre geolocalización. El RGPD sigue la misma senda que la Directiva 95/46/CE al entender que esta categoría de datos no revela datos sensibles, cuando ha sido demostrado por el propio CEPD y la AEPD que la geolocalización puede revelar datos sensibles como tendencias ideológicas, sexuales o relacionadas con la salud. Debido a que la ley sigue sin corregirlo, se ve necesario que la jurisprudencia adopte la perspectiva que aquí defendemos para que los titulares del derecho a la protección de datos recuperen el control de sus datos.

Cuarta. La anonimización total es imposible. El análisis de las diferentes técnicas recomendadas por el CEPD y las propias conclusiones del grupo revelan que la anonimización absoluta es una utopía y que siempre existe el riesgo latente de una revelación de datos personales. Por ello el RGPD ha asumido tal posición y permite no someter los datos a la legislación sobre datos personales cuando «razonablemente» se haya comprobado que con *los medios existentes no sea posible identificar al usuario*.

Quinta. La sujeción del Big Data a la norma está asegurada. El legislador ha observado los problemas de aplicación de la ley de Protección de Datos a los supuestos actuales planteados con la Directiva 95/46, que se veía superada por el avance de nuevas tendencias tecnológicas como el *Big Data,* el *Cloud Computing* o el *Internet of Things*; cuyas tendencias están marcadas por la deslocalización del tratamiento de los datos. El nuevo artículo 4 RGPD trata este fenómeno con la obligatoriedad de la aplicación de la legislación europea cuando los datos tratados en terceros países involucren a residentes de la Unión, además de contemplar un supuesto específico dedicado al *Big Data* en el artículo 4.2 b), que no entendemos la exclusión que realiza la doctrina en cuanto a la aplicación de este supuesto a los productos o servicios diferentes a los servicios de Internet. Con este nuevo artículo, 1) se asegura que los datos de los ciudadanos de la Unión estén protegidos incluso más allá del territorio y 2) se protegen los tratamientos de datos que controlen el comportamiento, objeto del *Big Data*.

Sexta. La fórmula para otorgar el consentimiento se endurece para no dar lugar al consentimiento tácito. La inclusión en la redacción de medios busca disipar las dudas respecto al consentimiento afirmativo del afectado al tratamiento de sus datos, más cuando en el contrato de seguro intervienen datos relacionados con la salud, que están bajo el máximo nivel de protección. Aunque las palabras que se han usado para redefinir el concepto no resuelvan con toda firmeza esta cuestión. Esto se demuestra en las condiciones para el tratamiento ulterior de datos para fines diferentes a los que se destinaron para recabar los datos.

Séptima. Las cláusulas contractuales tipo no se presentan como opción segura para la transferencia internacional de datos. Aunque hayan ascendido como alternativa frente a la derogación de la decisión del *Safe Harbour,* en la propia STJUE que derogó

la decisión cuestionaba también la posible legalidad de las cláusulas contractuales tipo. Debido a ello, la Comisión Europea reformó las decisiones relativas a tales cláusulas con el fin de evitar la posible derogación que busca la autoridad irlandesa de protección de datos y Max Schems en un litigio contra Facebook en Irlanda ante la *High Court*. Las hipotéticas derogaciones de las decisiones de ejecución de las cláusulas supondrían la ruptura de otro de los pilares que sustentan las transferencias internacionales de datos.

Octava. Las normas corporativas vinculantes se alzan como la medida «estrella» de las transferencias internacionales. El RGPD ha normativizado por completo las transferencias internacionales de datos con el objetivo de homogeneizar la regulación en los Estados miembros. Podemos destacar en concreto la prerrogativa de la Comisión Europea de estipular mediante una decisión de ejecución determinados procedimientos respecto de las normas corporativas vinculantes. Como consecuencia, las instituciones europeas eliminan la ya de por sí reducida autonomía de la que disfrutaban las empresas, para asemejarse más al modelo de las cláusulas contractuales tipo, que se rigen fundamentalmente de las decisiones de la Comisión.

Novena. El Privacy Shield *sigue presentando riesgos para la privacidad.* La aprobación de la Decisión de Ejecución 2016/1250 ha comportado un aumento de la protección de las transferencias internacionales de datos a Estados Unidos respecto al *Safe Harbour,* pero tal aumento de protección no ha resultado ser tan convincente como se esperaba, y más con la entrada de la nueva Administración estadounidense y las reformas emprendidas por ella para limitar el ámbito de aplicación de la ley de Protección de Datos estadounidense. El último ataque ha provenido del Parlamento Europeo mediante una resolución en la que instaba a su derogación. Los ataques bidireccionales al escudo no hacen más que debilitarlo y mostrar las carencias que protege.

Décima. La estipulación de un régimen específico del derecho a la indemnización por daños y perjuicios supone un gran avance para la protección del individuo. El nuevo régimen supera con creces la regulación contenida en la Directiva 95/46, y unifica al máximo las disposiciones que deben cumplir los Estados miembros. La adición de indemnizar los daños inmateriales supone la culminación de una doctrina jurisprudencial europea que ya venía reconociendo los daños morales como un elemento más de la

indemnización. A esto, hay que sumarle los nuevos criterios otorgados por nuestro Tribunal Supremo, que añaden seguridad jurídica a la cuestión. El nuevo Proyecto de LOPD de 2017 extiende la responsabilidad solidaria al propio representante del responsable en el territorio europeo, por lo que supone además otro sujeto al que el afectado puede dirigirse para obtener una indemnización efectiva.

Undécima. El sistema de derecho internacional privado que instaura el RGPD cumple «a medias» la función protectora que debe tener el titular del derecho fundamental a la protección de datos. El nuevo RGPD ha demostrado tener una función clara: facilitar al afectado poder efectuar sus derechos en el Estado miembro que desee, en especial, en el propio Estado de residencia del afectado. La compatibilidad de foros con el reglamento «Bruselas I bis» permite suplir la falta de foros especiales para el responsable-asegurador, aparte de añadir una mayor disposición de foros para el afectado. Aunque esta dualidad normativa crea un efecto complejo de interpretación entre ambos textos, cuyo problema pudo haberse resuelto trasladando las cuestiones relacionadas con la competencia judicial internacional al reglamento «Bruselas I bis». Debemos lamentar la inexistencia de avances en cuanto a la determinación de la ley aplicable en los casos de ejercicio de la acción del artículo 82 del RGPD, que nos sigue llevando a una aplicación heterogénea de las normas autónomas de los diferentes Estados miembros de la Unión Europea que, en nuestro caso, se sigue rigiendo por la *lex loci delicti commissi*. Por eso se debe avanzar en una norma de conflicto unificada a través de la modificación del reglamento «Roma II» que estipule una norma de conflicto que favorezca a la parte débil del litigio en función del *favor laesi,* como es la persona perjudicada, como la ley del Estado de residencia habitual del afectado o del «centro de intereses de la víctima».

ANEXO

FAQ *«BIG DATA,* ÁMBITO ASEGURADOR Y PROTECCIÓN DE DATOS»

1. **¿Qué es el *Big Data*?** El análisis de macrodatos de calidades variadas derivados de diversas fuentes que fluctúan a gran velocidad mediante los sistemas informáticos adecuados, con el objetivo de obtener un valor añadido en los productos ofrecidos.

2. **¿Una aseguradora puede aplicar el *Big Data*?** Sí. El *Big Data* en el negocio asegurador está empezando a aplicarse, por lo que no todas las aseguradoras utilizan esta tecnología. Es, pues, el mejor momento para llevar a cabo su práctica.

3. **¿En qué beneficia el *Big Data* al negocio asegurador?** 1) en la creación de pólizas «a medida» según el riesgo real presentado por el asegurado mediante el estudio de los datos que genera y 2) en la prevención del fraude mediante el estudio de casos pasados y estableciendo modelos predictivos.

4. **¿Qué tipos de datos aportan más valor?** Debemos destacar tres categorías: 1) datos biométricos, 2) datos de geolocalización, y 3) datos relativos a la salud.

5. **¿Qué es un algoritmo?** Son procesos lógicos formados por una serie de instrucciones o reglas que permiten resolver problemas partiendo de unos datos de entrada, mediante la obtención de unos datos de salida.

6. **¿El algoritmo se puede proteger?** Sí, aunque su protección hasta ahora es muy débil. El mejor método para hacerlo es mediante el secreto comercial del artículo 13 de la ley de Competencia Desleal.

7. **¿Las bases de datos se pueden proteger?** Sí, mediante la propiedad intelectual, que otorga dos medios de defensa: 1) el derecho *sui generis* propio de las bases de datos de los artículos 133-137 LPI, y 2) el derecho de autor del artículo 12.

8. **¿Qué es un dato personal?** Aquel que permita que una persona pueda ser identificada o la identifique.

9. **¿Qué es el consentimiento?** Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el afectado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

10. **¿El consentimiento ha cambiado?** El consentimiento tácito ha dejado de tener validez y esa es la principal diferencia. Por lo demás, en aquellos contratos de seguro donde estuvieran presente datos de salud, el consentimiento no ha cambiado ya que la cesión de dichos datos debe hacerse de forma explícita.

11. **¿Quién debe probar el consentimiento?** La carga de la prueba recae siempre sobre el responsable o encargado, por lo que siempre es la entidad aseguradora que recaba los datos la que deberá probar que obtuvo los datos personales de manera lícita.

12. **¿Tengo que aplicar la legislación sobre protección de datos siempre?** No. Solo se aplican sobre los datos personales, los datos anónimos quedan al margen de su aplicación, pero el proceso de anonimización de datos no garantiza unos datos 100 % anónimos.

13. **¿Qué es una transferencia internacional de datos?** Una comunicación o cesión de datos personales, tratados de forma automatizada o no, a un responsable o encargado establecido en un tercer país respecto de la Unión Europea.

14. **¿Cuándo es posible realizar una transferencia internacional de datos?** Las transferencias internacionales están prohibidas como norma general, pero pueden ser efectuadas bajo determinadas situaciones: 1) cuando la Comisión Europea haya decidido que el país al que se vayan a transferir los datos sea seguro; 2) mediante un contrato entre encargados o responsables con las debidas garantías; 3) mediante la adopción de unas reglas corporativas jurídicamente vinculantes cuando la transmisión se realice entre empresas del mismo grupo.

15. **¿Qué son las normas corporativas vinculantes?** Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento

establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

16. **¿Es posible realizar transferencias internacionales a Estados Unidos?** Sí, pero la decisión no afecta a todo el país. Solo se podrán realizar transferencias sin necesidad de una autorización por parte de la autoridad de protección de datos a las empresas que estén certificadas.

17. **¿Dónde puede demandar un afectado por un mal uso de sus datos personales?** Depende del instrumento normativo, y si no se acuerda en el contrato, puede resumirse en que el afectado podrá demandar en: 1) el Estado en el que el *responsable* o encargado tenga un establecimiento (pudiendo coincidir con el domicilio del asegurador); 2) el Estado de residencia del afectado (siendo el beneficiario, asegurado o tomador).

18. **¿Cuál es la naturaleza de la acción indemnizatoria contenida en el RGPD?** La naturaleza de la acción responde a una situación de responsabilidad extracontractual, por lo que no será necesario que el ilícito se efectúe en un marco contractual. Sin embargo, es común que las entidades aseguradoras y las empresas en general se comprometan contractualmente a proteger los datos según la legislación vigente, por lo que también cabe exigir una responsabilidad por incumplimiento contractual.

19. **¿Cuál será la ley aplicable a la controversia por responsabilidad extracontractual?** La ley aplicable coincidirá con la ley del Estado en el que se haya producido el daño, generalmente, en el Estado de la residencia habitual.

20. **¿Cuál será la ley aplicable a la controversia por responsabilidad contractual?** La ley variará según la naturaleza del seguro y de las características personales de las partes.

BIBLIOGRAFÍA

AEPD, *Orientaciones y garantías en los procedimientos de anonimización de datos personales,* AEPD, 2016.

AGUILAR GRIEDER, Hilda, «Alcance de la regulación europea relativa a la competencia judicial internacional en materia civil y mercantil en el marco del nuevo reglamento "Bruselas I Bis" (1215/2012): una apuesta parcialmente frustrada», en *Revista Aranzadi doctrinal*, n.º 9, Aranzadi, Cizur Menor, 2015.

AGUILAR GRIEDER, Hilda, «Problemas de derecho internacional privado en la contratación de seguros: especial referencia a la reciente Directiva (UE) 2016/97 sobre la distribución de seguros», *Cuadernos de Derecho Transnacional,* vol. 9, n.º 2, Área de Derecho Internacional Privado UC3M, Madrid, 2017.

ALBRECHT, Jan Philipp, «How the GDPR Will Change the World», en *European Data Protection Law Review,* vol. 2, n.º 3, Lexxion, Berlín, 2016.

ALBRECHT, Jan Phillipp y JOTZO, Florian, *Das neue Datenschutzrecht der EU,* Baden-Baden, Nomos, 2017.

ALCAIDE CASADO, Juan Carlos, *Fidelización de clientes,* 2.ª ed., ESIC, Madrid, 2015.

ALE, Ben, «Risk analysis and big data», en *Safety and Reliability,* vol. 36, n.º 3, Taylor & Francis, 2016.

ALEXIN, Zoltán, «Does fair anonymization exist?», en *International Review of Law, Computers & Technology,* vol. 18, n.º 1, Routledge, 2014.

ÁLVAREZ HERNANDO, Javier y CAZURRO BARAHONA, Víctor, *Practicum Protección de datos 2016,* Aranzadi, Cizur Menor, 2015.

ÁLVAREZ LATA, Natalia, *Cláusulas restrictivas de responsabilidad civil,* Comares, Granada, 1998.

BATISDA FREIJEDO, Francisco José, *Teoría general de los derechos fundamentales en la Constitución Española de 1978,* Tecnos, Madrid, 2004.

BELTRÁN AGUIRRE, Juan Luis, «La protección de los datos personales relacionados con la salud», en *Jornada sobre Protección de Datos Personales,* Defensor del Pueblo de Navarra-INAP, Navarra, 2012.

BERNAL RIOBOO, Lourdes, «Diccionario de conceptos relativos a la protección de datos», en *Diario La Ley*, n.º 6921, La Ley, Madrid.

BOLOGA, Ana-Ramona, BOLOGA, Razvan y FLOREA, Alexandra, «Big Data and Specific Analysis Methods for Insurance Fraud Detection», en *Database Systems Journal,* vol. I, n.º 1, The Bucharest University of Economic Studies, Bucarest, 2010.

BOOBIER, Tony, *Analitics for Insurance,* WILEY, Chichester (RU), 2016.

BRKAN, Maja, «Data protection and conflict-of-laws: a challenging relationship», en *European Data Protection Law Review,* vol. 2, n.º 3, 2016.

BRKAN, Maja, «Data Protection and European Private International Law», *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, julio de 2015.

BU-PASHA, Shakila, «Cross-border issues under EU data protection law with regards to personal data protection», en *Information & Communications Technology Law,* Taylor & Francis, 2017.

BÜHLMANN, Peter, DRINEAS, Petros, KANE, Michael y VAN DER LAAN, Mark, *Handbook of Big Data*, CRC Press, 2016.

BUSTO LAGO, José Manuel, «La responsabilidad civil de los servidores y operadores de datos», en *Seminario sobre Protección de Datos*, UCLM, Ciudad Real, 2005.

BUTTARELLI, Giovanni, *Banche dati e tutela della riservatezza (La* privacy *nella Società dell'Informazione)*, Giuffrè Editore, Milán, 1997.

CARRASCOSA GONZÁLEZ, Javier y CALVO CARAVACA, Alfonso-Luis (dirs.), *Derecho internacional privado,* vol. II, 16.ª ed., Comares, Granada, 2016.

CISCO, «Cisco Visual Networking Index: Forecast and Methodology, 2015-2020», 2014.

CONESA CARALT, Jordi (coord.) y CURTO DÍAZ, Josep, *Introducción al Business Intelligence,* Editorial UOC, Barcelona, 2012.

DAVARA FERNÁNDEZ DE MARCOS, Isabel, *Hacia la estandarización de la protección de datos personales,* La Ley, Madrid, 2011.

DAVARA RODRÍGUEZ, Miguel Ángel, «*Big Data*», en *El Consultor de los Ayuntamientos,* n.º 15, Wolters Kluwer, Madrid, 2013.

DAVARA RODRÍGUEZ, Miguel Ángel, *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones,* Fundación VODAFONE, Madrid, 2004.

DE LIMA PINHEIRO, Luís, «Sobre a lei aplicável ao contrato de seguro perante o Regulamento Roma I», *Cuadernos de Derecho Transnacional*, vol. 4, n.º 2, Área de Derecho Internacional Privado UC3M, Madrid, 2012.

DE MIGUEL ASENSIO, Pedro Alberto, «Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del tribunal de justicia», en *La Ley Unión Europea*, La Ley, Madrid, n.º 31, 2015.

DE MIGUEL ASENSIO, Pedro Alberto, «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», en *Revista Española de Derecho Internacional*, vol. 69, n.º 1, Madrid, 2017.

DE MIGUEL ASENSIO, Pedro Alberto, «La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google», en *Diario La Ley,* n.º 8773, La Ley, Madrid, 2016.

DE VERDA Y BEAMONTE, José Ramón, «Las cláusulas de exoneración y limitación de responsabilidad en el derecho español», en *Revista Chilena de Derecho Privado*, n.º 4, Universidad Diego Portales, Santiago, 2005.

DEL PESO NAVARRO, Emilio, RAMOS GONZÁLEZ, Miguel Ángel, DEL PESO RUIZ, Margarita y DEL PESO RUIZ, Mar, *Nuevo Reglamento de Protección de Datos de Carácter Personal: medidas de seguridad,* Díaz de Santos, Madrid, 2012.

DELOITTE, *Big Data, Big Brother? Striking the right balance with privacy,* 2015.

DÍAZ DÍAZ, Efrén, «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», en *Revista Aranzadi Doctrinal*, n.º 6, Aranzadi, Cizur Menor, 2016.

DICKINSON, Andrew, *The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008.

DÖRR, Dieter y WEAVER, Russell (eds.), *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries,* De Gruyter, Berlín, 2015.

ECHEBARRÍA SÁENZ, Joseba Aitor (coord.), *El comercio electrónico,* EDISOFER, Madrid, 2001.

EL EMAM, Khaled y ÁLVAREZ, Cecilia, «A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques», en *International Data Privacy Law Journal*, vol. 5, n.º 1, Oxford University Press, Oxford, 2015.

ELIAS, Howard, «El desafío de *Big Data:* cómo desarrollar una estrategia ganadora», *CIO*, julio de 2012.

ERDOZÁIN LÓPEZ, José Carlos, «La protección de los datos de carácter personal en las telecomunicaciones», en *Revista Doctrinal Aranzadi Civil-Mercantil,* n.º 1, Aranzadi, Cizur Menor, 2007.

ESPLUGUES MOTA, Carlos (dir.), *Derecho del comercio internacional,* 7.ª edición, Tirant lo Blanc, 2016.

GANDOMI, Amir y HAIDER, Murtaza, «Beyond the hype: Big data concepts, methods, and analytics», en *International Journal of Information Management,* n.º 35, Elsevier, Ámsterdam, 2015.

GARCÍA NOBLIA, Analore, «¿Realmente cambiará el consentimiento el Reglamento Europeo?», en *Noticias Jurídicas,* noviembre de 2016.

GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación obicua,* Dykinson, Madrid, 2016.

GEIST, Michael, «Is There a There There? Toward Greater Certainty for Internet Jurisdiction», *Berkeley Technology Law Journal,* vol. 16, n.º 3, California, 2001.

GIL GONZÁLEZ, Elena, «*Big Data* y datos personales, ¿es el consentimiento la mejor manera de proteger nuestros datos?", *Diario La Ley*, n.º 9050, La Ley, Madrid, 2017.

GIL GONZÁLEZ, Elena, *Big Data, privacidad y protección de datos,* AEPD, Madrid, 2016.

GONÇALVES, Maria Eduarda «The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward», en *Information & Communications Technology Law,* vol. 26, n.º 2, Taylor & Francis, 2017.

GONZÁLEZ ROYO y PINA, Carolina, «¿Cómo se protegen legalmente los algoritmos?», en *Diario La Ley*, n.º 8776, La Ley, Madrid, 2016.

GONZÁLEZ ROYO, Ignacio, «La protección de los intangibles intelectuales e industriales en el contexto del Fintech», en *Diario La Ley,* n.º 8795, La Ley, Madrid, 2016.

GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria,* AEPD, Madrid, 2014.

GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón, «Cloud computing, cláusulas contractuales y reglas corporativas vinculantes», en *Revista de Derecho UNED*, n.º 14, 2014.

HIJMANS, Hielke, *The European Union as Guardian of Internet Privacy: The Story of Artículo 16 TFEU,* Springer, Bruselas, 2015.

HUA TAN, Kim, JI, Guojun, PENG LIM, Chee y TSENG, Ming-Lang, «Using Big Data to make better decisions in the digital economy», en *International Journal of Production Research,* vol. 55, n.º 17, Taylor & Francis, 2017.

IDC, *Worldwide Big Data Technology and Services 2012-2015 Forecast*, marzo de 2012.

JAIN, Vijay Kumar, *Big data and Hadoop,* Khanna Publishing, Nueva Delhi, 2017.

JIMÉNEZ-BENÍTEZ, William Guillermo, «Rules for offline and online in determining Internet jurisdiction. Global overview and colombian cases», en *Revista Colombiana de Derecho Internacional,* n.º 26, Bogotá (Colombia), 2015.

JOYANES AGUILAR, Luis, *Big Data. Análisis de grandes volúmenes de datos en organizaciones*, Alfaomega, México D.F, 2013.

KAŠĆELAN, Vladimir, KAŠĆELAN, Ljiljana y NOVOVIĆ BURIĆ, Milijana, «A nonparametric data mining approach for risk prediction in car insurance: a case study from the Montenegrin market», en *Economic Research-Ekonomska Istraživanja,* vol. 29, n.º 1, 2016, Informa UK, 2016.

KSHETRI, Nir, FREDRIKSSON, Torbjörn y ROJAS TORRES, Diana Carolina, *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South,* Routledge, Oxford, 2017.

KUNER, Christopher, «The European Union and the Search for an International Data Protection Framework», en *Groningen Journal of International Law,* vol. 2, 1.ª ed., 2015.

LANEY, Douglas, «3D Data Management: Controlling Data Volume, Velocity and Variety». Gartner, febrero de 2001.

LESMES SERRANO, Carlos (coord.), *La ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008.

LI, Tiancheng y LI, Ninghui, «On the Trade off Between Privacy and Utility in Data Publishing», en *CERIAS Tech Report 2009-2017,* Center for Education and Research Information Assurance and Security, Purdue University, West Lafayette (IN), 2009.

LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo,* Francis Lefebvre, Madrid, 2016.

LOSHIN, David, *Enterprise Knowledge Management: The Data Quality Approach,* Morgan Kaufmann, San Diego (CA), 2003.

MARR, Bernard, «How Big Data Is Changing Insurance Forever», *Forbes,* diciembre de 2015.

MARTÍNEZ ROJAS, Ángela, «Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea», *Revista Aranzadi de Derecho y Nuevas Tecnologías,* n.º 42, Aranzadi, Cizur Menor, 2016.

MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth, *Big Data. A Revolution That Will Transform How We Live,* Houghton Mifflin Harcourt, Nueva York, 2013.

MCKINSEY GLOBAL INSTITUTE, «Big data: The next frontier for innovation, competition, and productivity», 2011.

MOEREL, Lokke, «The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?», en *International Data Privacy Law,* vol. 1, n.º 1, Oxford University Press, 2011.

OREJUDO PRIETO DE LOS MOZOS, Patricia, «La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia», en *La Ley Unión Europea,* n.º 4, 2013.

ORTEGA GIMÉNEZ, Alfonso, «El Reglamento General de Protección de Datos de la UE en la empresa: novedades prácticas», en *Diario La Ley,* n.º 15, Sección Ciberderecho, 7 de marzo de 2018, Editorial Wolters Kluwer.

ORTEGA GIMÉNEZ, Alfonso, *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal,* Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos de carácter personal ilícitas,* Aranzadi, Cizur Menor, 2017.

ORTEGA GIMÉNEZ, Alfonso, «Propuestas ante un futuro incierto para la protección en la Unión Europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto *vs.* armonización a través de unos principios comunes?», en *Revista Aranzadi Unión Europea,* n.º 10, Aranzadi, Cizur Menor, 2016.

ORTEGA GIMÉNEZ, Alfonso, «Transferencia internacional de datos personales: del *Safe Harbour* al *Privacy Shield*», *Revista Lex Mercatoria Doctrina, Praxis, Jurisprudencia y Legislación*, n.º 4, Universidad Miguel Hernández, Elche, 2016.

ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita,* AEPD, Madrid, 2015.

ORTEGA GIMÉNEZ, Alfonso, «La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español», en *Diario La Ley,* n.º 8661, La Ley, Madrid, 2015.

ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional de datos», en *Revista Boliviana de Derecho,* n.º 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013.

PAAL, Boris y PAULY, Daniel (coords.), *Datenschutz-Grundverordnung*, C.H. Beck, Múnich, 2017.

PASTOR VITA, Francisco Javier, «Las condiciones generales y cláusulas abusivas en los contratos celebrados entre empresarios», en *Diario La Ley,* n.º 6367, La Ley, Madrid, 2005.

PÉREZ CAMBERO, Raúl, «Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de Privacidad UE-EE. UU.**», en** *Actualidad Administrativa,* n.º 4, Wolters Kluwer, Madrid, 2017.

PINAR MAÑAS, José Luis (dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Editorial Reus, Madrid, 2016.

POKORNY, Jaroslav y STANTIC, Bela, «Challenges and opportunities in Big Data Processing», en MA, Zongmin, *Managin Big Data ni Cloud Computing envionments*, IGI Global, Pensilvania, 2016.

PUYOL MORENO, Javier, «Una aproximación al *Big Data*», *Revista de Derecho UNED*, n.º 14, Madrid, 2014.

PWC y IRON MOUNTAIN, «Beyond good intentions. The need to move from intention to action to manage information risk in the mid-market», 2016.

PWC y IRON MOUNTAIN, «Seizing the information advantage**.** How organizations can unlock value and insight from the information they hold», 2015.

RALLO LOMBARTE, Artemi y GARCÍA MAHAMUT, Rosario, *Hacia un nuevo derecho europeo de protección de datos,* Tirant lo Blanc, Valencia, 2015.

RECIO GAYO, Miguel, *Protección de los datos personales e innovación: ¿(in)compatibles?,* Editorial Reus, Madrid, 2016.

REMONILA, Nelson, *Recolección internacional de datos personales: un reto del mundo post-Internet,* AEPD, Madrid, 2015.

RODRÍGUEZ LAINZ, José Luis, «GPS y balizas policiales», en *Diario La Ley,* n.º 8416, La Ley, Madrid, 2015.

RODRÍGUEZ-PRADO, José Miguel, «Los seguros gamificados de vida y salud. *Insurance telematics* (tendencias actuales y oportunidades en seguros de personas)», en *Revista Española de Seguros: publicación doctrinal de derecho y economía de los seguros privados,* n.º 167, SEAIDA, Madrid, 2016.

ROSELLÓ MALLOL, Víctor, «Marketing y protección de datos (I). Concepto de dato personal», en *Noticias Jurídicas,* diciembre de 2009.

SÁNCHEZ BRAVO, Álvaro (ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez,* Punto Rojo Libros, Sevilla.

SANCHO VILLA, Diana, *Negocios internacionales de tratamiento de datos personales,* Navarra, Civitas, 2010.

SCHROEDER, Ralph, «Big data business models: Challenges and opportunities», en *Cogent Social Sciences*, vol. 2, n.º 1, Taylor & Francis, 2016.

SCHWABE, Jürgen «Bundesverfassungsgericht und "Drittwirkung" der Grundrechte», en *Archiv für offentliches Recht*, n.º 100, 1975.

SOARES Sunil, «Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today», *dataversity.net*, junio de 2012.

SOARES Sunil, *Big Data Governance. An Emerging Imperative,* MC Press, Boise (ID), 2012.

SOLER FUENSATA, Juan Ramón y GUASCH PORTAS, Vicente, «Identificación y autentificación de clientes en establecimientos hoteleros. La difícil combinación entre biometría y hotelería», en *Revista de Análisis Turístico,* Facultad de Trismo de la Universidad de Málaga, Málaga, n.º 16, 2013.

STARMANS, Richard, «The Advent of Data Science: Some Considerations on the Unreasonable Effectiveness of Data», en BÜHLMANN, Peter, DRINEAS, Petros, KANE, Michael y VAN DER LAAN, Mark, *Handbook of Big Data,* CRC Press, 2016.

SVANTESSON, Dan Jerker, *Extraterritoriality in Data Privacy Law,* Ex tuto Publishing, Copenhague, 2013.

TASCÓN, Mario y COULLAUT, Arantza*, Big Data y el Internet de las Cosas. Qué hay detrás y cómo nos va a cambiar,* Catarata, Madrid, 2016.

TAYLOR, Mistale, «Permissions and prohibitions in data protection jurisdiction», en *Brussels Privacy* Hub *working paper,* vol. 2, n.º 6, Universidad Libre de Bruselas, 2016.

TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas, Madrid, 2010.

VANSON BOURNE, «The State of Big Data Infrastructure: Benchmarking global Big Data users to drive future performance», 2015.

VEDDER, Anton, «Accountability for the use of algorithms in a Big Data environment», en *International Review of Law, Computers & Technology,* vol. 31, n.º 2, Routledge, 2017.

VELASCO NÚÑEZ, Eloy, «Tecnovigilancia, geolocalización y datos: aspectos procesales penales», en *Diario La Ley,* n.º 8338, La Ley, Madrid.

VICTOR, Nancy y LOPEZ, Daphne, «Privacy models for big data: a survey», en *International Journal of Big data Intelligence,* vol. 3, nº. 1, 2016.

VINAIXA MIQUEL, Mónica, *La responsabilidad civil por contaminación transfronteriza derivada de residuos,* Universidad de Santiago de Compostela, 2006.

VIVAS TESÓN, Inmaculada, «La tutela "sui generis" de las bases de datos», en *Revista de Derecho Patrimonial*, n.º 21, Aranzadi, Cizur Menor, 2008.

VV. AA, «Gamification: Toward a Definition», artículo presentado en el *Conference on Human Factors in Computing Systems,* Vancouver, 2011.

WASSER, Thomas, «Using "big data" to validate claims made in the pharmaceutical approval process», en *Journal of Medical Economics,* vol. 18, n.º 12, Taylor & Francis, 2015.

YANG, Chaowel, «Big Data and Cloud Computing: innovation opportunities and challenges», en *International Journal of Digital Earth,* vol. 10, n.º 1, Informa UK, 2017.

ZABÍA DE LA MATA, Juan, *Protección de datos: comentarios al reglamento,* Lex Nova, 2012, Madrid.

ZELL, Anne-Marie, «Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field», en *German Law Journal,* vol. 15, n.º 3, Washington & Lee University School of Law, Washington, 2014.

ZIKOPOULOS, Paul, *Harness the power of big data, the IBM Big data platform,* McGraw-Hill, 2013.

ENLACES WEB

Agencia Española de Protección de Datos
https://www.agpd.es

Boletín Oficial del Estado
https://www.boe.es

Comité Europeo de Protección de Datos
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

European Securities and Markets Authority
https://www.esma.europa.eu

Fundación MAPFRE
https://www.fundacionmapfre.org/fundacion/es_es/

Parlamento Europeo
http://www.europarl.europa.eu/madrid/es/portada.html

Supervisor Europeo de Protección de Datos
https://edps.europa.eu/edps-homepage_en?lang=es

Taylor & Francis
http://www.tandfonline.com

ÍNDICE DE CASOS PRÁCTICOS

ÍNDICE DE FIGURAS

COLECCIÓN "CUADERNOS DE LA FUNDACIÓN"

Para cualquier información sobre nuestras publicaciones consulte:
www.fundacionmapfre.org

229. Las aplicaciones del *Big Data* en el ámbito asegurador y el tratamiento legal de sus datos. 2019

228. Otimização conjunta do capital baseado em risco e da carateira de ativos.

227. Fundamentos de primas y reservas de fianzas y seguros de caución. Enfoque de Solvencia II. 2018

226. Determinantes de la performance de los fondos de pensiones. 2018

225. Estudio sobre el employer branding del sector seguros en España. 2018

224. El impacto de Solvencia II en los grupos de entidades aseguradoras. 2018

223. Contributions to Risk Analysis: RISK 2018

222. Individual Cancer Mortality Prediction. 2017

221. Defensa jurídica y dolo del asegurado en el seguro de responsabilidad civil. 2017

220. El proceso precontractual en el contrato de seguro: nuevo marco jurídico. 2017

219. Teoría de cópulas. Introducción y aplicaciones a Solvencia II. 2017

218. Cualificación profesional del actuario. Estudio internacional comparado. 2016

217. El seguro de responsabilidad civil derivada de la navegación de buques. 2016

216. El impacto de las últimas reformas en materia de jubilación: envejecimiento activo, sostenibilidad financiera y planes de pensiones. 2016

215. Previsión complementaria empresarial: estudio comparado internacional. 2016

214. Normas sobre protección de los derechos de los consumidores en el contrato de seguro en Chile. 2016

213. *Gamificación:* un modelo de fomento y gestión de comportamientos deseados en las relaciones entre individuos y organizaciones. 2015

212. Modelo de gestión integral para el sector atunero. 2015

211. Opções embutidas em planos *unit-linkeds* brasileiros: avaliação sob a medida de probabilidade real. 2015

210. El enfoque de Solvencia II para las pensiones ocupacionales españolas. 2015

209. El seguro privado de obras de arte. 2015

208. Definición y medición de la cultura aseguradora. Aplicación al caso español. 2015

207. Tipos de interés para valorar las provisiones técnicas de seguros. 2015

206. Teledetección aplicada a la elaboración de mapas de peligrosidad de granizo en tiempo real y mapas de daños en cultivos e infraestructuras. 2015

205. Current Topics on Risk Analysis: ICRA6 and Risk 2015 Conference. 2015

204. Determinantes do Premio de Default de (Res)seguradores. 2014

203. Generación de escenarios económicos para la medición de riesgos de mercado en Solvencia II a través de modelos de series temporales. 2014

202. Valoración de los inmuebles del patrimonio histórico y los riesgos sísmicos en el contrato de seguro: el caso de Lorca. 2014

201. Inteligencia computacional en la gestión del riesgo asegurador: operadores de agregación OWA en proceso de tarificación. 2014

200. El componente transfronterizo de las relaciones aseguradoras. 2014

199. El seguro basado en el uso (Usage Based Insurance). 2014

198. El seguro de decesos en la normativa aseguradora. Su encaje en Solvencia II. 2014

197. El seguro de responsabilidad civil en el arbitraje. 2014

196. La reputación corporativa en empresas aseguradoras: análisis y evaluación de factores explicativos. 2014

195. La acción directa del perjudicado en el ordenamiento jurídico comunitario. 2013

194. Investigaciones en Seguros y Gestión del Riesgo: RIESGO 2013

193. Viability of Patent Insurance in Spain. 2013

192. Viabilidad del seguro de patentes en España. 2013

191. Determinación de zonas homogéneas de riesgo para los rendimientos de distintos cultivos de la región pampeana en Argentina. 2013

190. Género y promoción en los sectores financiero y asegurador. 2013

189. An Introduction to Reinsurance. 2013

188. El control interno y la responsabilidad penal en la mediación de seguros privados. 2013

187. Una introducción al gobierno corporativo en la industria aseguradora en América Latina. 2013

186. Mortalidad de jóvenes en accidentes de tráfico. 2012

185. Las reclamaciones derivadas de accidentes de circulación por carretera transfronterizos. 2012

184. Efecto disuasorio del tipo de contrato sobre el fraude. 2012

183. Claves del Seguro Español: una aproximación a la Historia del Seguro en España. 2012

182. La responsabilidad civil del asegurador de asistencia sanitaria. 2012

181. Colaboración en el contrato de Reaseguro. 2012

180. Origen, situación actual y futuro del seguro de Protección Jurídica. 2012

179. Experiencias de microseguros en Colombia, Perú y Brasil. Modelo socio agente. 2012

178. El agente de seguros y su Responsabilidad Civil. 2012

177. Riesgo operacional en el marco de Solvencia II. 2012

176. Un siglo de seguros marítimos barceloneses en el comercio con América. (1770-1870). 2012

175. El seguro de Caución. 2012

174. La contabilidad de los corredores de seguros y los planes y fondos de pensiones. 2012

173. El seguro de Vida en América Latina. 2011

172. Gerencia de riesgos sostenibles y Responsabilidad Social Empresarial en la entidad aseguradora. 2011

171. Investigaciones en Seguros y Gestión del Riesgo. RIESGO 2011

170. Introdução ao Resseguro. 2011

169. La salud y su aseguramiento en Argentina, Chile, Colombia y España. 2011

168. Diferencias de sexo en conductas de riesgo y tasa de mortalidad diferencial entre hombres y mujeres. 2011

167. Movilización y rescate de los compromisos por pensiones garantizados mediante contrato de seguros. 2011

166. Embedded Value aplicado al ramo No Vida. 2011

165. Las sociedades cautivas de Reaseguro. 2011

164. Daños del amianto: litigación, aseguramiento de riesgos y fondos de compensación. 2011

163. El riesgo de tipo de interés: experiencia española y Solvencia II. 2011

162. I Congreso sobre las Nuevas Tecnologías y sus repercusiones en el Seguro: Internet, Biotecnología y Nanotecnología. 2011

161. La incertidumbre bioactuarial en el riesgo de la longevidad. Reflexiones bioéticas. 2011

160. Actividad aseguradora y defensa de la competencia. La exención antitrust del sector asegurador. 2011

159. Estudio empírico sobre la tributación de los seguros de vida. 2010

158. Métodos estocásticos de estimación de las provisiones técnicas en el marco de Solvencia II. 2010

157. Introducción al Reaseguro. 2010

156. Encuentro Internacional sobre la Historia del Seguro. 2010

155. Los sistemas de salud en Latinoamérica y el papel del seguro privado. 2010

154. El Seguro de Crédito en Chile. 2010

153. El análisis financiero dinámico como herramienta para el desarrollo de modelos internos en el marco de Solvencia II. 2010

152. Características sociodemográficas de las personas con doble cobertura sanitaria. Un estudio empírico. 2010

151. Solidaridad impropia y seguro de Responsabilidad Civil. 2010

150. La prevención del blanqueo de capitales en las entidades aseguradoras, las gestoras y los corredores de seguros 2010

149. Fondos de aseguramiento agropecuario y rural: la experiencia mexicana en el mutualismo agropecuario y sus organizaciones superiores. 2010

148. Avaliaçao das Provisoes de Sinistro sob o Enfoque das Novas Regras de Solvência do Brasil. 2010

147. El principio de igualdad sexual en el Seguro de Salud: análisis actuarial de su impacto y alcance. 2010

146. Investigaciones históricas sobre el Seguro español. 2010

145. Perspectivas y análisis económico de la futura reforma del sistema español de valoración del daño corporal. 2009

144. Contabilidad y Análisis de Cuentas Anuales de Entidades Aseguradoras (Plan contable 24 de julio de 2008). 2009

143. Mudanças Climáticas e Análise de Risco da Indústria de Petróleo no Litoral Brasileiro. 2009

142. Bases técnicas dinámicas del Seguro de Dependencia en España. Una aproximación en campo discreto. 2009

141. Transferencia Alternativa de Riesgos en el Seguro de Vida: Titulización de Riesgos Aseguradores. 2009

140. Riesgo de negocio ante asegurados con múltiples contratos. 2009

139. Optimización económica del Reaseguro cedido: modelos de decisión. 2009

138. Inversiones en el Seguro de Vida en la actualidad y perspectivas de futuro. 2009

137. El Seguro de Vida en España. Factores que influyen en su progreso. 2009

136. Investigaciones en Seguros y Gestión de Riesgos. RIESGO 2009.

135. Análisis e interpretación de la gestión del fondo de maniobra en entidades aseguradoras de incendio y lucro cesante en grandes riesgos industriales. 2009

134. Gestión integral de Riesgos Corporativos como fuente de ventaja competitiva: cultura positiva del riesgo y reorganización estructural. 2009

133. La designación de la pareja de hecho como beneficiaria en los seguros de vida. 2009

132. Aproximación a la Responsabilidad Social de la empresa: reflexiones y propuesta de un modelo. 2009

131. La cobertura pública en el seguro de crédito a la exportación en España: cuestiones prácticas-jurídicas. 2009

130. La mediación en seguros privados: análisis de un complejo proceso de cambio legislativo. 2009

129. Temas relevantes del Derecho de Seguros contemporáneo. 2009

128. Cuestiones sobre la cláusula cut through. Transferencia y reconstrucción. 2008

127. La responsabilidad derivada de la utilización de organismos genéticamente modificados y la redistribución del riesgo a través del seguro. 2008

126. Ponencias de las Jornadas Internacionales sobre Catástrofes Naturales. 2008

125. La seguridad jurídica de las tecnologías de la información en el sector asegurador. 2008

124. Predicción de tablas de mortalidad dinámicas mediante un procedimiento bootstrap. 2008

123. Las compañías aseguradoras en los procesos penal y contencioso-administrativo. 2008

122. Factores de riesgo y cálculo de primas mediante técnicas de aprendizaje. 2008

121. La solicitud de seguro en la Ley 50/1980, de 8 de octubre, de Contrato de Seguro. 2008

120. Propuestas para un sistema de cobertura de enfermedades catastróficas en Argentina. 2008

119. Análisis del riesgo en seguros en el marco de Solvencia II: Técnicas estadísticas avanzadas Monte Carlo y Bootstrapping. 2008

118. Los planes de pensiones y los planes de previsión asegurados: su inclusión en el caudal hereditario. 2007

117. Evolução de resultados tecnicos e financieros no mercado segurador iberoamericano. 2007

116. Análisis de la Ley 26/2006 de Mediación de Seguros y Reaseguros Privados. 2007

115. Sistemas de cofinanciación de la dependencia: seguro privado frente a hipoteca inversa. 2007

114. El sector asegurador ante el cambio climático: riesgos y oportunidades. 2007

113. Responsabilidade social empresarial no mercado de seguros brasileiro influências culturais e implicações relacionais. 2007

112. Contabilidad y análisis de cuentas anuales de entidades aseguradoras. 2007

111. Fundamentos actuariales de primas y reservas de fianzas. 2007

110. El Fair Value de las provisiones técnicas de los seguros de Vida. 2007

109. El Seguro como instrumento de gestión de los M.E.R. (Materiales Específicados de Riesgo). 2006

108. Mercados de absorción de riesgos. 2006

107. La exteriorización de los compromisos por pensiones en la negociación colectiva. 2006

106. La utilización de datos médicos y genéticos en el ámbito de las compañías aseguradoras. 2006

105. Los seguros contra incendios forestales y su aplicación en Galicia. 2006

104. Fiscalidad del seguro en América Latina. 2006

103. Las NIC y su relación con el Plan Contable de Entidades Aseguradoras. 2006

102. Naturaleza jurídica del Seguro de Asistencia en Viaje. 2006

101. El Seguro de Automóviles en Iberoamérica. 2006

100. El nuevo perfil productivo y los seguros agropecuarios en Argentina. 2006

99. Modelos alternativos de transferencia y financiación de riesgos "ART": situación actual y perspectivas futuras. 2005

98. Disciplina de mercado en la industria de seguros en América Latina. 2005

97. Aplicación de métodos de inteligencia artificial para el análisis de la solvencia en entidades aseguradoras. 2005

96. El Sistema ABC-ABM: su aplicación en las entidades aseguradoras. 2005

95. Papel del docente universitario: ¿enseñar o ayudar a aprender? 2005

94. La renovación del Pacto de Toledo y la reforma del sistema de pensiones: ¿es suficiente el pacto político? 2005

92. Medición de la esperanza de vida residual según niveles de dependencia en España y costes de cuidados de larga duración. 2005

91. Problemática de la reforma de la Ley de Contrato de Seguro. 2005

90. Centros de atención telefónica del sector asegurador. 2005

89. Mercados aseguradores en el área mediterránea y cooperación para su desarrollo. 2005

88. Análisis multivariante aplicado a la selección de factores de riesgo en la tarificación. 2004

87. Dependencia en el modelo individual, aplicación al riesgo de crédito. 2004

86. El margen de solvencia de las entidades aseguradoras en Iberoamérica. 2004

85. La matriz valor-fidelidad en el análisis de los asegurados en el ramo del automóvil. 2004

84. Estudio de la estructura de una cartera de pólizas y de la eficacia de un Bonus-Malus. 2004

83. La teoría del valor extremo: fundamentos y aplicación al seguro, ramo de responsabilidad civil autos. 2004

81. El Seguro de Dependencia: una visión general. 2004

80. Los planes y fondos de pensiones en el contexto europeo: la necesidad de una armonización. 2004

79. La actividad de las compañías aseguradoras de vida en el marco de la gestión integral de activos y pasivos. 2003

78. Nuevas perspectivas de la educación universitaria a distancia. 2003

77. El coste de los riesgos en la empresa española: 2001.

76. La incorporación de los sistemas privados de pensiones en las pequeñas y medianas empresas. 2003

75. Incidencia de la nueva Ley de Enjuiciamiento Civil en los procesos de responsabilidad civil derivada del uso de vehículos a motor. 2002

74. Estructuras de propiedad, organización y canales de distribución de las empresas aseguradoras en el mercado español. 2002

73. Financiación del capital-riesgo mediante el seguro. 2002

72. Análisis del proceso de exteriorización de los compromisos por pensiones. 2002

71. Gestión de activos y pasivos en la cartera de un fondo de pensiones. 2002

70. El cuadro de mando integral para las entidades aseguradoras. 2002

69. Provisiones para prestaciones a la luz del Reglamento de Ordenación y Supervisión de los Seguros Privados; métodos estadísticos de cálculo. 2002

68. Los seguros de crédito y de caución en Iberoamérica. 2001

67. Gestión directiva en la internacionalización de la empresa. 2001

65. Ética empresarial y globalización. 2001

64. Fundamentos técnicos de la regulación del margen de solvencia. 2001

63. Análisis de la repercusión fiscal del seguro de vida y los planes de pensiones. Instrumentos de previsión social individual y empresarial. 2001

62. Seguridad Social: temas generales y régimen de clases pasivas del Estado. 2001

61. Sistemas Bonus-Malus generalizados con inclusión de los costes de los siniestros. 2001

60. Análisis técnico y económico del conjunto de las empresas aseguradoras de la Unión Europea. 2001

59. Estudio sobre el euro y el seguro. 2000

58. Problemática contable de las operaciones de reaseguro. 2000

56. Análisis económico y estadístico de los factores determinantes de la demanda de los seguros privados en España. 2000

54. El corredor de reaseguros y su legislación específica en América y Europa. 2000

53. Habilidades directivas: estudio de sesgo de género en instrumentos de evaluación. 2000

52. La estructura financiera de las entidades de seguros, S.A. 2000

51. Seguridades y riesgos del joven en los grupos de edad. 2000

50. Mixturas de distribuciones: aplicación a las variables más relevantes que modelan la siniestralidad en la empresa aseguradora. 1999

49. Solvencia y estabilidad financiera en la empresa de seguros: metodología y evaluación empírica mediante análisis multivariante. 1999

48. Matemática Actuarial no vida con MapleV. 1999

47. El fraude en el Seguro de Automóvil: cómo detectarlo. 1999

46. Evolución y predicción de las tablas de mortalidad dinámicas para la población española. 1999

45. Los Impuestos en una economía global. 1999

42. La Responsabilidad Civil por contaminación del entorno y su aseguramiento. 1998

41. De Maastricht a Amsterdam: un paso más en la integración europea. 1998

39. Perspectiva histórica de los documentos estadístico-contables del órgano de control: aspectos jurídicos, formalización y explotación. 1997

38. Legislación y estadísticas del mercado de seguros en la comunidad iberoamericana. 1997

37. La responsabilidad civil por accidente de circulación. Puntual comparación de los derechos francés y español. 1997

36. Cláusulas limitativas de los derechos de los asegurados y cláusulas delimitadoras del riesgo cubierto: las cláusulas de limitación temporal de la cobertura en el Seguro de Responsabilidad Civil. 1997

35. El control de riesgos en fraudes informáticos. 1997

34. El coste de los riesgos en la empresa española: 1995

33. La función del derecho en la economía. 1997

32. Decisiones racionales en reaseguro. 1996

31. Tipos estratégicos, orientación al mercado y resultados económicos: análisis empírico del sector asegurador español. 1996

30. El tiempo del directivo. 1996

29. Ruina y Seguro de Responsabilidad Civil Decenal. 1996

28. La naturaleza jurídica del Seguro de Responsabilidad Civil. 1995

27. La calidad total como factor para elevar la cuota de mercado en empresas de seguros. 1995

26. El coste de los riesgos en la empresa española: 1993

25. El reaseguro financiero. 1995

24. El seguro: expresión de solidaridad desde la perspectiva del derecho. 1995

23. Análisis de la demanda del seguro sanitario privado. 1993

22. Rentabilidad y productividad de entidades aseguradoras. 1994

21. La nueva regulación de las provisiones técnicas en la Directiva de Cuentas de la C.E.E. 1994

20. El Reaseguro en los procesos de integración económica. 1994

19. Una teoría de la educación. 1994

18. El Seguro de Crédito a la exportación en los países de la OCDE (evaluación de los resultados de los aseguradores públicos). 1994

16. La legislación española de seguros y su adaptación a la normativa comunitaria. 1993
15. El coste de los riesgos en la empresa española: 1991
14. El Reaseguro de exceso de pérdidas 1993
12. Los seguros de salud y la sanidad privada. 1993
10. Desarrollo directivo: una inversión estratégica. 1992
9. Técnicas de trabajo intelectual. 1992
8. La implantación de un sistema de controlling estratégico en la empresa. 1992
7. Los seguros de responsabilidad civil y su obligatoriedad de aseguramiento. 1992
6. Elementos de dirección estratégica de la empresa. 1992
5. La distribución comercial del seguro: sus estrategias y riesgos. 1991
4. Los seguros en una Europa cambiante: 1990-95. 1991
2. Resultados de la encuesta sobre la formación superior para los profesionales de entidades aseguradoras (A.P.S.). 1991
1. Filosofía empresarial: selección de artículos y ejemplos prácticos. 1991

LIBROS

La Responsabilidad Civil en el ámbito de los ciberriesgos. 2017

Longevidad y envejecimiento en el tercer milenio. 2017

El Ahorro en perspectiva histórica. 2016

Lo bueno, si breve... Microrrelatos de Seguros. 2016

The risk of longevity and its practical application to Solvency II. 2015

Historia de FIDES –Federación Interamericana de Empresas de Seguros. 2015

El riesgo de longevidad y su aplicación práctica a Solvencia II. 2014

Historia del Seguro en España. 2014

Actas del III Congreso Internacional de Nuevas Tecnologías: sus repercusiones en el seguro: internet, biotecnología y nanotecnología: 12 y 13 de noviembre de 2012, Santiago de Chile. 2013

Emergencia y reconstrucción: el antes y después del terremoto y tsunami del 27F en Chile. 2012

Riesgo sistémico y actividad aseguradora. 2012

La historia del seguro en Chile (1810-2010). 2012

Modelo de proyección de carteras de seguros para el ramo de decesos. 2011

Desarrollo comercial del seguro colectivo de dependencia en España. 2010

La mediación de seguros en España: análisis de la Ley 26/2006, de Mediación de Seguros y Reaseguros Privados. 2010

Museo del Seguro. Catálogo. 2010

Diccionario MAPFRE de Seguros. 2008

Teoría de la credibilidad: desarrollo y aplicaciones en primas de seguros y riesgos operacionales. 2008

El seguro de caución: una aproximación práctica. 2007

El seguro de pensiones. 2007

Las cargas del acreedor en el seguro de responsabilidad civil. 2006

Diccionario bilingüe de expresiones y términos de seguros: inglés-español, español-inglés. 2006

El seguro de riesgos catastróficos: reaseguro tradicional y transferencia alternativa de riesgos. 2005

La liquidación administrativa de entidades aseguradoras. 2005

INFORMES Y RANKINGS

Desde 1994 se publican anualmente estudios que presentan una panorámica concreta de los mercados aseguradores europeos, de España e Iberoamérica y que pueden consultarse en formato electrónico en castellano y en inglés desde la página web: www.fundacionmapfre.org

Mercado español de seguros. 2018

Mercado asegurador latinoamericano. 2018

Ranking de grupos aseguradores europeos. 2018

Ranking de grupos aseguradores iberoamericanos. 2018

Panorama económico y sectorial. 2018

Regímenes de regulación de solvencia. 2018

Elementos para el expansión del seguro en América Latina. 2017

Sistemas de Pensiones. 2017

Los millennials y el seguro en España. 2016

Tendencias de crecimiento de los mercados aseguradores de América Latina para 2016

Estudio social sobre la jubilación: expectativas y experiencias. 2015

La percepción social del seguro en España. 2014

Informe de predicción de la actividad aseguradora en España. 2014

La internacionalización de la empresa española: riesgos y oportunidades. 2014

El seguro en la sociedad y la economía españolas. 2013

Papel del seguro en el desarrollo sostenible. ICEA. 2013

Emprender en momentos de crisis: riesgos y factores de éxito. 2012

La percepción social del seguro en España. 2012

Puedes descargarte la versión digital
en el **Centro de Documentación**

www.fundacionmapfre.org/documentacion

Fundación **MAPFRE**

Fundación **MAPFRE**

C / 29

Paseo de Recoletos, 23
28004 Madrid (España)
www.fundacionmapfre.org

P.V.P.: 20€
978-84-9844-723-1