BIG DATA, PROTECCIÓN DE DATOS, Y DERECHO INTERNACIONAL PRIVADO

ÍNDICE

RESUMEN

El *Big Data* ha revolucionado la manera de entender un negocio, un sector o, incluso, una sociedad. Esta nueva forma de entenderla permite descubrir los hábitos y las costumbres de determinadas personas con el fin de adaptar los productos ofertados ofertados por una empresa al verdadero mercado objetivo.

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, las cuales pueden hacer variar la propia definición del concepto según la relativa importancia que los autores decidan dar a cada una de ellas; y la continua evolución de la cual es objeto.

Hemos podido observar las diferentes fuentes de datos personales que son utilizados en el *Big Data*, los cuales provienen de muy diversas fuentes que todos poseemos, como 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 según sea el medio por los cuales se recaban (mediante bases de datos o no).

Las afecciones legales que supone el *Big Data* son varias, es destacable la implicación en la normativa de protección de datos que ello 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.

A todo esto, el nuevo RGPD ha venido a reformar el panorama no solo europeo, sino internacional, de la protección de datos personales. La imposición de nuevas obligaciones y derechos a todas las partes involucradas hace que el marlo legislativo de

la protección de datos se adecue a las necesidades actuales de la «sociedad del dato», derivadas fundamentalmente de una normalizada internacionalización del flujo de datos.

La consideración de «tratamiento» sobre unos datos personales supone el punto de partida para la aplicación del marco normativo sobre protección de datos personales 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. RGPD viene a tratar este problema mediante la aplicación extraterritorial de la norma cuando los datos tratados correspondan a residentes en la Unión.

Las transferencias internacionales de datos personales continúan siendo uno de los elementos más importantes de las normas de protección de datos. Ello se demuestra en la gran extensión de su régimen en comparación con lo estipulado en la Directiva. La institucionalización de las Normas Corporativas Vinculantes suponen 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 garantía se encuentra cuestionada.

El *Privacy Shield* supone un nuevo régimen para las transferencias internacionales de datos con Estados Unidos, sustituyendo al derogado *Safe Habour*, y aumentando la protección sobre los datos personales. Pero el escudo no protege tanto como pretenden ensalzar la Comisión Europea; puesto que las reformas emprendidas por la nueva administración estadounidense vienen a mitigar la protección sobre el derecho a la protección de datos de los no nacionales estadounidenses.

Las relaciones internacionales están a la orden del día, y con ellas, un constante flujo de datos internacional. Es por ello que el RGPD establece un régimen mucho más completo para derecho a indemnización por responsabilidad extracontractual del afectado por un uso ilícito de los datos personales del afectado, comparado con la mera obligación que la Directiva imponía a los Estados de incluir tal derecho en sus ordenamientos. Es por ello que el nuevo Reglamento ha creado nuevas normas de Derecho internacional

privado con el fin de proteger al afectado en supuestos transnacionales de vulneración de su derecho a la protección de datos, derivadas de las sentencias del TJUE relacionadas con la competencia judicial internacional. 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 –aunque también supone un solapamiento de foros– y mayores oportunidades de defensa para el afectado, los cuales aumentarán dependiendo del contrato en el que ejerciten tales acciones. Debemos lamentar las nulas novedades en cuanto a la ley aplicable, que nos obligan a seguir aplicando las normas autónomas clásicas.

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.

DOUE: Diario Oficial de la Unión Europea

GB: Gigabyte

GT29: Grupo de Trabajo del artículo 29.

IP: Internet Protocol

IWGDPT: Grupo de Trabajo Internacional sobre Protección de Datos de las Telecomunicaciones.

LOPD: Ley Orgánica de Protección de datos

LOPJ: Ley Orgánica del Poder Judicial.

MAC: Media Acess Control

Mbps: Megabit por segundo

NCV: Normas Corporativas Vinculantes

RAL: Resolución Alternativa de Litigios.

RLOPD: Reglamento de la Ley Orgánica de Protección de Datos.

SAN/SSAN: Sentencia/s de la Audiencia Nacional.

SEPD: Supervisor Europeo de Protección de Datos.

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* 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.

Pero el *Big Data* puede trae tantos problemas como beneficios si tales datos personales no son tratados correctamente. El uso de datos masivos de esos datos implica un riesgo para la 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

[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.

los derechos mencionados (ej. los datos biométricos o los datos relativos a la salud); y es por ello que 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.

Otro dato relevante aportado por las empresas PwC y Iron Mountain demuestra que 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[4].

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, garantizando al mismo tiempo un elevado nivel de protección de los datos personales[5].

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

a) Explicar la tecnología conocida como *Big Data* desde su concepto y características definitorias;

b) Elucidar el nuevo régimen sobre protección de datos que otorga el nuevo Reglamento (UE) 679/2016 General de Protección de Datos (en adelante

[4] *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.
[5] *Vid*. Considerando 6 del RGPD.

RGPD)[6], y destacar algunas menciones al futuro Reglamento sobre privacidad pendiente de aprobación; sin no por ello 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.[7] y la Ley Orgánica 15/1999 , de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD)[8] sobre la Protección de Datos de Carácter Personal, pero siendo conscientes de que representan el pasado de la regulación sobre la protección de datos de carácter personal;

c) 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 empresas sitas tanto en la Unión Europea mediante sus filiales o por un tratamiento de datos realizado fuera del territorio comunitario.

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

e) Observar las cuestiones legales derivadas de una responsabilidad civil extracontractual por el uso ilícito de los datos personales tratados desde la perspectiva del Derecho internacional privado.

El *Big Data* ha demostrado generar 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. Es por ello que 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.

[6] DOUE L 119/1, de 4 de mayo de 2016.
[7] DOCE L 281, de 23 de noviembre de 1995.
[8] BOE núm. 298, de 14 de diciembre de 1999.

La explicación de las implicaciones legales del *Big Data* se ha llevado a cabo desde el estudio de 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 Grupo de Trabajo del artículo 29, los cuales contienen una enriquecedora combinación de consideraciones científico-jurídicas. Todo ello con el fin de constatar su incidencia en la protección de datos.

Las implicaciones derivadas del uso ilícito de los datos personales se han estudiado 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»; se clasificarán los tipos de datos que son objeto del *Big Data* desde un punto de vista técnico; para así estudiar las aplicaciones tanto económicas como legales.

En segundo lugar, estudiaremos el artículo 3 del RGPD en lo referido a la aplicación de la normativa de protección de datos europea a las operaciones de tratamiento llevadas a cabo por los encargados y responsables del tratamiento, haciendo especial hincapié en el efecto entre matriz-filiales a raíz de las SSTJUE y los dictámenes del GT29.

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 Unión 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 las empresas 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, explicando el nuevo derecho a la indemnización que establece el RGPD, y abordando las cuestiones sobre la determinación de la competencia judicial internacional por el nuevo régimen de compatibilidad entre el Reglamento Bruselas I bis y el RGPD, y de la ley aplicable a la controversia, cuyas novedades son nulas, y nos vuelven a obligar a aplicar las leyes autónomas.

II. ¿Qué es del *Big Data*?

II.1. Concepto y características del *Big Data*: desde el 3V's hasta el 3^2V.

II.1.1. Concepto.

La sociedad está inmersa en una constante digitalización, no solo social, sino también económica. 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 concepto 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 concepto *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, You Tube, o en cualquier red social constituye una información, un dato al fin y al cabo.

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»[9]. **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. Es por ello que 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, de hace unos minutos, puede arrojar resultados no apropiados al fin que buscamos con el *Big Data.* **Tan fundamental es la velocidad, que este término el 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 por menorizado.

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**[10]. 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»[11].

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*

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

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[12], o Deloitte[13]; 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)[14], como Gartner[15], o la velocidad (de creación y utilización) como IDC[16].

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 fundamental el *Big Data***[17]:

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 diferentes tipos de *Big Data*. Puede ser definida como una aplicación de procesamiento mediato de datos de la información generada por personas y generadas por máquinas;

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

[12] *Vid.* MCKINSEY GLOBAL INSTITUTE, *op. cit,* pp. 6.
[13] *Vid.* DELOITTE, «Big Data, Big Brother? Striking the right balance with privacy», 2015, pp. 4.
[14] *Vid*. JOYANES AGUILAR, Luis, *op. cit*, pp.19.
[15] *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/
[16] *Vid*. IDC, Worldwide Big Data Technology and Services 2012-2015 Forecast, marzo, 2012, pp. 1.
[17] *Vid*. BUYYA, Rajkumar, CALHEIROS, Rodrigo, y VAHID DASTJERDI, *Big Data: Principles and Paradigms*, Elsevier, Ámsterdam, 2016, pp. 10.

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 cuales quiera. PUYOL MONTERO incluye a tales medios en la concepción del *Big Data*[18].

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* están conformadas por las «uves», que vienen a ser uno de los rasgos más representativos del *Big Data.* Hemos observado 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 el *Big Data***. Debido a su expansión, las características se han ido agrupado en *domains* o dominios, que podemos definirlos como sectores especializados de un determinado campo.

[18] *Vid*. PUYOL MONTERO, Javier, *Aproximación jurídica y económica al Big Data*, Tirant lo Blanc, Valencia, 2016, pp. 286.

El primer conjunto de características clásicas están agrupadas en el denominado *Data domain*[19]. **En los albores de su entendimiento, se consideraban 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 los dinámicos 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, semi-estructurados o no estructurados[20]. Como ejemplo, un dato semi-estructurado puede consistir en el texto de un correo electrónico. Como dato no estructurado, un ejemplo 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, a lo que la velocidad del flujo de datos se 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

[19] El *Data domain* está basado en el categoría del dato, consistente tanto en una lista enumerada de valores determinados, como 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, pp. 302.

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

veracidad, la validez, y la variabilidad[21]; 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*[22] son:

- **Valor**: ¿los datos recogidos tienen información valiosa para mis necesidades empresariales? Es la pregunta que se busca responder.
- **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 (Fig. 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. 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.

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 o la fuente de datos está contaminada o el modelo estadístico es incorrecto. El análisis llegará a una conclusión incorrecta.

---

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

[22] 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, pp. 18.

- **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*[23]. 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[24].

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 esas características mediante un Diagrama de Venn que agrupe todas las características y *domains* que conforman el *Big Data* en la teoría de las 3^2V **(Figura 1)**. Si los atributos de datos originales de 3Vs representaban un significado sintáctico de *Big Data*, entonces 3^2V. (o 9Vs) representan el significado semántico (relación de datos, BI y estadísticas). Para muchos problemas o aplicaciones complejas, las 3^2V. podrían ser interpretados como un modelo jerárquico, para el cual tres atributos claves forman un nivel superior de 3Vs.

[23] *Vid*. ZIKOPOULOS, Paul, *Harness the power of big data, the IBM Big data platform*, McGraw-Hill, 2013, pp. 9.
[24] *Vid*. GANDOMI, Amir y HAIDER, Murtaza, «Beyond the hype: Big data concepts, methods, and analytics», en *International Journal of Information Management*, nº 35, Elsevier, Amsterdam, 2015, pp. 139.

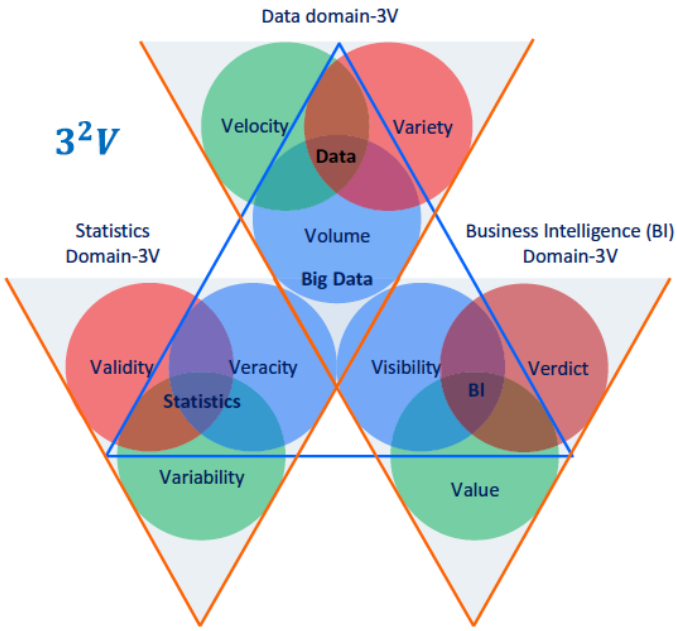

Figura. 1

Diagrama de Venn creado sobre una estructura jerárquica. Fuente: *Big Data: Principles and Paradigms*. pp. 14.

II.2. Clasificación de los datos objetos del *Big Data*.

Cada día generamos una cantidad ingente de datos. **Todos esos de datos son generados por *tablets*, teléfonos y sistemas inteligentes, como los conocidos *smartwatch*. Como ejemplos de datos que generamos día a día**[25]:

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

[25] *Vid*. PUYOL MORENO, Javier, «Una aproximación al Big Data», en *Revista de Derecho UNED*, nº 14, Madrid, 2014, pp. 474.

- 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.

Los datos se clasifican en tres tipos[26]:

1) **Datos estructurados**: hace referencia a **todo dato que puede ser recabado mediante una base de datos SQL[27] 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»)[28].
2) **Datos semi-estructurados**: 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 semi-estructurados[29].
3) **Datos no estructurados**: se refiere a la **información que no tiene un predefinido un dato modelo, o no está organizado de una manera**

[26] *Vid*. JAIN, Vijay Kumar, *Big data and Hadoop*, *op. cit*, pp. 12.
[27] SQL (Structure Query Language) es un lenguaje de programación creado para manejar y ordenar datos en sistemas de bases de datos relacionales.
[28] 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.

predefinida. La información no estructurada suele ser textos con una alta densidad de contenido, pero puede contener datos tales como fechas, números, y hechos también. Esto deriva en irregularidades y ambigüedades que lo hacen difícil para comprender el uso de programas tradicionales como comparación con datos almacenados en forma de ficheros en bases de datos, o anotados en documentos.

Técnicas como la minería de datos o 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…
    b. Datos de los *social media*: datos generados de webs con fuerte contenido social como You Tube, Facebook, Twitter, LinkedIn, y Flickr.
    c. Datos móviles: mensajes de texto, localización, tráfico online…
    d. Contenido web: proviene de cualquier sitio con un contenido deliberadamente no estructurado, como You Tube, Flickr, o Instagram.

Ahora bien, esos datos se pueden clasificar también según la fuente de la que procedan. SOARES realiza una clasificación de estas fuentes[30]:

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 capturan, almacenan y distribuyen dependiendo de su sub-origen: los datos generados en las redes sociales como consecuencia de determinadas acciones realizadas en éstas (*cliks*, *twitts*, *retwitts*, 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 u 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 y registros de facturación, reclamaciones de consumidores. Los grandes datos de transacciones están cada vez más disponibles en formatos semi-estructurados 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

[30] 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.

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 período de retención para que estos datos se adhieran a las regulaciones y para administrar los costos de almacenamiento.

Los resultados concretos que se pueden obtener con el *Big Data* son la conclusión 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»[31]. El algoritmo es el paso intermedio entre la recolecta masiva de datos y su aplicación práctica **(Figura 2)**.

[31] *Vid.* GONZÁLEZ ROYO y PINA, Carolina, «¿Cómo se protegen legalmente los algoritmos?», en *Diario La Ley*, Nº 8776, La Ley, Madrid, 2016, pp. 1.

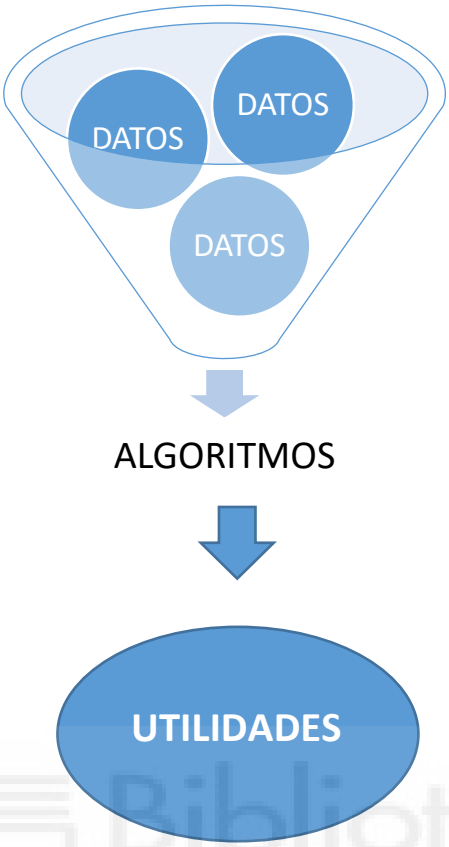

Figura 2

Explicación simplificada del funcionamiento del *Big Data*. Fuente: elaboración propia.

II.3. Implicaciones del *Big Data* en la normativa sobre protección de datos.

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[32]:

- Los datos utilizados para nuevos propósitos;

[32] *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>;.

- Maximización de datos y la falta de transparencia en su tratamiento;
- 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 36ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, la cual otorga unas reglas de comportamiento[33]:

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

[33] *Vid*. Resolucion de la 36ª 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**[34].

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 WP29 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»[35]. En dicha opinión, el GT29[36] 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 grupo es consciente 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. Es por ello que 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[37]. De los

[34] *Vid.* Artículos 22, 25, 35, y Considerando 28.
[35] WP 221. Adoptado el 17 de septiembre de 2014.
[36] El GT29 pasará a llamarse Comité Europeo de Protección de datos según el artículo 61 RGPD a partir del 25 de mayo.
[37] Véanse 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* March 2014; Discurso de Giovanni Buttarelli, *The EU Data Protection Reform: Updated Perspectives and the Challenges posed by Big Data*, Istanbul, mayo, 2014; *Report of EDPS workshop on privacy, consumers, competition and big data*, junio, 2014; Discurso de Giovanni Buttarelli, *Privacy and Competition in the Digital Economy*, enero, 2015; Discurso de Giovanni Buttarelli, *Antitrust, Privacy and Big Data*, febrero, 2015; EDPS Opinion 4/2015, *Towards a New Digital Ethics: Data, Dignity and Technology*, septiembre, 2015; Discurso de by Giovanni Buttarelli, *Competition Rebooted: Enforcement and Personal Data in Digital Markets*, septiembre, 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

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»[38], el cual destaca, en el mismo sentido que el GT29, **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, y
- Las organizaciones deberán ser más responsables de sus actos.

Una vez analizado lo anterior, podemos destacar las siguientes reflexiones[39]:

1ª) 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 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

Rights and Smart Enforcement, 29 de septiembre de 2016; EDPS blog post, *Big Data Rights: Let's Get Together*, octubre, 2016.

[38] (2016/C 67/05).

[39] *Vid*. GIL GONZÁLEZ, Elena, *Big Data, Privacidad Y Protección de Datos*, AEPD, Madrid, 2016, pp. 52-53.

empresas a rediseñar sus procesos para minimizar los datos recabados. Pero 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».

2ª) 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.

3ª) 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.

4ª) 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 que son analizados por medio de los 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*; 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 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[40].

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

Ejemplo 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 en cuanto 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.

Mediante este ejemplo, queremos mostrar las consecuencias de la elaboración de un perfil[41] por parte de una empresa a determinados afectados[42]. **Un perfil implica**

[40] *Vid.* DAVARA RODRÍGUEZ, Miguel Ángel, «*Big Data*», en *El Consultor de los Ayuntamientos,* Nº. 15, Wolters Kluwer, Madrid, 2013, pp. 1.
[41] 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.
[42] Es más adecuado utilizar el término «afectado» que «interesado»: los interesados en los datos personales pueden ser muchos, y algunos de ellos no con buenas intenciones.

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, sus discriminación en varios actos de su vida[43]. Es por ello que 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 distintos datos recogidos por varias vías[44]. Esos datos por los cuales se basan para la creación de perfiles suelen ser enfermedades que parecimos o parecemos actualmente, accidentes de tráfico que hemos sufrido, deudas pasadas y presentes, y una de sus principales manifestaciones es la creación de «listas negras»[45], 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**, viéndose afectado el control sobre la identidad de la persona interesada, y siendo privada de de manera arbitraria

[43] *Vid*. GARRIGA DOMÍNGUEZ, Ana, *Nuevos retos para la protección de datos personales*. En la Era del Big Data y de la computación obicua, Dykinson, Madrid, pp. 67.
[44] *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, pp. 18.
[45] *Vid*. WP 65 Documento de Trabajo sobre las listas negras. Adoptado el 3 de octubre de 2002.

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 35ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad:

- Garantizar la necesidad del *profiling* y establecer las garantías adecuadas para tal operación.
- 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 el 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 estableciendo que el afectado tendrá derecho a no ser objeto de tales conductas cuando le afecten jurídicamente o tengan un efecto similar.

El ejercicio de este derecho comporta una serie de límites cuando sea necesario para la ejecución o celebración de un contrato entre el afectado y un responsable del tratamiento, lo permita el Derecho de la Unión o de los Estados miembros, o se base en el consentimiento.

El responsable deberá garantizar que se tomarán las medidas necesarias para salvaguardar los derechos e intereses legítimos del afectado, entre ellos, el derecho a la intervención humana por parte del responsable, a expresar su punto de vista, y a impugnar la decisión.

Se prohíbe que las decisiones no se basen en el tratamiento de categorías especiales de datos, salvo si el afectado ha otorgado su consentimiento.

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, y en los artículos 16 de la LOPD y 36 del RLOPD en cuanto al derecho de oposición. Ahora, con el nuevo reglamento, el derecho se configura de forma autónoma respecto al derecho de oposición.

III. 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[46], 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.

En comparación con la rúbrica estipulada en la Directiva 95/46/CE, la cual 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 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[47]. Por ello, las empresas se enfrentarán a un solo derecho paneuropeo de protección de datos, no a veintiocho.

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 éste como un conjunto organizado de datos[48], con la consecuencia de que **prácticamente cualquier actividad con datos personales quedará englobada en el concepto de «tratamiento»**[49].

---

[46] *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, pp. 61.
[47] Como la determinación de la edad mínima del menor para otorgar su consentimiento (artículo 8 RGPD).
[48] *Vid*. ERDOZÁIN LÓPEZ, José Carlos, «La protección de los datos de carácter personal en las telecomunicaciones», en *Revista Doctrinal Aranzadi Civil-Mercantil*, nº 1, Aranzadi, Cizur Menor, 2007, pp. 2.
[49] *Ibídem*, pp. 3.

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.

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[50].

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.

III.1. En el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión.

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 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

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

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[51].

En definitiva, que el concepto de «establecimiento» *se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable* (párrafo 31). 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 se lleve a cabo la administración central en la Unión. Pero como norma especial, si las**

[51] *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, Nº 31, 2015, pp. 8.

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 el 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[52], **tal tratamiento debe llevarse a cabo «en el contexto de las actividades del establecimiento».** Para explicar tal concepto, debemos acudir al Dictamen 8/2010, el cual 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.
2) **Naturaleza de las actividades del establecimiento**. La cuestión de si un 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*, 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,**

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

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. Es por ello que 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 ésta una de ellas. Cada caso es distinto, y se deben atener a los hechos del caso concreto. Ni la sentencia debe interpretar de forma totalmente expansiva, ni de forma restrictiva a las empresas con modelos de negocio relacionados con los motores de búsqueda.

Ejemplo 1: Tratamiento de datos por establecimiento fuera de la UE y con establecimiento promocional

Una empresa se dedica a la oferta de servicios con sede en Rusia. Para ello, utiliza medios electrónicos para recabar los datos y tratarlos.

A su vez, esta empresa 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 empresa. En este caso, se podríamos establecer tal relación; ya que los servicios de publicidad favorecen el aumento de los ingresos de esa concreta línea de negocio. Por lo tanto, el tratamiento de esos datos está cubierto por el artículo 3.1 del RGPD.

III.2. Actividades de tratamiento relacionadas con la oferta de bienes o servicios a afectados en la Unión, independientemente de si a estos se les requiere su pago.

Como apunte general al criterio de la situación del afectado del apartado 3.2 del RGPD, **facilita el sometimiento de 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**[53]. Este criterio genera una mayor protección de los individuos al haber ampliado en alcance de la norma, sobre todo en lo que viene siendo la monitorización de su conducta[54].

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.

Pasando a estudiar el inciso a), debemos partir de la descripción que realiza el Considerando 23, el cual 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.* el Considerando no contempla que 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 responsible dirige su oferta al territorio de la Unión.

DE MIGUEL ASENSIO considera que, salvaguardando las distancias entre un caso y otro[55], sería de aplicación los criterios mostrados en la STJUE *Pammer y Hotel Alpenhor*.

---

[53] *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, nº 1, Madrid, 2017, pp. 14.

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

[55] El caso tratado en la STJUE citada no versa sobre protección de datos, sino de controversias en materia mercantil.

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 ofrece 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 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**.

Aunque, según este autor, observa cumplida las condiciones del artículo 3.2 a) del 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[56].

Ejemplo 2: Oferta de bienes por empresa externa a la Unión

Una empresa se dedica a la ofertas bienes con sede en la India. Para ello, utiliza plataformas de internet para ofertarlos.

La página web de la empresa está disponible en idiomas singulares de la Unión Europea como alemán, inglés, italiano, austriaco, y español; aparte de dispone 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 empresa 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 éstos dos últimos no cabe considerarlos

[56] *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, pp. 16.

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 estarán cubiertos por el artículo 3.2 a) del RGPD.

III.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 que se encuentren en la Unión, en la medida en que este tenga lugar 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 lo tanto el ofrecimiento de productos o servicios[57]. **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**.

Si entendemos el comportamiento como el conjunto de actos realizados por el ser humano producidos por la interacción con el entorno en el que vive, algunas de las categorías de datos tratados por el *Big Data* revelan dichos actos[58].

El Considerando 24 determina que se entenderá como un control de comportamiento el seguimiento del afectado en internet; pero a continuación estipula una referencia 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.

[57] *Vid*. ALBRECHT, Jan Phillipp y JOTZO, Florian, *Das neue Datenschutzrecht der EU*, Baden-Baden, Nomos, 2017, p. 67; ERNST, S, «Artículo 3» en PAAL, M.P. y PAULY, D.A. (Coords.), *Datenschutz-Grundverordnung*, C.H. Beck, Munich, 2017, pp. 25-26, y DE MIGUEL ASENSIO, Pedro Alberto, *op. cit*, pp. 16.

[58] *Vid*. *p. ej*., la ubicación de los individuos, los hábitos diarios relacionados con las horas de sueño o la actividad deportiva.

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**.

Ejemplo 3: Uso de aplicaciones deportivas.

Una empresa se dedica a la ofertas aparatos electrónicos 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 una pulsera inteligente 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 determinadas acciones (por ejemplo, al ir a dormir, metros recorridos…), y tales comportamientos pueden ser usados por un tercero, como por ejemplo, ceder el uso de tales datos a una entidad aseguradora para ejecutar 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 estarán cubiertos por el artículo 3.2 b) del RGPD.

IV. Transferencias internacionales de datos personales.

Las Transferencias internacionales de datos personales (TID) han sido uno de los caballos de batalla que ha tenido que afrontar la Unión Europea en materia de protección de datos. Como principales hitos[59]:

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[60], insta a la Comisión Europea a actuar sobre la posible suspensión del acuerdo SWIFT de transmisión de datos bancaria.

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

[59] *Vid*. ORTEGA GIMÉNEZ, Alfonso, «Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield», en *REVISTA LEX MERCATORIA Doctrina, Praxis, Jurisprudencia y Legislación*, nº 4, Universidad Miguel Hernández, Elche, 2016, pp. 85.
[60] Texto aprobado, P7_TA(2013) 0449.

> 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**.

El RGPD es consciente de la importancia de las transferencias de los flujos de datos a terceros países para la expansión del comercio y de la cooperación internacional, pero las transferencias internacionales de datos no deben menoscabar el derecho a la protección de datos de los particulares[61].

Por ello, el nuevo régimen de las transferencias internacionales de datos del RGPD tiene una doble razón de ser[62]: **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 reforzando también el régimen de las transferencias, aumentando las garantías que se deben asegurar para llevarlas a cabo.

[61] *Vid*. Considerando 101 RGPD.
[62] *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, pp. 430.

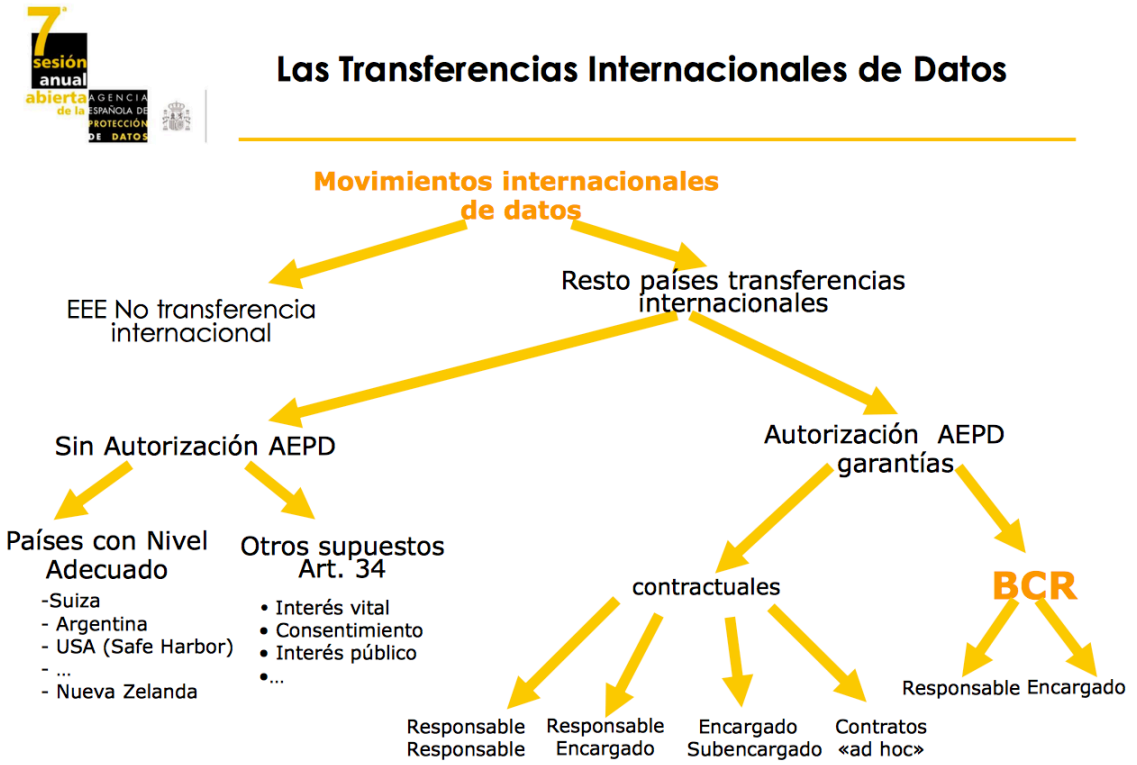

Figura 2.

Esquema de las transferencias internacionales de datos. Fuente: AEPD.

IV.1. Concepto.

La definición de «transferencia internacional de datos» no se encuentra en ningún instrumento legislativo europeo; 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 alojamiento domiciliado en la Unión, en la que se puede acceder desde cualquier lugar debe ser considerada como una transferencia internacional (apartado 71), la cual 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. Es por ello que 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 este argumento: 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 lo tanto; una «transferencia internacional de datos» **deberá constar de los siguientes elementos**[63]:

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 permitan identificar o hacer identificable a una persona de manera directa o indirecta»[64].
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 realizados por medios convencionales).

[63] *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, pp. 23; y *Transferencias internacionales de datos de carácter personal ilícitas*, Aranzadi, Cizur Menor, 2017, pp. 31
[64] *Vid*. artículos 3.a) LOPD, 5.1.f) del RLOPD, y 4.1) del RGPD.

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 los mismos.
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 15 de marzo de 2002, y confirmada por la STS 25 de 09 de 2006.

Posteriormente, el RLOPD definió el concepto en el artículo 5.1s) 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

cualesquiera comunicación de datos fuera del territorio español[65]. Aunque solo deben considerarse «transferencia internacional de datos» en sentido estricto las transferencias a terceros países que no pertenecen al Espacio Económico Europeo (EEE)[6667].

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[68], **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»**[69].

La consideración de los supuestos de acceso internacional como transferencias internacionales **indudablemente reforzará el derecho del titular a la protección de datos**[70]; 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 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

[65] *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, pp. 391.
[66] *Vid*. FERNÁNDEZ-LONGORIA, Paula y FERNÁNDEZ-SAMANIEGO, Javier, «Transferencias internacionales de datos personales», en RONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley*…, *op. cit*, pp. 1779.
[67] Actualmente está compuesto por los veintiocho Estados de la UE más Liechtenstein, Islandia, y Noruega.
[68] *Vid*. ERDOZÁIN LÓPEZ, José Carlos, «La protección de los…», *op. cit*, pp. 10.
[69] *Vid*. ORTEGA GIMÉNEZ, Alfonso, La (des) protección del titular…, *op. cit*, pp. 28; el mismo, Transferencias internacionales…, *op. cit*, pp. 36.
[70] *Ibídem*.

disposición de los datos[71], misma postura que mantiene el Supervisor Europeo de Protección de Datos[72].

IV.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 los titulares del derecho fundamental a la protección de datos mediante una norma que reduce la fragmentación jurídica y aumenta la seguridad jurídica por la introducción de un conjunto de normas básicas unificadoras, 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, y con ello, del mercado interior.

Es por ello que 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 corporativas vinculantes, además de contemplar significativas excepciones para dar viabilidad práctica a situaciones específicas[73].

---

[71] *Vid*. PINAR MAÑAS, José Luis, «Transferencias de datos personales a terceros países u organizaciones internacionales»…, *op. cit*, pp. 433.
[72] *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.
[73] *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*, nº 6, Aranzadi, Cizur Menor, 2016, pp. 13.

IV.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**[74].

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**[75].

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 publicas a los datos personales, así como 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;

[74] «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».
[75] *Ibídem*, nota 72.

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos 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[76], Canadá[77], Argentina[78], Guernsey[79], Isla de Man[80], Jersey[81], Islas Feroe[82], Andorra[83], Israel[84], Uruguay[85], Nueva Zelanda[86], y Estados Unidos de América[87].

[76] Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
[77] 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.
[78] Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
[79] Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
[80] Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
[81] Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
[82] Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
[83] Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
[84] Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
[85] Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
[86] Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
[87] 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.

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 su ordenamientos jurídicos.

IV.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;
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 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 GT29 dictaminó que las cláusulas contractuales tipo y las normas corporativas vinculantes serían suficientes para garantizar la seguridad de los datos[88]. 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

[88] *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).

«son una herramienta de gran utilidad que permite transferir datos personales desde todos los Estados miembros mediante un conjunto de normas comunes»[89].

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[90]; 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 transferencia de datos personales a terceros Estados[91] (versión consolidada de 1 de abril de 2005), modificada por la Decisión de ejecución 2016/2297/CE [92].

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 de responsabilidad basado en la debida diligencia[93] 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.

[89] *Vid.* GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria*, AEPD, Madrid, 2014, pp. 162.
[90] DOCE L 181, 4 de julio de 2001.
[91] DOUE L 385, de 29 de diciembre de 2004.
[92] DOUE L 344/100, 17 diciembre de 2016.
[93] *Ibídem*, nota 89.

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 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; 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 GT29[94] y el Considerando 23 de la Decisión 2010/87/UE[95], las cláusulas recogidas en la mencionada decisión solo son de aplicación a las

[94] *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»

[95] 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

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 GT29 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 la Decisión 2010/87/UE.

Esta última solución es la que ha adoptado la AEPD. El conjunto de cláusulas prevé que la solicitud 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 de la 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 del 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).

---

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.

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).

Las cláusulas contractuales tipo se encuentran en entredicho a raíz de la STJUE *Schrems*. Debido a esto, la autoridad de protección de datos irlandesa busca la pronunciación del Tribunal de Justicia de la Unión Europea. Actualmente, hay un procedimiento abierto en la *High Court* irlandesa[96] en el que vuelven a intervenir Facebook y Max Schrems. Las inquietudes suscitadas por el caso *Schrems*[97], 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 a Comisión[98].

IV.2.3. Normas corporativas vinculantes (artículo 47 de RGPD).

Cuando se traten 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

[96] "Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems". The Court Record Number: 2016/4809P.
[97] *Vid*. los Considerando 1, 6, y 7 de la Decisión de ejecución 2016/2297/CE.
[98] 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.

otras entidades del grupo situadas en terceros países, siempre que tales normas incluyan las garantías necesarias[99].

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 GT29 mediante numerosos *papers* quien ha ido perfilando el contenido de las NCV hasta la entrada en vigor del RGPD**. 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 establecer 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.

IV.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.

Actualmente, el artículo 4.20) del RGPD los define como «**las políticas de protección de datos personales asumidas por un responsable o encargado del**

[99] 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.

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»[100], el RGPD consagra que tales normas serán exigibles jurídicamente «tanto a nivel 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 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;
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

[100] Debido a que el régimen legal anterior a ello era ínfimo, se dudaba de que la adopción de tales reglas entre las sociedades pudieran llegar a ser exigibles legalmente entre las partes. *Vid*. ÁLVAREZ RIGAUDAS, Cecilia, «Movimiento internacional de datos: las transferencias internacionales de datos personales», en RONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley…, *op. cit,* pp. 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*, núm. 4, septiembre 2003.

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 establecidos 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 auditorias 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 país tercero 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, y

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 GT29: WP 74[101] ,WP 107[102], WP 108[103], WP 153[104], WP 154[105], y WP 155[106].

El uso de estas normas por los responsables del tratamiento de los grupos multinacionales ha aumentado rápidamente en el paso de los años debido a la flexibilidad que estas otorgan[107]; para adaptarse a los nuevos modelos de negocios, el GT29 ha elaborado unas nuevas RCV destinadas a los encargados del tratamiento, cuyo régimen se encuentra en los WP 195[108], 195a[109], y WP 204[110].

[101] «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.

[102] «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.

[103] «Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules». Adoptado el 14 de abril de 2005.

[104] «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.

[105] «Working Document Setting up a framework for the structure of Binding Corporate Rules». Adoptado el 24 de junio de 2008.

[106] «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules». Adoptadp el 24 de junio de 2008, y modificado el 7 de febrero de 2017.

[107] *Vid*. GUASCH PORTAS, Vicente, y SOLER FUENSANTA, José Ramón, «Cloud computing, cláusulas contractuales y reglas corporativas vinculantes», en *Revista de Derecho UNED*, nº 14, Madrid, 2014, pp. 266.

[108] «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.

[109] «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.

[110] «Explanatory Document on the Processor Binding Corporate Rules». Adoptado el 19 de abril de 2013, y modificado el 22 de mayo de 2015.

El WP 204 considera que las NCV 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».

IV.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.

    i. 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.
    ii. 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

sólo 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»[111].

b) **Segundo paso**: la empresa redacta las NCV cumpliendo con los requisitos establecidos en los documentos de trabajo adoptados por el Grupo de Trabajo del artículo 29. 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 de las NCV 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 de las NCV y los que no estén reconocidos mutuamente han considerado que las NCV cumple con los requisitos establecidos en el WP29 (en el plazo de un mes)[112]
e) **Quinto paso**: el RGPD exige en el artículo 64.1.f) exige que el futuro Comité emita un dictamen previo a la aprobación de las reglas, que deberá ser seguido por la autoridad 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 las NCV hayan 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

[111] *Vid.* Considerando 135 del RGPD.
[112] *Vid*. artículos 47.1, 57.1.s), y 58.3.j) del RGPD.

adherido los encargados, y otros requisitos adicionales para garantizar la protección de los afectados.

IV.3. *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 Como 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 meanismo de autocertificación de empresas estadounidenses en el que se permite la transferencia de datos a las empresas que hayan sido certificadas mediante el cumlimiento de unos requisitos de seguridad y el cumplimiento 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[113]. 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.

[113] DO L 207/1, de 1 de agosto de 2016.

El *Privacy Shield* se aplica tanto a los responsables como a los encargados del tratamiento, si bien éstos 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[114]:

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 EEUU). Además de diversas obligaciones formales ((i) su adhesión al *Privacy Shield* y la indicación del enlace a la lista de entidades adheridas al mismo; (ii) los tipos de datos que se han recogido; (iii) el compromiso que tiene la entidad de cumplir con dichos principios; (iv) la finalidad para la cual se recogen los datos; (v) el procedimiento para contactar con la entidad para presentar reclamaciones y quejas).

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

[114] *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 la privacidad UE-EE. UU», en *Actualidad Administrativa,* Nº. 4, Wolters Kluwer, Madrid, 2017, pp. 3

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 sólo 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 esta bastante relacionado con el origical, 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 EEUU o no. Si los datos son enviados a otra empresa para tratarlos en su nombre, ésta 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 de los datos 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 transmitr datos a terceros de manera lícita sólo 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 de 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 EEUU. Tambien se puede optar por una APD europea.
c) Ante el Departamento de Comercio de los 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 los EE. UU. (o el Departamento de Transportes de los 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. Sólo 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 EEUU, 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 los EE. UU.
    - 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 estadounidentes para ello. Si no se está de acuerdo al resultado del arbitraje, puede recurrirse ante los tribunales. Si la reclamación se efectuara contra una

autoridad pública estadounidente, se activa el mecanismo del *Ombudsperson*, un alto funcionario de EEUU 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, auditorias, 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 EE.UU adoptó la ley de recurso judicial que permite salvaguardar la protección de los derechos y datos provenientes de la Unión[115].

Tras la publicación y entrada en vigor de la decisión, el GT29 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 EEUU con fines comerciales.

Pero no todo es positivo en esta nueva decisión: la falta de concreción de determinados conceptos y la poca rigidez en las obligaciones impuestas a los Estados Unidos[116], 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*[117], 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"*[118]; aunque recientemente **se ha**

[115] Public Law No: 114-126 (02/24/2016).
[116] *Vid.* Wolters Kluvier, «El "Escudo de Privacidad" entre la UE y EE.UU. necesita mejorar», en *Diario La Ley*, Nº 8760, Wolters Kluvier, Madrid, 2016.
[117] Executive Order 13768. 27 de enero de 2017.
[118] Public Law No: 115-22 (04/03/2017).

nombrado al nuevo *ombudsperson*, cargo desinado a dirimir las reclamaciones relacionados con el *Privacy Shield*.

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[119] donde ha lamentado las nuevas reformas estadounidenses y pide a la Comisión Europea medidas destinadas a asegurar los principios estipulados en la Decisión. Por estos motivos, es **debemos mantener una postura cautelosa respecto al cumplimiento por parte de la nueva administración estadounidense del Escudo de Privacidad e, incluso, temer por la supervivencia del escudo cuando en septiembre se procederá a la revisión conjunta de la Decisión**.

[119] (2016/3018(RSP)).

V. Tratamiento ilícito de los datos: Reclamaciones de los afectados desde el Derecho internacional privado.

V. Tratamiento ilícito de los datos: Reclamaciones de los afectados.

Los tratamientos de datos personales **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 del origen de las mismas 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 cualesquiera 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 establecer 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, y por otro, 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 extracontrac**tuales, 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 ésta responsabilidad.

El daño causado puede afectar tanto a la esfera patrimonial, que abarcará tanto la perdida efectiva como el lucro cesante, como a la esfera moral, que incluirá 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 si mismo considerado[120].

A partir de estas consideraciones, debemos resaltar que **la acción de responsabilidad contemplada en el RGPD se refiere a una responsabilidad**

[120] *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

extracontractual como 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 una empresa se haya comprometido a custodiar los datos conforme a la legislación vigente y a los fines que se determinen en el propio contrato.

Debido a que en la práctica resulta más común una reclamación extracontractual que una basada en un incumplimiento contractual, y que la explicación de esta última escapa del propio objeto de estudio, **abordaremos la reclamación de los afectados desde el punto de vista de una reclamación extracontractual**.

V.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[121]; al contrario que la Directiva, la cual se dedicaba en el artículo 23 a obligar a los Estados a configurar el derecho a la indemnización en sus ordenamientos internos. Es España, la transposición se realizó en el artículo 19 de la LOPD.

El artículo 82 establece la responsabilidad del responsable del tratamiento *que participe en la operación de tratamiento responderá de los daños y perjuicios causados*

[121] «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».

en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Se estables la responsabilidad del responsable cuando participe en una operación el 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 tercero 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 cómo lógica esta limitación, puesto que el encargado del tratamiento actúa por mandato del responsable[122].

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**[123]**.**

En este punto, cabe **distinguir una doble esfera de responsabilidad**[124]:

1. La que se deriva del incumplimiento de las disposiciones del RGPD y sus normas de desarrollo, que conlleva automáticamente a indemnizar el daño.
2. Demostrar la usencia de responsabilidad en el hecho 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[125]. La anterior afirmación hace que nos situemos en el supuesto del artículo 1902 del CC[126].pero es un mero espejismo; puesto que el mismo Considerando debe demostrar, además, la conformidad de

[122] *Vid.* RECIO GAYO, Miguel, «Acerca de la evolución de la figura del encargado del tratamiento», en *Revista de Privacidad y Derecho Digital,* nº 0, 2015.
[123] *Vid.* Considerando 146 del RGPD.
[124] LÓPEZ ÁLVAREZ, Luis Felipe, *Protección de datos personales*…, *op, cit,* pp. 176.
[125] *Vid.* Considerando 74
[126] «El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado».

las actividades del tratamiento con el RGPD. Esto conlleva a invertir a 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[127].

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 operacion de tratamiento al responsible y encargado si se demuestra que no es responsible 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**[128], por lo que se viene a buscar una reparación integral del daño sufrido. En cuanto a los daños morales, 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;

[127] *Vid.* PÁEZ MAÑÁ, Jorge, «Responsabilidades derivadas del…», *op, cit.*
[128] *Vid.* Considerando 146 del RGPD. En cuanto a la doctrina del TJUE, *Vid.* STJUE *Liffers* (Asunto C-99/15).

- Naturaleza de las personas consultantes de los ficheros.
- Que el afectado no haya podido acceder a servicios ofrecidos por las empresas consultantes.

El RGPD regula la responsabilidad solidaria del el 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.

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, de diferentes jurisdicciones. Ambas sentencias discuten sobre quién es el responsable del tratamiento de los datos, a lo que las salas dan respuestas contradictorias[129].

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

[129] *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° 8773, La Ley, Madrid, 2016, pp. 1-6.

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 casos la filial**; ya que según el TJUE, interpretando 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 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 STS 210/2016 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, está 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[130].

V.2. 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, el cual dispone que las acciones dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro 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[131].

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»[132], 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 cuando se estudie**

[130] 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 del RGPD.
[131] 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.
[132] DOUE L 351/1, de 20 de diciembre de 2012.

caso por caso el objeto del contrato[133]. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente; Aunque también podemos encontrar supuestos (la mayoría de ellos) de responsabilidad extracontractual, sin que quepa admitir el supuesto dentro del objeto contractual, como pueden ser las transferencias internacionales de datos ilícitas.

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**»[134]. 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 considerar 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[135], **siendo posible considerar como «establecimiento» un representante de la sociedad si actúa con un grado de estabilidad suficiente**[136].

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

[133] *Vid*. SSTJUE de 13 de marzo de 2014, *Brogsitter*, C-548/12; 14 de julio de 2016, *Granarolo*, C-196/15.
[134] *Vid.* Apartados 31 de la sentencia *Weltimmo* y apdo. 75 de la sentencia *Amazon EU Sàri*.
[135] *Vid.* Apartados 76 y 77.
[136] *Vid.* Apartado 30 de la STJUE *Weltimmo*.

necesario que el afectado **tenga un grado de permanencia que revele una situación de estabilidad**[137].

La residencia habitual no es un concepto sinónimo al de «centro de intereses de la víctima» que promulga la STJUE *eDate Advertising*, 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**[138]. Por lo que se puede dar el caso, por ejemplo, de que una persona conocida en Islandia que resida en España sin que sea conocido, sufra una difamación en España. En este supuesto, el nacional islandés podrá demandar ante los tribunales españoles, aunque no se haya producido efectivamente el daño. 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[139]. **En este sentido, creemos que hubiera sido mejor el criterio del Abogado General del asunto estudiado, el cual proponía como criterio para determinar la competencia –el cual rechazó seguir el TJUE– el «centro de gravedad del conflicto»**. Este criterio bebe del asimilado por el TJUE, que lo consagra como el lugar **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, y
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 ésta contenga o las palabras clave que se han

[137] *Vid.* STJUE 22 de diciembre de 2010, C-497/10, *Mercredi*.
[138] *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*, Nº.4, 2013, pp. 23.
[139] *Ibídem.*

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.

Observando lo anterior, revela que **el RGPD pone a disposición de los afectados la posibilidad 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 recogidos en el RGPD son complementarios a los recogidos por el Reglamento Bruselas I bis**[140]. Por lo que podemos distinguir diferentes de foros:

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**[141]. 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**

[140] *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 2015, *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40, pp. 23.
[141] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional de datos», en *Revista boliviana de Derecho*, Nº 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013, pp. 138.

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 Tácita** (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[142]; 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**.
3. **Foro del domicilio del demandado** (artículo 4 Bruselas I bis). Este foro de competencia en 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, el cual 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**[143], 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.

[142] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional…», *op, cit,* pp. 139.
[143] 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».

4. **Foro especial en materia de obligaciones extracontractuales: el «lugar donde se hubiere producido o pudiere producirse el hecho dañoso»**. En el Reglamento Bruselas I bis encontramos en el artículo 7.3) un foro especial (y concurrente con el anterior) en el caso de efectuar una acción por daños y perjuicios. La competencia del tribunal del lugar donde 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[144]:
    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).

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 tienen lugar 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 sistema 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

[144] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional…», *op, cit,* pp. 142.

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*[145], 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 el 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).

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 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: 1) por un lado, establecer un foro de protección especial para la parte que ha sufrido el daño y perjuicio, que 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; 2) 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**.

[145] STJCE de 7 de marzo de 1995, Asunto C-68/03, *Ixora Trading Inc; Chequepoint SARL, Chequepoint International Ld. C Press Alliance SA*.

Ejemplo 5. Competencia judicial internacional del RGPD

El afectado, residente en Austria, pero con intereses económicos 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 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 Tácita. Artículo 26 Bruselas I bis**).
c) Que decida demandar en en los Estados en los que el responsable posea un establecimiento (**Foro del domicilio del demandado**. **Artículo 4 Bruselas I bis/foro del establecimiento del responsable. Artículo 79.2 RGPD**).
d) Que demande en su Estado de residencia (**Foro de la residencia habitual del demandante. Artículo 79.2 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»**. **Reglamento Bruselas I bis. Artículo 7.3**))

V.3. Determinación de la Ley aplicable a la controversia.

En el apartado III estudiamos la ley aplicable en cuanto a las operaciones de tratamiento sujetas al régimen del RGPD, **cuya aplicación es imperativa debido a que el RGPD viene a proteger el derecho fundamental internacionalmente reconocido a la protección de datos**[146].

[146] *Vid.* DE MIGUEL ASENSIO, Pedro Antonio, «Competencia…», *op. cit,* pp. 39.

La primacía de la legislación de protección de datos **se manifiesta en una limitada autonomía de la ley aplicable en una cláusula contractual, la cual 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 Roma I**. Podemos tomar como ejemplo la STJUE *Amazon EU Sàri,* la cual **determinó como ilegales cláusulas contractuales que contradecían a la legislación sobre protección de datos**. Por ello, se ha previsto la unificación de la norma de conflicto en los supuestos de ejercicio de la acción de indemnización.

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»**[147].

El Reglamento «Roma II» es un texto legal con **carácter universal**[148]; 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**[149]; 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[150], exclusión muy criticada por la doctrina[151]. 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***[152]. La reforma del Reglamento Roma II incluye un nuevo artículo 5 bis en el que introduce **dos nuevos supuestos: 1) la**

[147] DOCE L 199/40, de 31 de julio de 2007.
[148] *Vid*. artículo 3.
[149] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos…, op, cit,* pp. 138.
[150] *Ibídem* nota 236, pp. 42.
[151] *Vid.* DICKINSON, Andrew, *The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008, pp. 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° 8661, La Ley, Madrid, 2015, pp. 8; BRKAN, Maja, «Data Protection…», *op. cit,* pp. 27-28, y DE MIGUEL ASENSIO, Pedro Alberto, «Competencia…», *op. cit*, pp. 41-42.
[152] P7_TA-PROV(2012)0200.

ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño o perjuicio», o 2) «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».

El supuesto del primer inciso adopta los criterios de la *lex loci damni* (la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño) o *lex loci delicti commissi* (la ley del país en el que se produzcan o sea más probable que se produzcan 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[153]. 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).

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**.

[153] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «La (des) protección…», *op. cit,* pp. 8.

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)**.

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 ilícitos que se suelen desarrollar en otros Estados, el cual 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**[154]. Entonces, para poder aplicar la legislación española**,** a) el responsable del fichero tuviera su domicilio fuera de la UE y, b) el tratamiento de datos se hubiera realizado en España.

En cuanto a la segunda opción (*lex loci damni*), Frecuentemente **es el lugar donde se manifiesta la consecuencia directa para la víctima, que 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**; pero como hemos comentado a raíz de la STJUE *eDate Advertising*, no solo se materializa el perjuicio en el Estado de residencia habitual, también en aquel estado en el que existan un vínculo estrecho con ese otro Estado.

Debido a los ya resaltados problemas, conviene que ahondemos en **la crítica al precepto**[155]:

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

[154] *Vid*. ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos…, op, cit,* pp. 143.
[155] *Vid.* ORTEGA GIMÉNEZ, Alfonso, «La (des) protección…», *op. cit,* pp. 7.

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 parte 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 del RGPD invita a aplicar aplicar «la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado»**[156]. 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 correspondan 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[157].

[156] *Vid.* DE MIGUEL ASENSIO, Pedro Alberto, «Competencia…», *op. cit*, pp. 42.
[157] *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*, Nº 10, Aranzadi, Cizur Menor, 2016, pp. 6.

VII. 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 el derecho a la protección de datos de los sujetos. Las consecuencias reales del *Big Data* se manifiestan en un peligroso deterioro de la privacidad y la pérdida de oportunidades por determinados afectados. No son pocas las instituciones que advierten de los usos éticos del *Big Data* a la hora de plasmarlo en sus productos y en sus relaciones con potenciales clientes. Es destacable el peligro latente de la toma de decisiones basadas totalmente en tratamientos automatizados, cuyo impacto en la sociedad crearía un efecto «deshumanizador», costumbrista, y nocivo.

Segunda.- El *Big Data* no es una herramienta de futuro, lo es también de presente. El uso de los datos permite a las empresas crear productos a medida para adaptarse a un mercado cada vez más personalista y heterogéneo, además de otorgar los medios necesarios para la prevención del fraude entre otros. 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, la cual puede traer graves efectos colaterales para otros posibles clientes, puesto 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.- 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, la cual se veía superada por el avance de nuevas tendencias tecnologías 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 3 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 art. 3.2 b), el cual 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 personales

de los ciudadanos de la Unión estén protegidos incluso más allá de del territorio, 2) y se protegen los tratamientos de datos que controlen el comportamiento, objeto del *Big Data*.

Cuarta.- 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.

Quinta.- 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 homogenizar 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, las cuales se rigen fundamentalmente de las Decisiones de la Comisión.

Sexta.- 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.

Séptima.- **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 unificando 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.

Octava.- **El sistema de Derecho internacional privado que instaura el RGPD cumple 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 la parte demandada, aparte de añadir una mayor disposición de foros para el afectado. La equiparación de la ley aplicable en la controversia a la del Estado donde se litiga otorga una mayor seguridad y unidad a los afectados, que vuelven a beneficiarse de la función protectora del RGPD.

IX. Bibliografía consultada

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*, Nº 9, Aranzadi, Cizur Menor, 2015.

ALBRECHT, Jan. Phillipp y JOTZO, Florian, *Das neue Datenschutzrecht der EU*, Baden-Baden, Nomos, 2017.

ÁLVAREZ HERNANDO, Javier, y CAZURRO BARAHONA, Victor, *Practicum Protección de datos 2016*, Aranzadi, Cizur Menor, 2015.

BATISDA FREIJEDO, Francisco José, *Teoría General de los Derechos Fundamentales en la Constitución Española de 1978*, Tecnos, Madrid, 2004.

BELTRÁN AGUIRRE, Juan Luís, «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 relativo a la Protección de Datos», en *Diario La Ley*, nº 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, Nº 1, The Bucharest University of Economic Studies, Bucarest, 2010.

BOOBIER, Tony, *Analitics for Insurance,* WILEY, Chichester (RU), 2016.

BRKAN, Maja, «Data Protection and European Private International Law», Julio 2015, *Robert Schuman Centre for Advanced Studies,* Research Paper No. RSCAS 2015/40.

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.

BUYYA, Rajkumar, CALHEIROS, Rodrigo, y VAHID DASTJERDI, *Big Data: Principles and Paradigms*, Elsevier, Ámsterdam, 2016.

CARRASCOSA GONZÁLEZ, Javier; y CALVO CARAVACA, Antonio-Luis (Dirs.), *Derecho internacional privado*, vol. II, 16ª 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, *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones*, Fundación VODAFONE, Madrid, 2004.

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, Nº 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, nº 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° 8773, La Ley, Madrid, 2016.

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*, nº 6, Aranzadi, Cizur Menor, 2016.

DICKINSON, Andrew, *The Rome II Regulation (The Law Applicable to Non-Contractual Obligations),* Oxford, OUP, 2008.

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», en *CIO*, julio, 2012.

ERDOZÁIN LÓPEZ, José Carlos, «La protección de los datos de carácter personal en las telecomunicaciones», en *Revista Doctrinal Aranzadi Civil-Mercantil,* nº 1, Aranzadi, Cizu Menor, 2007.

ESPLUGUES MOTA, Carlos (Dir.), *Derecho del comercio internacional*, 7ª edición, Tirant lo Blanc, 2016.

GARCÍA NOBLIA, Analore, «¿Realmente cambiará el Consentimiento el Reglamento Europeo?», en *Noticias Jurídicas*, noviembre, 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.

GANDOMI, Amir y HAIDER, Murtaza, «Beyond the hype: Big data concepts, methods, and analytics», en *International Journal of Information Management*, nº 35, Elsevier, Amsterdam, 2015.

GIL GONZÁLEZ, Elena, *Big Data, Privacidad Y Protección de Datos*, AEPD, Madrid, 2016.

GONZÁLEZ ROYO, Ignacio, y PINA, Carolina, «¿Cómo se protegen legalmente los algoritmos?», en *Diario La Ley*, Nº 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*, Nº 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*, Nº 14, 2014.

HIJMANS, Hielke, *The European Union as Guardian of Internet Privacy: The Story of Artículo 16 TFEU*, Springer, Bruselas, 2015.

JAIN, Vijay Kumar, *Big data and Hadoop*, Khanna Publishing, Nueva Delhi, 2017.

JOYANES AGUILAR, Luis, *Big Data, Análisis de grandes volúmenes de datos en organizaciones*, Alfaomega, México D.F, 2013.

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.

LANEY, Douglas, «3D Data Management: Controlling Data Volume, Velocity and Variety». *Gartner*, febrero, 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 Tradeoff Between Privacy and Utility in Data Publishing», en *CERIAS Tech Report 2009-17*, 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*, nº 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.

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*, Nº.4, 2013.

ORTEGA GIMÉNEZ, Alfonso, «Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield», *Revista Lex Mercatoria Doctrina, Praxis, Jurisprudencia y Legislación*, nº 4, Universidad Miguel Hernández, Elche, 2016.

ORTEGA GIMÉNEZ, Alfonso, «Imagen y circulación internacional de datos», en *Revista boliviana de Derecho*, Nº 15, Fundación Iuris Tantum, Santa Cruz (Bolivia), 2013.

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° 8661, La Ley, Madrid, 2015.

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*, Nº 10, Aranzadi, Cizur Menor, 2016.

ORTEGA GIMÉNEZ, Alfonso, *Transferencias internacionales de datos de carácter personal ilícitas*, Aranzadi, Cizur Menor, 2017.

PAAL, Boris, y PAULY, Daniel, (Coords.), *Datenschutz-Grundverordnung*, C.H. Beck, Munich, 2017.

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 la privacidad UE-EE. UU», en *Actualidad Administrativa,* Nº. 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.

PUYOL MORENO, Javier, «Una aproximación al Big Data», *Revista de Derecho UNED*, nº 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 organisations can unlock value and insight from the information they hold», 2015.

RAYO 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.

RONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010.

ROSELLÓ MALLOL, Víctor, «Marketing y Protección de Datos (I). Concepto de dato personal», en *Noticias Jurídicas*, diciembre de 2009.

SANCHO VILLA, Diana, *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010.

SÁNCHEZ BRAVO, Álvaro (Ed.), *Derechos humanos y protección de datos personales en el siglo XXI. Homenaje a Cinta Castillo Jiménez*, Punto Rojo Libros, Sevilla.

SOARES Sunil, *Big Data Governance. An Emerging Imperative*, MC Press, Boise (ID), 2012.

SOARES Sunil, «Not Your Type? Big Data Matchmaker On Five Data Types You Need to Explore Today», *dataversity.net*, junio, 2012.

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.

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.

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

VELASCO NÚÑEZ, Eloy, «Tecnovigilancia, geolocalización y datos: aspectos procesales penales», en *Diario La Ley*, nº 8338, La Ley, Madrid.

VIVAS TESÓN, Inmaculada, «La tutela "sui generis" de las bases de datos», en *Revista de Derecho Patrimonial*, Nº 21, Aranzadi, Cizur Menor, 2008.

ZABÍA DE LA MATA, Juan, *Protección de datos: comentarios al reglamento*, Lex Nova, Madrid, 2009.

ZIKOPOULOS, Paul *Harness the power of big data, the IBM Big data platform*, McGraw-Hill, 2013.

X. Enlaces web consultados

Agencia Española de Protección de Datos

https://www.agpd.es

Grupo de Trabajo del Artículo 29

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Boletín Oficial del Estado

https://www.boe.es

Supervisor Europeo de Protección de Datos

https://edps.europa.eu/edps-homepage_en?lang=es

Parlamento Europeo

http://www.europarl.europa.eu/madrid/es/portada.html