VNIVERSITAT DE VALÈNCIA

FACULTAD DE DERECHO

PROGRAMA DE DOCTORADO EN ESTUDIOS JURÍDICOS, CIENCIA POLÍTICA Y CRIMINOLOGÍA

TESIS DOCTORAL

De los microdatos a los datos masivos. Cuestiones legales.

PRESENTADA POR

María Loza Corera

DIRECTOR

Javier Plaza Penadés

Mayo de 2017

VNIVERSITAT DE VALÈNCIA

FACULTAD DE DERECHO

PROGRAMA DE DOCTORADO EN ESTUDIOS JURÍDICOS, CIENCIA POLÍTICA Y CRIMINOLOGÍA

TESIS DOCTORAL

De los microdatos a los datos masivos. Cuestiones legales.

PRESENTADA POR

María Loza Corera

DIRECTOR

Javier Plaza Penadés

Mayo de 2017

A mis padres, Mª Cruz y Rafael,
por tanto y por todo.

“People talk about data being the new oil, [but] I think ultimately it's going to be like the new water”

Joel GURIN, fundador de OpenDataNow.com.

“Lo más grande de los seres humanos es precisamente lo que no revelan los algoritmos y los chips de silicio, aquello que no pueden revelar porque no puede ser capturado en forma de datos”.

Viktor MAYER-SCHÖNBERGER y Kenneth CUKIER

ÍNDICE

ÍNDICE **9**

INTRODUCCIÓN **13**

CAPÍTULO I : *BIG DATA* **17**

1.Concepto de *Big data* **17**

1.1 Cambio de paradigma 28

1.2 Datos abiertos. Concepto, origen y normativa aplicable 32

2. Utilidades del *Big data* **39**

2.1 Sector publico / sector privado 41

CAPÍTULO II : ENCUADRE JURÍDICO DEL *BIG DATA* **45**

1. Derecho de protección de datos de carácter personal **45**

1.1 Origen y delimitación 45

1.1.1 Origen del derecho 46

1.1.2 Derecho a la intimidad 55

1.1.3 Bien jurídico protegido 59

1.1.4 Contenido esencial del derecho a la protección de datos. Configuración jurisprudencial 61

1.2 Reconocimiento normativo y principios 72

1.2.1 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) 72

1.2.2 Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de carácter personal, (LOPD) 76

1.2.2.1 Objeto 77

1.2.2.2 Ámbito de aplicación 78

1.2.2.3 Definiciones 90

1.2.2.4 Principios 92

1.2.2.4.1 Principio de Calidad de los datos 92

1.2.2.4.2 Deber de información en la recogida de los datos 100

1.2.2.4.3 Principio de Consentimiento 113

1.2.2.4.3.1 Características del consentimiento: inequívoco e informado 115

1.2.2.4.3.2 Excepciones al Principio del consentimiento 123

1.2.2.4.3.3 Revocación del consentimiento 130

1.2.2.4.3.4. Datos especialmente protegidos 132

Especial referencia a los datos genéticos 142

1.3 Marco jurídico 146

1.3.1 Internacional 146

1.3.2 Normativa comunitaria 158
1.4 Evolución del derecho a la protección de datos 201
2. Los datos como un bien económico 248
2.1 Economía digital. Impacto del *big data* en la economía 248
2.2 ¿*Big data* como nuevo bien jurídico? 266
2.3 Derecho de acceso a la información 267
2.3.1 Sector Privado 267
2.3.2 Sector Público 272

CAPÍTULO III : EUROPA VS EE.UU. 275
1. El derecho a la privacidad en EE.UU. 276
1.1 Origen 276
1.2. Evolución 281
1.3. *Informational privacy*: el derecho a la protección de datos en EE.UU. 299
1.3.1 Dato personal vs *informational privacy* 300
1.3.2 Concepto FTC dato personal 302
2. Ámbito de aplicación de la normativa europea 308
2.1 Directiva 1995/46 de protección de datos de carácter personal 308
2.2 Reglamento europeo de protección de datos 315
2.3 El Escudo de privacidad o *Privacy Shield* 320

CAPÍTULO IV : PROBLEMÁTICA DEL *BIG DATA* 327
1.Posibles peligros del *big data* 327
2. *Big data* y protección de datos 332
2.1 Falta de transparencia y control 335
2.2 Anonimización y privacidad. Seudonimización 336
2.2.1 Anonimización: ¿Uso posterior compatible? 337
2.2.2 Irreversibilidad vs reidentificación 340
2.2.3 Principios de la anonimización 344
2.2.4 Técnicas de anonimización 346
2.3 Seudoanonimización 353
2.4 ¿Datos ya recogidos? metadatos y reidentificación 360
2.5 Toma automatizada de decisiones 369
2.6 Privacidad por defecto 379
2.7 Requisitos para el tratamiento 383

CAPÍTULO V : APLICACIÓN DE LA REGULACIÓN ACTUAL: PROBLEMÁTICA 393
1.Control sobre nuestros datos personales 393
2.Globalización 395

3.Problemas con actuales figuras 399
3.1 Concepto de dato personal 401
3.2 El individuo no decide 411
3.3 Vigencia del principio del consentimiento.....415
3.4 Derecho olvido y anonimización 428
3.5 Derecho de oposición a decisiones automatizadas.....445

CONCLUSIONES 451

BIBLIOGRAFÍA 465

INTRODUCCIÓN

Los datos siempre han estado ahí. Hasta ahora sólo nos daban información acerca de sus titulares, de ahí que hablemos de "datos personales". No obstante, ahora somos capaces de leer e interpretar lo que los datos pueden decirnos, y no sólo con respecto a su titular. La exactitud y calidad ceden en favor de la posibilidad de obtener correlaciones que nos revelen información en sí misma valiosa y no por constituir datos de carácter personal. Es la era de los datos masivos o *big data*. Donde el pasado nos ayuda a obtener información sobre el futuro o, como mínimo, sobre cómo manejarnos mejor en él.

Con la normativa de protección de datos de carácter personal actual, hemos conseguido que el titular de los datos decida quien, cuándo, cómo y qué operaciones se realizarán con sus datos, garantizando en todo momento su poder de disposición sobre los mismos, parte esencial del derecho fundamental a la protección de datos. Es lo que llamaremos el mundo de los "datos escasos" o microdatos.

La revolución en la que nos hallamos inmersos actualmente, nace de la posibilidad de analizar ingentes cantidades de datos que hasta ahora no disponíamos o no resultaban "interesantes" debido a la incapacidad técnica para poder interpretarlos. Únicamente eran valiosos precisamente por su relación con el titular de los mismos. En este momento ,"ni siquiera recurriendo a los datos masivos se puede predecir cómo van a evolucionar los datos masivos", así lo afirman Viktor Mayer-Schönberger y Kenneth Cukier en su libro "La Revolución de los datos masivos". Es por esto que resulta necesario e imprescindible plantearnos el escenario jurídico en el que esta nueva fuente de información ha de desenvolverse dadas las consecuencias directas que tiene sobre los derechos fundamentales de las personas, especialmente el derecho a la protección de datos y el derecho a la intimidad y de esta manera, aun no pudiendo predecir qué ocurrirá,

podemos establecer unos límites que a priori garanticen qué NO ocurrirá.

Se pondrá de manifiesto cómo el actual esquema jurídico que garantiza los derechos de los titulares de los datos deviene inservible en el mundo de los datos masivos. El reto es enorme, pues en un mundo globalizado, donde la protección jurídica no es uniforme, resulta que todos los principios asentados hasta la fecha, han de ser revisados desde otra perspectiva, y además, partiendo de modelos jurídicos diferentes (EEUU vs Europa).
En el presente trabajo, además de analizar los escenarios jurídicos existentes actualmente, intentaremos plantear las posibles alternativas que ante el fenómeno de los datos masivos, los agentes jurídicos han de sopesar. Todo ello, partiendo de la base de que ya estamos inmersos en el mundo de los datos masivos, aunque sin haber tomado conciencia de ello, es decir, sin que nadie nos lo haya "notificado" y mucho menos, solicitado consentimiento. Asímismo, si no se toman ningún tipo de medidas regulatorias al respecto, probablemente nos encontraremos con situaciones de abuso de poder por parte de las grandes multinacionales o incluso los gobiernos, en detrimento de los derechos de los titulares de datos, siendo prioritario por tanto garantizar un equilibrio de los diferentes agentes intervinientes que garantice un adecuado grado de protección.
Se plantearán cuestiones tales como si pasar del mundo de los datos escasos tal y como lo conocemos hoy, al mundo de los datos masivos, ha de suponer la renuncia por parte de los titulares de datos a determinados derechos, o si por el contrario, debe seguir vigente el Principio del consentimiento que preside el actual mundo de la protección de datos de carácter personal.
No supone un reto fácil, pues no se trata de *adaptar* los principios actuales de la protección de datos, sino que es necesario un ***completo ejercicio de análisis*** más allá de las fronteras marcadas por los mencionados principios y por tanto, debemos estar dispuestos a albergar nuevas categorías de datos, nuevos agentes intervinientes y en suma, ser capaces de definir el papel que juega el titular de los

datos dentro de este nuevo escenario, donde la anonimización, como se pondrá de manifiesto, no es una solución definitiva.

De forma pararela, desde un punto de vista sociológico, deberemos ser capaces de convivir con este tipo de predicciones, preservando la autonomía de voluntad en el lugar que se merece y evitando que determinadas finalidades subrepticias para las que los datos masivos pueden servir, condicionen nuestras decisiones y juicios.
También deberá resolverse la cuestión de qué hacer ante bases de datos ya existentes y que sirvan como tratamiento de datos masivos, es decir, si el titular dispone de algún derecho al respecto.
Ahora somos capaces de entender lo que los datos nos dicen, pero desde luego, no todo lo que nos dicen, así que sólo será cuestión de tiempo ver hacia dónde podemos llegar, pero no sin antes plantearnos los riesgos inherentes al tratamiento de datos masivos, y establecer unas reglas que hagan que la transición hacia la era de los datos masivos no se realice en beneficio de determinados intereses económicos y de poder, salvaguardando los derechos de las personas. Pero desde luego que no desaparecerá el mundo de la protección de datos tal y como lo conocemos hoy, sino que ambos sistemas están condenados a convivir.

CAPÍTULO I : *BIG DATA*

1.Concepto de *Big data*

Internet ha supuesto una revolución en todas las áreas de nuestra vida, la manera que tenemos de trabajar, de comunicarnos y relacionarnos con los demás, de comprar y vender, creando nuevos hábitos y costumbres, una nueva forma de vivir en definitiva.

Conforme vamos avanzando en la Sociedad de la Información, más se pone de relieve el debate entre seguridad y privacidad, lo privado (intimidad) y lo público, lo que debe permanecer o "borrarse" de internet y es ahora cuando mayor importancia adquiere la normativa en materia de protección de datos de carácter personal, que se ve obligada a trazar unos límites en un mundo no físico, que no conoce de distancias, barreras, tiempos ni olvidos.

La evolución en el ámbito de la informática con las distintas generaciones de ordenadores[1] junto con la irrupción de internet, ha desembocado en un proceso de **datificación** de nuestras vidas. Todo[2] es medible, analizable, y por tanto, rastreable. Es por ello que sin un proceso de datificación previo, no es posible hablar de *big data*. Siguiendo a MAYER-SCHÖNBERGER y CUKIER[3], "datificar" un fenómeno es plasmarlo en un formato cuantificado para que pueda ser

---

[1] Vid. GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Dykinson, 2016, pp. 18-19.

[2] MAYER-SCHÖNBERGER, V. y CUKIER, K., *Big Data. La revolución de los datos masivos*, Turner Publicaciones, 1ª edición Junio 2013, p. 98, ponen el ejemplo de Shigeomi Koshimizu, que consiguieron transformar en datos (datificar) la manera de sentarse de un conductor de un vehículo, midiendo con sensores la presión en 360 puntos diferentes del asiento e indexando cada punto en una escala de 0 a 256, obteniendo un código digital único para cada individuo. Como resultado, una nueva tecnología antirrobo de vehículos.

[3] MAYER-SCHÖNBERGER, V. y CUKIER, K., *op. cit.*, p. 100.

tabulado y analizado. Lo cual, precisan los autores, no es sinónimo de digitalizar que supone transformar información analógica en código binario para que sea procesable por un ordenador. Los autores ponen como ejemplo[4] para mostrar la diferencia entre digitalizar y datificar, el proyecto llevado a cabo por Google en 2004. Se digitalizaron millones de libros, escaneando todas sus páginas, pero no era posible hacer búsquedas sin saber qué libro podía contener la información, porque los libros no habían sido "datificados". Así, Google utilizó un programa de reconocimiento óptico de caracteres, que haría posible la búsqueda por palabras o frases. Pero no sólo eso, sería posible saber cuándo se utilizaron por primera vez determinadas expresiones o incluso comparar estilos de escritura lo cual podría ser muy útil en disputas sobre la autoría o detección de plagio. Es decir, gracias a la datificación, podemos alcanzar nueva información que antes no podíamos a partir de datos pasados, y además, generar nueva información sobre información que actualmente generamos pero inexistente en el pasado, como por ejemplo, la localización geográfica o el poder analizar el estado de ánimo de los usuarios[5]. La datificación nos permite monitorizar actividades que en el pasado eran invisibles. Y no sólo eso, pues si pensamos en el Internet de las cosas, los objetos diferentes al terminal móvil, también serán emisores y receptores de información, por lo que podemos pensar que en un futuro no muy lejano, poco quedará de este mundo sin datificar, y como señalan

[4] MAYER-SCHÖNBERGER, V. y CUKIER, K., *op. cit.,* pp. 106-107.

[5] La datificación de la información, aplicando técnicas de *big data*, puede ofrecernos información de la que antes no disponíamos, y como todo proceso que tecnológicamente se perfecciona, no sólo puede ofrecernos información digamos objetiva (trayectos realizados por una persona) sino también sobre sus actitudes y estados de ánimo. MAYER-SCHÖNBERGER y CUKIER citan (*op. cit*., p. 119) como ejemplo el caso de Salathé y Khandelwal, que descubrieron a través del análisis de tuits y sus metadatos, el análisis de sentimientos, lo cual en la práctica podía llegar a predecir comportamientos. Como muy acertadamente señalan los autores, las redes sociales y Google "están apostadas encima de un enorme cofre del tesoro lleno de información datificada que, una vez sometida a análisis, arrojará luz sobre la dinámica social a todos los niveles, desde el individuo hasta la sociedad en su conjunto".

MAYER-SCHÖNBERGER y CUKIER[6], "una vez se ha datificado el mundo, los usos potenciales de la información no tienen más límite que el ingenio personal".

Los factores que han creado el perfecto caldo de cultivo para el surgimiento del *big data* son 1) el abaratamiento de los sistemas de almacenamiento, 2) el aumento de la velocidad de procesamiento, 3) la evolución de los sistemas de procesamiento, 4) la datificación de la información. Ello hace que haya 5) aumentado exponencialmente la tipología y cantidad de datos que se generan y recogen. Todos estos factores hacen que se den las condiciones perfectas para el nacimiento del tratamiento masivo de datos.

En cuanto al concepto de *Big Data*, a primera vista, podría desprenderse del término que los datos tal y como los hemos conocido hasta ahora, eran "pocos" o "escasos", pero debemos interpretar "*big*" como abundante, debido a la ingente cantidad de datos que actualmente tenemos a nuestra disposición y podemos analizar, frente al mundo de los datos "escasos" anterior; no tanto porque fueran "pocos", sino porque o no existían (no se habían generado), o no estaban disponibles (no se habían datificado), bien por cuestiones de formato o bien porque no contamos con los medios tecnológicos para procesarlos e interpretarlos conjuntamente y, por tanto, explotarlos.

Hecha esta precisión previa, los datos masivos o *big data*, pueden definirse como grandes cantidades de datos que, mediante la aplicación de técnicas de procesamiento y estadísticas, permiten obtener conclusiones rápidamente sobre la probabilidad de que determinados sucesos o patrones puedan ocurrir.

Otros[7] lo definen como "la información que no puede ser procesada o analizada mediante procesos o herramientas tradicionales". No estamos muy de acuerdo con tal definición ya que únicamente podrá tener sentido en el presente, debido a que toma como parte de la misma las herramientas tecnológicas "actuales". Además, sólo incide

---

[6] MAYER-SCHÖNBERGER, V., y CUKIER, K., *op. cit.,* p. 121.

[7] PAREDES-MORENO, A., "Big Data: Estado de la cuestión". *International Journal of Information Systems and Software Engineering for Big Companies* (IJISEBC), 2015, vol. 2, n. 1, p. 40. Consultado el 13/07/2016 en www.ijisebc.com

en un aspecto del *big data*, como son las técnicas de procesamiento, cuando *big data* no sólo consiste en procesar grandes cantidades de datos.

Actualmente, es cierto que podíamos disponer de los datos pero no de las herramientas y conocimientos necesarios para procesarlos. Comenzamos a hablar de *big data* cuando podemos manejar ingentes bases de datos y, mediante los conocimientos necesarios, sabemos interpretar lo que dichos los datos nos pueden decir. Pero lógicamente, la tecnología no puede hacer sino mejorar, por lo que del mismo modo que ahora somos capaces de procesar bases de datos no relacionales, en un futuro probablemente podamos obtener información de la que ahora quizá no somos ni conscientes que podamos tener, es decir, tendremos mejores conocimientos y mejor tecnología para obtener nuevas informaciones[8] de los datos, tal y como está ocurriendo ahora, en los inicios del *Big Data*.

Cierto es que lo que se quiere poner de manifiesto con dicha definición en negativo, es que se aplican nuevas técnicas de análisis[9],

---

[8] Aquí debe hacerse referencia al concepto de lago de datos o *data lake*, que, siguiendo a AHMED BANAFA, supone el almacenaje de datos en su formato nativo hasta que sea necesaria su utilización, o cuando sepamos cómo utilizarlos. Al contrario que el almacenamiento jerárquico de datos (por ej. en carpetas), se almacenan utilizando una arquitectura plana asignando un identificador único a cada archivo que permite hacer consultas. El uso de un *data lake* permite conservar el archivo con todos los datos, sin eliminar ninguno, dotando de un potencial mayor valor a la información almacenada. El mero almacenaje de la información no equivale a utilizar técnicas de *big data* pero es la antesala de su utilización. Sobre las ventajas y desventajas de un "lago de datos", ver BANAFA, AHMED, "Un lago de datos: ¿una oportunidad o un sueño para el Big Data?", 07 diciembre 2015, disponible en https://www.bbvaopenmind.com/un-lago-de-datos-una-oportunidad-o-un-sueno-para-el-big-data/ Una de las principales desventajas es el riesgo que este tipo de repositorios supone para la privacidad.

[9] Siguiendo a TORRES I VIÑALS, J., "Del cloud computing al Big Data", FUOC. Fundación para la Universitat Oberta de Catalunya, Septiembre 2012, CC-BY-NC-ND, disponible en http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud_.Computing.al_.Big_.Data_.JordiTorres.ES_.pdf, pp. 25-27, "han surgido nuevas variedades de bases de datos (llamadas NoSQL) que permiten resolver los problemas de escalabilidad y rendimiento que el *big data*

estadísticas y de procesamiento, gracias a las cuales podemos hablar de big data, que hasta ahora no se utilizaban, ya que las técnicas tradicionales de bases de datos relacionales[10] no sirven para analizar grandes cantidades de datos. Por tanto, lo más conveniente sería referenciar en la definición a dichas técnicas "tradicionales" de análisis (bases de datos relacionales), o bien poner el énfasis, no sólo en la capacidad de analizar grandes cantidades de datos, sino que gracias a dicha capacidad podemos obtener determinadas respuestas o correlaciones. Es por ello que entendemos que big data no puede definirse simplemente como "aquella información que no puede ser procesada o analizada mediante procesos o herramientas tradicionales", pues big data es mucho más. La AEPD y ISMS Forum, en su Código de buenas prácticas para proyectos big data[11],

---

presenta. NoSQL aglutina las diferentes soluciones de bases de datos centradas al ser no relacionales, distribuidas y escalables de forma horizontal. Hay numerosos productos disponibles, muchos de ellos open source, como Cassandra, que pertenece al proyecto open source Hadoop (…). Las bases de datos NoSQL no suponen que no se haya de usar el SQL, sino simplemente que hay soluciones mejores para determinados problemas y aplicaciones. Por eso, NoSQL también lo podemos leer como not only SQL."Con respecto a los nuevos modelos de procesamiento, el autor menciona MapReduce de Google, y Hadoop MapReduce de Yahoo (open source). "La innovación clave de MapReduce es la capacidad de hacer una consulta, dividiéndola y ejecutándola en paralelo a la vez, a través de muchos servidores sobre un conjunto de datos inmenso. De este modo se resuelve el problema de los datos cuando son demasiado grandes para que quepan en una sola máquina. Este modelo tiene dos fases: 1) FaseMap, en la que los datos de entrada son procesados, uno a uno, y transformados en un conjunto intermedio de datos. 2) FaseReduce, donde estos resultados intermedios se reducen a un conjunto de datos resumidos, que es el resultado final deseado. Hoy por hoy es un proceso tipo batch, que puede requerir de minutos u horas para completarlo".

[10] Las bases de datos relacionales suponen que los datos se almacenan y consultan gracias a que previamente se han establecido unas relaciones ("relaciones base" o "relaciones derivadas"). Existen diferentes aplicaciones o programas informáticos para manejar bases de datos relacionales, entre los que destacan MySQL, Microsoft SQL server, DB2, Oracle etc

[11] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS y Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, *Código de buenas prácticas en protección de datos para proyectos Big Data* disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/G

entienden que con dicho término se hace referencia al "conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo". Como afirma[12] MATÉ JIMÉNEZ no tendremos una definición universal hasta que la Organización Mundial de Normalización (ISO) redacte la norma de vocabulario ISO 3534-5, dedicada al mundo del *big data* y la analítica predictiva. Hasta ese momento y a pesar del amplio uso del término *Big data*, no parece fácil ofrecer una definición del mismo y "no existe ninguna definición rigurosa de los datos masivos[13]". De hecho, desde la Universidad de Berkeley, concretamente desde su *Master of Information and Data Science (MIDS),* lanzaron la pregunta a más de cuarenta expertos de diferentes sectores[14] y hay definiciones "para todos los gustos"; desde aquellas que ponen el énfasis en la mera acumulación de datos o hasta las que lo denominan un cambio cultural, en el que las decisiones se toman en base a algoritmos.

Siguiendo a LANEY[15], ya en el año 2001 conceptualizó la denominada teoría de las tres "V": velocidad, volumen, y variedad, en base a las características del *Big Data*: manejar un gran volumen de información (en relación a la cantidad), procesar los datos a gran velocidad o en tiempo real (rapidez en la obtención de resultados interpretativos), integrar gran variedad de fuentes de información que podrían generar conocimiento a partir de conexiones no evidentes. Almacenamos

---

uias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf Licencia Reconocimiento- No comercial- Sin Obra Derivada 4.0 Internacional de Creative Commons, p 3.

[12] MATÉ JIMÉNEZ, C., "Big data. Un nuevo paradigma de análisis de datos". *Anales de Mecánica y Electricidad*, v. 91, Fasc. 6, 2014, p. 11.

[13] MAYER-SCHÖNBERGER, V., y CUKIER, K., *op. cit.*, p. 17.

[14] https://datascience.berkeley.edu/what-is-big-data/

[15] LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", Application Delivery Strategies, META Group Inc, 6 February 2001, File 949. Disponible en inglés en https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

información hoy para descubrir lo que nos pueda decir, si no es hoy, mañana.

En relación al **volumen,** automáticamente pensamos en la palabra "*big*" del término *big data*, debido a las grandes cantidades de datos que pueden analizarse. Ya no es necesario hacer análisis de una determinada muestra y extrapolar los resultados, pueden analizarse todos los datos a la vez, y eso es precisamente lo que aporta Valor.

Cada vez se crea y almacena una mayor cantidad de datos. En el año 2000 se generaron 800.000 petabytes (PB), de datos almacenados y se espera que esta cifra alcance los 35 zettabytes (ZB) en el 2020[16].

La **velocidad**, por la rapidez con que pueden obtenerse y procesarse los datos (ya no se utilizan procesos *batch* o procesamiento por lotes, sino que los datos se procesan en tiempo real gracias a que llegan al servidor por técnicas de *streaming* y por tanto directamente de la fuente generadora de la información*)* y la **variedad,** porque pueden utilizarse datos provenientes de múltiples fuentes y por tanto, en múltiples formatos (estructurados, no estructurados, semi-estructurados[17]). No obstante, precisar que no resulta del todo necesario obtener los datos de una gran variedad de fuentes, ya que quizá para determinados casos no es necesaria la combinación de tantas fuentes diferentes, pero además, no son éstas las que generan el conocimiento estrictamente, pues lo importante es realizar las preguntas adecuadas y combinar las bases de datos pertinentes para obtener las respuestas, esa es la dificultad, pues no por combinar muchas y muy diferentes bases de datos obtendremos mejores

---

[16] CAMARGO VEGA, J. J., CAMARGO ORTEGA, J. F., JOYANES AGUILAR, L., "Conociendo Big Data", *Revista Facultad de Ingeniería* (Fac. Ing.), enero-abril 2015, vol. 24, n. 38, p. 66.

[17] "Datos estructurados" son aquellos que tienen un determinado formato (ej números, palabras determinadas) y que pueden ser almacenados en bases de datos relacionales. "Datos no estructurados" son aquellos que carecen de un formato determinado y por tanto no encajan en bases de datos relacionales. Pueden ser texto, una imagen, audio etc. "Datos semiestructurados" son aquellos que, aunque no pueden ser tratados en bases relacionales por carecer de un formato definido, poseen una determinada organización que permite su tratamiento. Por ejemplo un documento html o xml.

respuestas, siempre será necesaria una suerte de *Business Inteligence* o analistas de datos, que sepan hacer las preguntas adecuadas en función de los fines perseguidos, a las bases de datos idóneas. No obstante lo anterior, hay quien piensa que de las tres "Vs", la variedad es la más importante, pues cuando procesamos información de fuentes externas, por muy grande que sea nuestra base de datos propia o interna, "se está haciendo algo cualitativamente diferente que puede ser denominado *big data*"[18].

En cualquier caso, las tres características (Volumen, Velocidad, Variedad) van intrínsecamente unidas, pues no podemos hablar de *big data* si los resultados se demorasen en el tiempo, o si no analizásemos grandes cantidades de datos y de diferentes fuentes y formatos.

Posteriormente, hay autores o empresas que han ido completando la definición con más "V". Por ejemplo, IBM añade la "Veracidad", en referencia a la posible alteración o incertidumbre de los datos. Así, IBM afirma[19] "la veracidad hace referencia al nivel de fiabilidad asociado a ciertos tipos de datos. Esforzarse por conseguir unos datos de alta calidad es un requisito importante y un reto fundamental de *big data*, pero incluso los mejores métodos de limpieza de datos no pueden eliminar la imprevisibilidad inherente de algunos datos, como el tiempo, la economía o las futuras decisiones de compra de un cliente. La necesidad de reconocer y planificar la incertidumbre es una dimensión de *big data* que surge a medida que los directivos intentan comprender mejor el mundo incierto que les rodea" . No estamos de acuerdo con esta característica de *big data (*veracidad*)*, pues precisamente entendemos que asociado a *big data* siempre hay que

---

[18] Informe de ICO, *UK Information Commissioner's Office*, "*Big data and data protection*", 28 de Julio de 2014, disponible en https://ico.org.uk/media/1541/big-data-and-data-protection.pdf, p. 7, epígrafe 25.

[19] Informe Ejecutivo de IBM Global Business Services Business en colaboración con la Escuela de Negocios Saïd en la Universidad de Oxford, "Analytics and Optimisation, Analytics: el uso de big data en el mundo real *Cómo las empresas más innovadoras extraen valor de datos inciertos",* IBM Corporation 2012, p. 5. Disponible en http://www-05.ibm.com/services/es/gbs/consulting/pdf/El_uso_de_Big_Data_en_el_mundo_real.pdf

asumir un margen de error[20]. Como afirman MAYER-SCHÖNBERGER y CUKIER[21] "lo que perdemos en exactitud en el nivel micro, lo ganamos en percepción en el nivel macro". Obviamente se realizarán esfuerzos por obtener los mejores datos, los más veraces, pero entendemos que es consustancial al *big data* la no fiabilidad de la totalidad de los datos, ya que siempre existirá un margen de error.

Otras opiniones[22] no favorables a la inclusión de esta cuarta "V" de Veracidad, afirman que tanto ésta como otras supuestas nuevas "V"(valor, validez, viabilidad etc.) "son características más propias para caracterizar a los datos, alejándose de las características del *Big Data* cuyas funciones son permitir el procesamiento masivo de muchos datos para generar información que antes resultaba inalcanzable con los sistemas tradicionales". No podemos estar más de acuerdo.

La OCDE es partidaria de incluir una cuarta V, relativa al valor. Opinan que, mientras las "clásicas" tres V son propiedades técnicas que por tanto dependerán de la evolución de las técnicas de almacenamiento y procesamiento, el Valor está relacionada con el creciente valor socioeconómico que se obtiene a partir de la utilización de los datos masivos. Opinan que es el potencial valor económico y social el que motiva la utilización de los datos, por lo que parece apropiado ir más allá de los aspectos técnicos (volumen,

---

[20] Al menos actualmente, ya que como afirman MAYER-SCHÖNBERGER y CUKIER, *op. cit.,* p 59, "la confusión no es algo inherente a los datos masivos. Se trata, por el contrario, de una función de la imperfección de las herramientas que usamos para medir, registrar y analizar la información. Si la tecnología llegara a ser perfecta, el problema de la inexactitud desaparecería".

[21] MAYER-SCHÖNBERGER y CUKIER, *op. cit.*, p. 26. En el mismo sentido, pp. 233 y 234. "No deberíamos aceptar datos que sean directamente incorrectos o falsos, pero algo de confusión sí puede aceptarse a cambio de captar un conjunto de datos mucho más amplio. De hecho en algunos casos, lo masivo y lo confuso pueden hasta representar una ventaja, dado que cuando intentamos usar únicamente una porción pequeña y exacta de los datos acabamos perdiendo la amplitud de detalle que encierra tanto conocimiento".

[22] "¿Cuántas V debería tener el Big Data?", Por Unidad de Innovación de Ingeniería del Software, de Indra Software Labs publicado en http://www.indracompany.com/es/blogneo/blogger/40494

velocidad, variedad) para ver la dimensión socioeconómica del *big data* como un nuevo "factor de producción"[23]. Así la OCDE afirma[24] que "la definición de las 3V y otras similares, se basan en propiedades técnicas vinculadas a la evolución de las tecnologías de almacenamiento y procesado de datos, y, por tanto, cambian continuamente". También opinan que estas definiciones se centran demasiado en los datos (lo cual es cierto para el Volumen) pero la Variedad y la Velocidad se centran en el análisis de esos datos. Por ello en lugar de centrarse en los "datos masivos", prefieren utilizar la expresión "innovación basada en datos".

En nuestra opinión, si bien es cierto que las clásicas tres V hacen referencia a aspectos técnicos, no por ello dejan de ser características del tratamiento de datos masivos, por mucho que las técnicas de procesamiento y almacenamiento evolucionen. De hecho, han pasado más de diez años desde su formulación y parece ser la definición más conocida y aceptada. Lógicamente, es el valor, es el resultado, el que mueve a utilizar técnicas de *big data*, pues es un *requisito sine qua non* realizar un planteamiento previo a la utilización de *big data*, para saber qué queremos obtener, qué preguntas realizar a los datos. Bien es cierto que podemos encontrar resultados o aplicaciones ni siquiera planteados en un inicio, pero siempre habrá un planteamiento previo en torno a la cuestión o problema que queramos analizar y mejorar con técnicas de *big data*. Consideramos que el Valor es el resultado, el conocimiento que nos permite introducir mejoras y optimizar

---

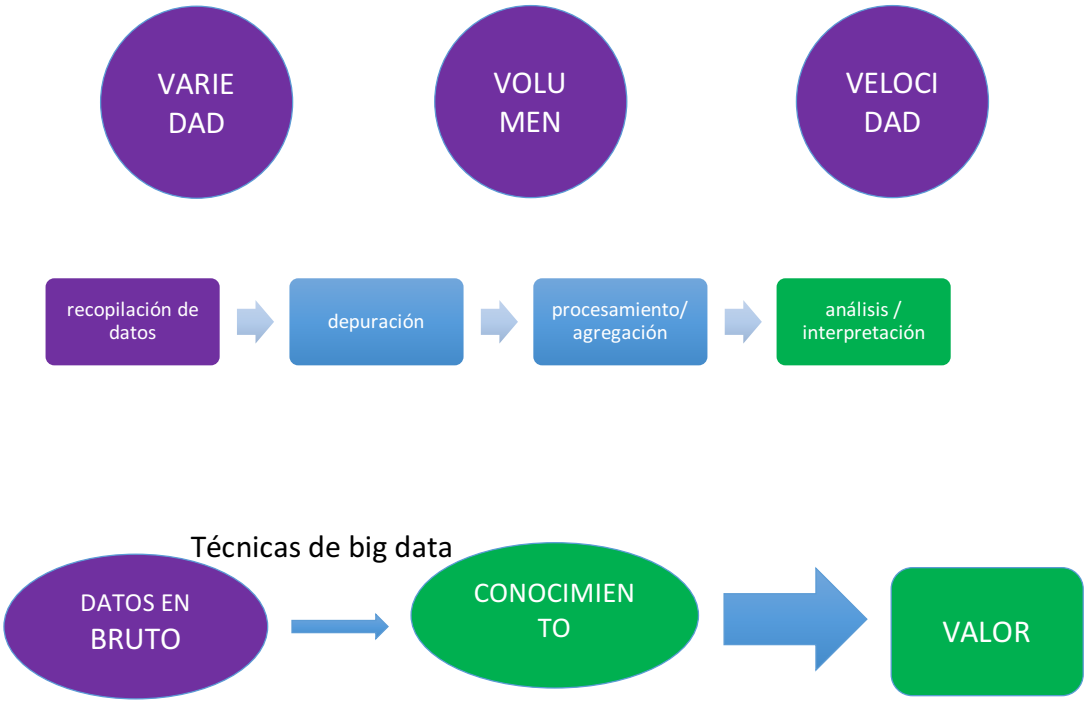
[23] OECD (2013), Working Paper "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by 'Big Data'", *OECD Digital Economy Papers*, n. 222, OECD Publishing, Paris, p. 12.

[24] OECD, *Perspectivas de la OCDE sobre la economía digital 2015*, Microsoft México, México D.F., 2016, p. 283. Disponible en http://www.oecd.org/sti/ieconomy/DigitalEconomyOutlook2015_SP_WEB.pdf

"Por otra parte, el término 'datos masivos' no indica cómo se utilizan los datos, los tipos de innovaciones que pueden desencadenar o la relación con otros conceptos, como 'datos abiertos', 'datos enlazados' o 'datos compuestos', entre otros. Por ello, el proyecto KBC2: DATA de la OCDE ha preferido centrarse no en el concepto de "datos masivos", sino en el de "innovación basada en datos", es decir, el uso de datos y analíticas para la innovación, el crecimiento y el bienestar.

procedimientos, gracias a la utilización de técnicas de *big data*, y en este sentido, es lógico que forme parte de la definición.

Tratamiento de datos masivos



Hoy en día disponemos de una gran cantidad de información, y como afirman MAYER-SCHÖNBERGER y CUKIER[25] "al tratar con conjuntos de datos cada vez más amplios, que captan no sólo un pequeño fragmento del fenómeno en cuestión sino muchas más partes del mismo, ya no necesitamos preocuparnos tanto por unos puntos de datos individuales que puedan sesgar el análisis global. Más que

[25] *Op. cit.*, p. 58.

aspirar a erradicar todo atisbo de inexactitud a un coste cada vez más elevado, calculamos con la confusión en mente".

Muchas veces se encuadra el *big data* dentro de la inteligencia artificial y específicamente dentro del área del aprendizaje automático o de máquinas (*machine learning*), pero siguiendo a MAYER-SCHÖNBERGER y CUKIER[26] en este punto, no es del todo correcto, ya que "el uso de datos masivos no consiste en enseñar a un ordenador a pensar como un ser humano. Más bien consiste en aplicar las matemáticas a enormes cantidades de datos para poder inferir probabilidades".

En 2013, WARD y BARKER[27], tras analizar las diferentes definiciones de *big data* más influyentes, intentaron obtener una única definición que reúna los requisitos comunes a las mismas sin entrar en contradicción. Así, concluyen que *big data* "es un término que describe el almacenamiento y análisis de conjuntos de datos de gran tamaño o complejidad, a través de una serie de técnicas que incluyen entre otras, NoSQL, *MapReduce* y el aprendizaje de máquinas (*machine learning*)".

1.1 Cambio de paradigma

"Lo más importante del Big Data es que supone un cambio de paradigma para el conocimiento", afirma CALABUIG[28]. En la misma línea, MATÉ JIMÉNEZ[29] afirma que "Big data representa un nuevo paradigma dentro del Análisis de Datos".

---

[26] *Op. cit.*, pp. 23 y 24.

[27] JONATHAN STUART WARD y ADAM BARKER, *Undefined By Data: A Survey of Big Data Definitions,* Universidad de St Andrews, UK, 20 de Septiembre de 2013, disponible en arXiv:1309.5821v1

[28] CALABUIG, O., "¿Qué es Big Data? Las entrañas de los datos". Dossier para el Institut de la Comunicació de la UAB, 2014. Consultable en http://portalcomunicacion.com/monograficos_det.asp?id=261

[29] MATÉ JIMÉNEZ, C., *op. cit.,* p. 16.

Siguiendo a MAYER-SCHÖNBERGER y CUKIER[30], los datos masivos tienen que ver con tres importantes cambios de mentalidad:
la capacidad de analizar enormes cantidades de información sobre un tema
disposición a aceptar la imprecisión y el desorden de los datos, en lugar de buscar la exactitud
respetar las correlaciones, en lugar de buscar la causalidad
Y es precisamente por estos cambios de mentalidad por lo que entendemos puede hablarse de un "cambio de paradigma".
Como señalan MAYER-SCHÖNBERGER y CUKIER [31], "puede que el día de mañana las generaciones siguientes tengan una conciencia de datos masivos: la presunción de que hay un componente cuantitativo en todo cuanto hacemos, y de que los datos son indispensables para que la sociedad aprenda". Podemos hablar de un cambio de paradigma a nivel tecnológico, pues hemos evolucionado hasta el punto de ser capaces de datificar todos los aspectos de la vida y ser capaces de analizar dicha información y obtener nuevos datos; pero también se produce un cambio de paradigma a nivel sociológico y humano, con consecuencias que no podemos obviar.
A nivel científico, se habla de *Big Data* como el "cuarto paradigma". Tradicionalmente el método científico se ha basado en dos paradigmas, la experimentación (*paradigma empírico*) y la teoría (*paradigma teórico*). Más adelante se añadió un tercer paradigma, la simulación computacional o *paradigma de la simulación*. A medida que el paradigma teórico fue evolucionando, la complejidad de sus teorías ya no podían experimentarse analítica o empíricamente, por lo que se recurrió a la simulación. Podríamos pensar que la simulación computacional forma parte de la experimentación misma (paradigma empírico), pero lo que diferencia a estos dos paradigmas, es que la simulación computacional utiliza datos generados a partir de programas informáticos, para simular fenómenos complejos.

---

[30] MAYER-SCHÖNBERGER y CUKIER, *op. cit.*, p. 33.
[31] MAYER-SCHÖNBERGER y CUKIER, *op. cit.*, p. 123.

Fue JIM GRAY[32] quien por primera vez incluyó al *big data* como el cuarto paradigma de la investigación científica (*paradigma de la computación intensiva de datos*). Gray observó lo que denominó el "iceberg de datos", es decir, tras una extensa investigación científica, en la que se producen multitud de datos y microinvestigaciones, luego únicamente se publica determinada información (el "iceberg de datos") quedando toda esa información no publicada, infrautilizada o no accesible. Es aquí cuando aparece la e-Ciencia[33], es decir, "donde las tecnologías de la información y los científicos convergen"[34]. Como afirma GRAY[35] no se trata de que toda la información se encuentre accesible a través de internet, sino de acceder de manera unificada a toda la información sobre determinada materia, no sólo a un concreto artículo de investigación, sino a toda la información que cita así como a los trabajos realizados con carácter previo, de modo que dicha información pudiera utilizarse en otras investigaciones.

En este sentido, ANDERSON[36] habla de la "era del *petabyte*", la cual entiende pondrá fin al método científico. "La era del *petabyte* es diferente porque más es diferente. Los kilobytes se almacenaban en disquetes. Los megabytes, en discos duros. Los terabytes, en sistemas *disk array* (matriz de discos). Los *petabytes* se almacenan en la nube. De igual modo que avanzamos en esa progresión, y fuimos de la analogía de la carpeta a la del archivador y de ahí a la de la biblioteca, al llegar al *petabyte* nos quedamos sin analogías organizativas. En la escala del *petabyte*, la información no es sólo una cuestión tridimensional —y tetradimensional— de simple taxonomía y orden

---

[32] Ver el libro tributo que sus compañeros de Microsoft publicaron: HEY, T., TANSLEY, S., & TOLLE, K. (eds.), *The Fourth Paradigm: Data-Intensive Scientific Discovery*: Microsoft Research, 2010.

[33] Término acuñado por John Taylor en el año 2000, siendo Director General de los Consejos de investigación del Reino Unido, vid. *op. cit., The Fourth Paradigm,* p. 245.

[34] The Fourth Paradigm, op. cit., p. xviii.

[35] The Fourth Paradigm, op. cit., p. xxvi.

[36] ANDERSON, C., "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete", publicado en *The Wire* el 23/06/2008 disponible en http://www.wired.com/2008/06/pb-theory/

sino de estadísticas dimensionalmente agnósticas. Esto exige un enfoque completamente distinto, que nos haga desprendernos de la red de datos como algo que pueda ser visualizado en su totalidad. Nos fuerza a ver los datos matemáticamente primero y establecer un contexto después". ANDERSON considera que ya no es necesario formular hipótesis sobre lo que los datos nos pueden mostrar, pues los algoritmos estadísticos pueden encontrar los patrones que la ciencia no puede, es decir, "los *petabytes* nos permiten decir: la correlación es suficiente".

No podemos coincidir con ANDERSON en este planteamiento, pues "el final de la teoría" sería, llevado al extremo, admitir como ciertas y causales las correlaciones encontradas. Creemos que una cosa es integrar el *big data* dentro del procedimiento de investigación, como una fuente de la que podemos obtener información, o incluso que nos descubra caminos que no nos habíamos planteado, pero eso no significa que podamos hablar del "fin de la teoría". Por el contrario, el filósofo BYUNG-CHUL HAN[37], sostiene que "no hay un pensamiento llevado por los datos. Sólo el cálculo es llevado por los datos", llegando a afirmar que "la masa de datos e informaciones, que crece sin límites, aleja hoy la ciencia de la teoría, del pensamiento", lo cual está claro no debemos dejar que ocurra, otorgando al *big data* su justo lugar.

Siguiendo a LYNCH[38] "en cierto sentido, el cuarto paradigma de Gray ofrece un marco integrador que permite la integración de los primeros tres y su mutuo fortalecimiento, de manera muy parecida al ciclo científico tradicional, en el que la teoría ofrecía predicciones que podían ser verificadas experimentalmente y estos experimentos identificaban fenómenos que requerían una explicación teórica".

En este sentido, WILBANKS[39], reacio a utilizar gratuitamente la expresión "cambio de paradigma", recuerda su origen en *La estructura de las revoluciones científicas*, de Thomas Kuhn, donde se produce un cambio de paradigma cuando un conjunto de ideas se

---

[37] BYUNG-CHUL HAN, "La agonía del eros", Herder, 2014, pp. 74 y 75.
[38] *The Fourth Paradigm*, *op. cit.*, CLIFFORD LYNCH, p. 191.
[39] *The Fourth Paradigm*, *op. cit.*, JOHN WILBANKS, p. 225.

vuelve dominante y se arraiga, creando una nueva visión del mundo. Para WILBANKS no estamos ante un cambio de paradigma en el sentido de Kuhn, "los datos no están barriendo la vieja realidad. Sencillamente están agregando una serie de cargas sobre las metodologías y los hábitos sociales con los que solemos abordar y comunicar nuestro empirismo y nuestra teoría sobre la solidez y la complejidad de nuestras simulaciones, y sobre la manera en que exponemos, transmitimos e integramos nuestro conocimiento".
En nuestra modesta opinión, coincidimos con WILBANKS en que no se trata, en propiedad, de un cambio de paradigma en el modelo de investigación científico, pues no se desecha el paradigma previo, como vaticinó ANDERSON, sino que simplemente estamos ante la irrupción del *big data* en el ámbito científico y de investigación, que como bien indica LYNCH, permite la integración de los primeros tres paradigmas y su mutuo fortalecimiento. Quizá podemos hablar de un "cambio de paradigma" en el sentido disruptivo que el *big data* causará en nuestras vidas a todos los niveles, incluyendo el de la investigación científica, pero no en el sentido definido por Kuhn. Sea como fuere, estemos ante un cambio de paradigma o no, lo que es indiscutible es que la forma de investigar así como de publicar lo investigado, sí que ha cambiado (o debería cambiar) gracias a internet y al tratamiento de datos masivos, pero sin que ello suponga en absoluto el "fin de la teoría".

1.2 Datos abiertos. Concepto, origen y normativa aplicable

Resulta interesante analizar el concepto de los datos abiertos, ya que constituyen una potencial fuente de datos para ser analizada con técnicas de *big data*.
El Manual sobre open data[40] (*Open Data Handbook*) los define como "datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando

[40] *Open Data Handbook* disponible en http://opendatahandbook.org/guide/es/

más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen".

La Comisión Europea publicó el *Libro Verde sobre la información del Sector Púbico en la Sociedad de la Información*[41] dando lugar así a una reflexión y debate en sede europea sobre la importancia de la información en manos de las Administraciones públicas.

La Comisión Europea pone sobre la mesa la importancia de la utilización de la información del sector público para el buen funcionamiento del mercado interior y para la libre circulación de mercancías, servicios y personas, ya que sólo así los agentes económicos podrán tomar decisiones con pleno conocimiento de causa. Así, una buena disponibilidad de la información pública incidirá en la competitividad de la industria europea. La Comisión Europea pone de relieve la gran desventaja competitiva que la UE tiene respecto a EE.UU., donde sí han sabido desarrollar "un sistema de información pública altamente desarrollado y eficaz a todos los niveles administrativos" lo cual ha fomentado enormemente el desarrollo de la industria de la información en EEUU. El hecho de que los ciudadanos y empresas no puedan utilizar la información pública disponible en cualquier estado miembro, "es algo anacrónico" y "constituye un desafío a los derechos garantizados a los ciudadanos por los Tratados comunitarios". La transparencia eliminaría las dificultades prácticas que puedan obstaculizar el libre ejercicio de las libertades fundamentales de los ciudadanos de la UE.

Con el objetivo de aumentar la transparencia, el Tratado de Ámsterdam estableció el derecho de acceso de cualquier ciudadano de la Unión, así como cualquier persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

Ante la falta de unos principios claros y coherentes sobre las condiciones de explotación de la información del sector público por parte del sector privado, se puso de manifiesto la necesidad de introducir un marco legislativo común europeo, desembocando en la

---

[41] COM 1998 (585) disponible en ftp://ftp.cordis.europa.eu/pub/econtent/docs/gp_es.pdf

aprobación de la Directiva 2003/98 CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, sobre la información del sector público. La Directiva establece[42] expresamente que no menoscabará ni afectará en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales. En España la Directiva se incorporó a través de la *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público* y su Reglamento, el Real Decreto 1495/2011, de 24 de octubre.

En Septiembre de 2010 la Comisión Europea lanzó una consulta pública sobre la Directiva 2003/98, en el marco del Plan de Acción de Administración Electrónica 2011-201543 que plasma las directrices marcadas en la Agenda Digital. Así, se aprobó la Directiva 2013/37/UE, de 26 de Junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. Como novedades más importantes que interesen al presente trabajo, destacar que se introducen nuevos conceptos[44], com "formato legible por máquina", "formato abierto", "norma formal abierta"; se añade entre los supuestos de no aplicación de la Directiva (artículo 1.2 c) quater "los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, y las partes de

[42] Artículo 1.4 Directiva 2003/98: "La presente Directiva no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales con arreglo a las disposiciones del Derecho comunitario y nacional, y, en particular, no altera las obligaciones ni los derechos establecidos en la Directiva 95/46/CE".

[43] https://ec.europa.eu/digital-single-market/european-egovernment-action-plan-2011-2015

[44] En el artículo 2 se añaden "6) 'un formato legible por máquina': un formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna";

7) 'formato abierto': un formato de archivo independiente de plataformas y puesto a disposición del público sin restricciones que impidan la reutilización de los documentos;

8) 'norma formal abierta': una norma establecida por escrito que especifica los criterios de interoperabilidad de la aplicación informática;

documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales";

Otra de las novedades que introduce la Directiva, es la introducción del Principio general de reutilización de datos, es decir, que la información pública pueda ser utilizada con fines comerciales y/o no comerciales, a diferencia de la Directiva anterior, que dejaba la decisión a los Estados o los organismos correspondientes.

En relación a las solicitudes de reutilización de datos (artículo 4) se modifican los apartados relativos a las Decisiones negativas, que quedan redactados así:

"3. En caso de adoptarse una Decisión negativa, los organismos del sector público comunicarán al solicitante los motivos de la denegación sobre la base de las disposiciones aplicables del régimen de acceso del Estado miembro correspondiente o de las disposiciones nacionales adoptadas con arreglo a la presente Directiva, en particular el artículo 1, apartado 2, letras a) a c quater), o el artículo 3. Si la Decisión negativa se basa en el artículo 1, apartado 2, letra b) *(derechos de propiedad intelectual de terceros)*, el organismo del sector público deberá incluir una referencia a la persona física o jurídica titular de los derechos, cuando esta sea conocida, o, alternativamente, al cedente del que el organismo del sector público haya obtenido el material en cuestión. Las bibliotecas, incluidas las universitarias, los museos y los archivos no estarán obligados a incluir tal referencia.

4. Toda decisión de reutilización deberá contener una referencia a las vías de recurso a que pueda acogerse en su caso el solicitante. Las vías de recurso incluirán la posibilidad de revisión por un órgano de revisión imparcial con la experiencia técnica adecuada, como la autoridad nacional de competencia, la autoridad nacional reguladora del acceso a los documentos o una autoridad judicial nacional, cuyas decisiones sean vinculantes para el organismo del sector público afectado".

En cuanto a los formatos disponibles (artículo 5) ya no bastará que los organismos del sector público faciliten sus documentos "en cualquier

formato o lengua en que existan previamente por medios electrónicos cuando resulte posible y oportuno", sino que se concreta que deberán facilitarse en "formato legible por máquina y conjuntamente con sus metadatos. Tanto el formato como los metadatos, en la medida de lo posible, deben cumplir normas formales abiertas". Se aclara que ello no significa que el sector público esté obligado a crear documentos, adaptarlos o facilitar extractos de documentos, cuando ello suponga un esfuerzo desproporcionado que conlleve algo más que una simple manipulación. Del mismo modo, no podrá exigirse a los organismos del sector público que mantengan la producción y el almacenamiento de un determinado tipo de documento con vistas a su reutilización por una entidad del sector privado o público.

Los Estados miembros crearán dispositivos prácticos que faciliten la búsqueda de los documentos disponibles para su reutilización, tales como listados de documentos principales con los metadatos pertinentes, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina, y portales conectados a los listados descentralizados. En la medida de lo posible, los Estados miembros facilitarán la búsqueda lingüística de los documentos en varios idiomas (artículo 9).

Respecto a las tarifas, se elimina la posibilidad de incrementar un margen de beneficio razonable de la inversión, pues ahora dicha tarifa se limitará a los costes marginales en que se incurra para su reproducción, puesta a disposición y difusión (Principio de los costes marginales).

Los Estados miembros presentarán, cada tres años, un informe a la Comisión, sobre la disponibilidad de información del sector público para reutilización, las condiciones que rigen su disponibilidad y las prácticas en materia de recurso. Dicho informe se hará público (artículo 13).

En el Ordenamiento español esta Directiva se transpone mediante la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Por otro lado, la OCDE aprobó en 2008 una *Recomendación*[45] *sobre acceso aumentado y uso más efectivo de la información del sector público*, actualmente en revisión, la cual establece una serie de principios para mejorar el acceso y uso de la información del sector público. Dichos Principios son:

- *Apertura*, como una regla por defecto, en el sentido de que la máxima información en poder del sector público, debe ser puesta a disposición, siendo las limitaciones muy concretas.
- *Acceso y transparencia en las condiciones de uso*: los sistemas de licencias y acceso deben ser sencillos, accesibles a través de internet y no establecer condiciones discriminatorias para el acceso.
- *Activos de Información*: la información disponible debe darse a conocer a través de listados o inventarios, así como las condiciones de acceso.
- *Calidad*: los métodos de recopilación, manipulación y almacenamiento deben cumplir con los estándares mínimos de calidad.
- *Integridad*: desarrollar e implementar las adecuadas salvaguardas para evitar modificaciones no autorizadas o denegaciones de acceso a la información.
- *Preservación*: los estándares que se utilicen deben asegurar la preservación de la información en el tiempo.
- *Derechos de propiedad intelectual*: deben respestarse los derechos de propiedad intelectual
- *Costes*: deben ser los menos posibles. No pueden exceder los costes de mantenimiento y distribución. En casos excepcionales podrá haber costes en la digitalización.
- *Competencia*: debe garantizarse un acceso igualitario a la información, no pudiendo darse situaciones que afecten a la libre competencia

[45] OCDE C, (2008), 36 Council Recommendation for Enhanced Access and More Effective Use of Public Sector Information, 30 de Abril de 2008. La Recomendación se revisa cada tres años.

- *Mecanismos de reclamación*: en relación a la información publicada, deberán existir mecanismos que permitan reclamar cualquier abuso en relación a la misma.
- *Alianzas público-privadas*: para aquellos casos en los que el sector público no pueda asumir determinados costes. No obstante, ello no podrá generar ningún tipo de privilegio o restricción en cuanto al acceso de la información por cualquier persona o empresa.
- *Uso internacional*: deberá fomentarse el uso transfronterizo de la información.
- *Mejores prácticas*: dar a conocer e incentivar las mejores prácticas en cuanto el uso y publicación de la información.

La OCDE publicó un estudio[46] en 2010, parte de la Estrategia de Innovación de la OCDE, en el que se pone de manifiesto que "el creciente interés de los gobiernos en la facilitación del acceso y la promoción del uso futuro de la información del sector público por parte de otras organizaciones del sector público, empresas e individuos, se basa en la expectativa de que el aumento del flujo y la reutilización de la información, la mayor competencia y el aumento de la actividad económica asociada con el uso comercial y no comercial contribuyen a la mejora de la eficiencia del gobierno, el crecimiento económico y el bienestar de los ciudadanos". No obstante, la OCDE es consciente de que existen obstáculos que impiden su "uso eficiente y eficaz", como por ejemplo, reglas restrictivas en relación al acceso a la información; en caso de que se pueda cobrar, altos e incongruentes precios; complejos procedimientos para obtener licencias; la distribución ineficiente a los usuarios finales; y las barreras para el desarrollo de los mercados internacionales y por ello se aprobó la

[46] *La estrategia de innovación de la OCDE. Empezar hoy el mañana* 2010, Organización para la Cooperación y el Desarrollo Económicos (OCDE), París, p. 168. Es el tercer volumen de un total de siete de la serie Estrategia de Innovación de la OCDE, coeditado con la Organización para la Cooperación y el Desarrollo Económicos. Disponible en castellano en http://www.foroconsultivo.org.mx/libros_editados/estrategia_innovacion_ocde.pdf

Recomendación anteriormente mencionada, para tratar de eliminar estos obstáculos.

2. Utilidades del *Big data*

Dejando a un lado los posibles inconvenientes que en materia de privacidad pueda suponer el *big data*, veamos ahora las utilidades que puede suponer este tipo de tratamiento de datos.

Big data no es simplemente almacenar grandes cantidades de datos. *Big data* es, analizar esas grandes y variadas cantidades de datos, y haciendo las preguntas correctas, obtener posibles patrones o respuestas relacionadas con una problemática concreta, que antes no teníamos (el "valor oculto de los datos").

Pensemos en un comercio, ¿y si pudiera saber qué día del año habrá más afluencia de clientes? ¿o cuándo se vende más determinado producto? Así podría prever el suficiente stock, personal para atender a los clientes y planificar determinadas ofertas. ¿cómo podría saberlo? Es lógico pensar que el propietario del comercio sabrá la cantidad de dinero que ha obtenido cada día, pero no el número de clientes. Podrían cuantificarse las operaciones realizadas, pero, ¿y cuántas unidades de un determinado producto se han vendido y en qué época del año? Es posible obtener estas y otras respuestas con técnicas de *big data.* Las utilidades del *big data* son muchas[47] y probablemente, desconozcamos todavía las aplicaciones que pueden darse.

Un ejemplo en el ámbito de la salud pública, mencionado por MAYER-SCHÖNBERGER y CUKIER[48], fue a raíz de un nuevo virus de la gripe en 2009 en EE.UU., para el cual no existía vacuna, por lo que el único remedio era evitar su propagación. Google fue capaz de diseñar un sistema que no se basaba exclusivamente en los términos de búsqueda introducidos por los usuarios, sino que buscaba correlaciones entre la

[47] PAREDES-MORENO, A., *op. cit.*, p. 52, cita diferentes áreas tanto del sector público como privado en las que se puede aplicar *big data*.

[48] MAYER-SCHÖNBERGER, V., y CUKIER, K., *op. cit.,* pp. 11-13.

frecuencia de ciertas búsquedas y la propagación de la gripe a lo largo del tiempo y del espacio. Además de poder saber por dónde se había propagado la gripe, podían hacerlo casi en tiempo real.

La industria de los servicios financieros genera (y almacena) una gran cantidad de datos. Además de las ventajas que el *big data* puede aportar a este sector, pensemos en la valiosa información de la que disponen. Las entidades financieras saben qué gastos hemos realizado, y por tanto, en qué lugar geográfico nos encontramos, qué gustos y costumbres tenemos en relación a nuestro poder adquisitivo o perfil de cliente, en qué momento realizamos determinadas compras etc. Podemos plantearnos si resulta ético o incluso legal, que dichas entidades utilicen nuestros datos, no ya para mejorar sus propios servicios y revertir en una mejora de sus clientes, sino para venderlos[49] a otras entidades que estén interesadas en dicha información, obteniendo una monetización. En el capítulo siguiente analizaremos en profundidad dicha cuestión.

Podemos plantear múltiples ejemplos casi prácticamente en cualquier ámbito de la vida, hasta en el método científico de investigación como se ha visto anteriormente, pero lo que está claro es que las empresas que utilicen técnicas de *big data*, podrán mejorar en competitividad, ya que ofrecerán mejores productos o servicios y los clientes se verán

---

[49] Juan Ramón Pujol, responsable de Big Data del Banco de Sabadell, afirmaba en *Expansión* (09/07/2015) que el principal reto "es saber qué hacer con todos estos datos. Crear un activo con nuestros datos y ofrecérselo a otras empresas para que puedan explotarlo, o bien centrar nuestros esfuerzos en mejorar la experiencia del usuario". "Nosotros por el momento no pensamos en monetizar nada, lo enfocamos más a la experiencia del cliente". Disponible en http://www.expansion.com/empresas/banca/2015/07/09/559e2f1d46163f14758b4578.html Por su parte, "BBVA quiere utilizar la información extraída de sus datos para que otras empresas puedan utilizarla en su toma de decisiones. De los datos del uso de las tarjetas de crédito, por ejemplo, se puede extraer una información muy valiosa de la auténtica realidad económica de un país, tanto por el tipo de compra como por la forma de pago o la evolución del comportamiento del consumidor. El BBVA asegura tener un activo muy relevante que quiere poner en valor. Está ya probando varios desarrollos". Información obtenida de http://www.media-tics.com/noticia/3864/dircom-2.0/la-caixa-bbva-y-bankinter-desarrollan-servicios-big-data.html (02/09/2014)

más satisfechos. Como afirma PAREDES MORENO[50], "Big Data permite obtener una imagen más completa de las preferencias y demandas de los clientes; a través de esta profunda comprensión empresas de todo tipo encuentran nuevas formas de interactuar con sus clientes actuales y futuros".

2.1 Sector publico / sector privado

Hasta ahora hemos visto las utilidades que el *big data* puede suponer para el sector privado, redundando en una mejora de la competitividad, ahorro de costes (mediante la optimización de procedimientos, detección del fraude, gestión eficiente del personal etc), desarrollo de nuevos productos y fidelización del cliente; pero no debemos olvidar que el sector público posee una gran cantidad de información (e.g. *open data*) y también puede aplicar técnicas de *big data.*

En 2013 la OCDE publicó un estudio[51] en el que se recogen cifras tales como que el uso de *big data* en los veintitrés gobiernos más grandes de Europa, reduciría los costes administrativos entre un 15 y un 20%, creando el equivalente de 150 a 300 billones de euros en nuevo valor y acelerando el crecimiento de la productividad anual en 0,5 puntos de porcentaje en los próximos diez años. Afirma el estudio que los principales beneficios serían una mayor eficiencia operativa (debido a una mayor transparencia), aumento de la recaudación de impuestos y un menor número de fraudes. Estudios similares del Reino Unido muestran que el sector público podría ahorrar 2 mil millones de libras esterlinas en la detección de fraudes y generar 4 mil millones GBP través de una mejor gestión del rendimiento mediante el uso de análisis de grandes volúmenes de datos.

---

[50] PAREDES-MORENO, A., *op. cit.,* p. 46.

[51] OECD, Working Paper "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by 'Big Data'", *OECD Digital Economy Papers*, n. 222, OECD Publishing, París, 2013. DOI: http://dx.doi.org/10.1787/5k47zw3fcp43-en

Pero los potenciales beneficios no quedan ahí. Señala el estudio como un área de creciente interés, la seguridad interna y el cumplimiento de la ley. Así, el uso de fuentes no tradicionales en este ámbito (como por ejemplo los SMS o redes sociales), pueden servir para completar las estadísticas oficiales de criminalidad. Ofreciendo a los ciudadanos medios digitales para reportar crímenes, el sistema de la *start-up* CitiVox, permite que los individuos permanezcan en el anonimato. Al mismo tiempo, los responsables políticos y los organismos de aplicación pueden extraer de los datos patrones de criminalidad que no serían detectados (o no lo suficientemente rápido) por las estadísticas oficiales. Las cifras anteriormente mencionadas, no incluyen los beneficios obtenidos a través de la provisión de la información del sector público, definida en la *Recomendación*[52] *del Consejo de la OCDE sobre mejora del acceso y utilización más eficaz de la información del sector público,* que supondría beneficios para la vida económica y social en áreas tan dispares como el tiempo, los atascos de tráfico, estadísticas de criminalidad local, librerías electrónicas etc.
Por su parte, la ONU ha impulsado el proyecto "GLOBAL PULSE[53]" en el que se asume el *big data* como un bien público para acelerar el descubrimiento, desarrollo y la adopción de la innovación para el desarrollo sostenible y la acción humanitaria en los países en desarrollo.

En sede europea, la Comisión Europea realizó en 2014 una Comunicación[54] al Parlamento Europeo, al Consejo, al Comité Económico y social europeo y al Comité de las regiones, en la que, siguiendo las conclusiones del Consejo Europeo de octubre de 2013, que abogaban porque la UE interviniera para establecer las

[52] OCDE C, (2008), 36.
[53] http://www.unglobalpulse.org
[54] Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las regiones, *Hacia una economía de los datos próspera,* COM/2014/0442 final.

condiciones marco adecuadas para un mercado único de los macrodatos (*big data*) y la computación en nube, trata de establecer las características de la futura economía de los datos.

Se afirma que estamos ante una "nueva revolución industrial impulsada por los datos digitales, la computación y la automatización" y que "esta tendencia mundial presenta un potencial enorme en diversos campos, que van desde la salud, la seguridad alimentaria o la eficiencia del clima y los recursos hasta la energía, los sistemas de transporte inteligentes y las ciudades inteligentes, que Europa no puede permitirse el lujo de descuidar", pues se es consciente de que "la economía digital europea ha sido lenta en adoptar la revolución de los datos en comparación con EE.UU.". Una de las causas, afirmaba la Comunicación, era la complejidad del marco jurídico existente, por lo que se concluía que la UE debía "concluir rápidamente los procesos legislativos sobre la reforma del marco de protección de datos de la UE y la seguridad de la información y de las redes, y apoyar el intercambio y la cooperación entre las autoridades pertinentes encargadas de su aplicación", así como asegurarse de que dicho marco jurídico y las políticas referentes por ejemplo a la interoperabilidad, la protección de datos, la seguridad y los derechos de propiedad intelectual fueran compatibles con los datos, dando lugar a una mayor seguridad reglamentaria para las empresas y conseguir la confianza del consumidor en las tecnologías de datos".

Asimismo, la Comunicación incluía entre sus conclusiones, la conveniencia de establecer una cooperación entre el sector público y privado, creando una asociación público-privada ("*the Big Data Value PPP*") europea de datos, que ve la luz el 13 de Octubre de 2014[55].

En 2017, y sobre la base de las conclusiones de la Comunicación mencionada de 2014, la Comisión Europea ha adoptado una nueva Comunicación[56] *Construyendo una economía europea de datos.* En

[55] Nota de prensa de la Comisión Europea http://europa.eu/rapid/press-release_IP-14-1129_es.htm

[56] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *Construyendo una economía europea de datos*, COM (2017) 9 final.

esta Comunicación, y tras la aprobación del RGPD y el proyecto de Reglamento sobre privacidad y comunicaciones electrónicas, el objetivo de la Comisión es crear un marco político y jurídico claro, adaptado para la economía de datos, suprimiendo las barreras que subsisten a la circulación de datos y abordando las incertidumbres jurídicas creadas por las nuevas tecnologías basadas en datos.

Nos enfrentamos por tanto al reto de regular los tratamientos masivos de datos provenientes tanto del sector público, sometido a las normativas sobre reutilización de la información pública (*open data*), como del sector privado, donde no existe regulación respecto a los datos no personales o anónimos, ni obligación de poner a disposición de terceros la información de que se dispone. En el sector público se ha establecido la obligación de poner la información a disposición de los diferentes agentes con fines privados o comerciales para "favorecer la circulación de información hacia los agentes económicos y la ciudadanía con el fin de fomentar el crecimiento económico, el compromiso social y la transparencia"[57]. La normativa francesa en materia de datos abiertos ha introducido la posibilidad de que el sector público pueda solicitar determinada información a entidades privadas siempre que ésta tenga "interés público". Vemos cómo se abre por tanto la posibilidad de establecer obligaciones sobre entidades privadas de compartir determinada información con el sector público, no siendo ya unidireccional el flujo de información. La Comisión Europea es consciente de que deben incluirse normas que incentiven al sector privado a compartir la información, ya que sólo así podremos hablar de una verdadera economía basada en datos. No obstante, este nuevo marco jurídico debe abordar cuestiones muy delicadas como el garantizar el derecho fundamental de protección de datos de los individuos, y el encaje jurídico que la creación de nuevos derechos sobre los datos no personales supone, pues como profundizaremos en el presente trabajo, la línea que separa los datos personales de la información no personal o anónima, es cada vez más difusa.

[57] Preámbulo de la Ley 18/2015.

CAPÍTULO II : ENCUADRE JURÍDICO DEL *BIG DATA*

Una vez analizado el concepto de *Big Data* y las utilidades del mismo, a la hora de plantearnos su encuadre jurídico debemos distinguir los siguientes escenarios o perspectivas:

a) la aplicación de la normativa de protección de datos de carácter personal, y por tanto, desde la perspectiva de la protección de un derecho fundamental
b) el valor de los datos como núcleo de la "futura economía de los datos", y por tanto, como un bien económico.

Ambas perspectivas abordan la protección de bienes jurídicos diferentes, pero queda claro en cualquier caso, cuál es el bien jurídico de protección preferente, por tratarse de un derecho fundamental de las personas. Esta situación conlleva que, en la práctica, se ha de ser muy cuidadoso en cuanto a las tipologías de datos tratados, no pudiendo excluir a priori de manera general la aplicación de la normativa de protección de datos.
Es por ello que resulta necesario analizar el origen y desarrollo del derecho fundamental de protección de datos y los Principios aplicables al mismo, para poder entender la importancia de la cuestión y así poder analizar las problemáticas que la nueva "economía de los datos" nos plantea, con especial incidencia en los tratamientos masivos de datos.

1. Derecho de protección de datos de carácter personal

1.1 Origen y delimitación

1.1.1 Origen del derecho

Hoy en día es indiscutible el carácter del derecho a la protección de datos como derecho fundamental y autónomo, pero no olvidemos que se trata de un derecho de los llamados de tercera generación[1] que ha venido configurándose jurisprudencial y doctrinalmente hasta verse positivizado en los diferentes Ordenamientos jurídicos[2].

No siempre fue pacífica la concepción del derecho a la protección de datos como un derecho fundamental autónomo. En un primer momento, la Doctrina que concibe el elenco de derechos fundamentales como una categoría estanca[3] basándose en una concepción predominantemente iusnaturalista o iusracionalista del sistema jurídico, lógicamente lo concibió como parte del derecho a la intimidad o como una garantía complementaria de la misma. No obstante, esta posición ha quedado superada imponiéndose el reconocimiento de un nuevo derecho fundamental. Así, no debemos pasar por alto su incardinación como derecho fundamental, es decir, epicentro del ordenamiento constitucional. Citando a LUCAS

---

[1] LUCAS MURILLO, P., *El Derecho a la Autodeterminación Informativa*, *Temas clave de la constitución española*, pp. 17 y 18, Tecnos, Madrid, 1990, p. 33 i.f. y 34, define los derechos de tercera generación como la categoría que "incluye aquellos derechos que pretenden satisfacer necesidades que las transformaciones tecnológicas de la sociedad post industrial ponen de manifiesto. Entran aquí por ejemplo, todas las repercusiones que, en el campo de los derechos, plantean la ecología o la preocupación por el medioambiente, la tutela del consumidor o de otros colectivos sociales con una problemática específica y, desde luego, la informática".

[2] Sobre el constitucionalismo de tercera generación vid. NOGUERA FERNÁNDEZ, A., "El Constitucionalismo de Tercera Generación: rompiendo la tensión entre la definición social del estado y el tratamiento constitucional degradado de los derechos sociales", *Anales de la Cátedra Francisco Suárez*, 43 (2009), pp. 245-265.

[3] LAPORTA F., "Sobre el concepto de derechos humanos", *Doxa* nº 4, 1987, p. 44 "(…) el ampliar más y más los catálogos de derechos humanos es incompatible con la mayoría de los rasgos que se predican de ellos" Cfr con ATIENZA, M., y RUIZ MANERO, J., "A propósito del concepto de derechos humanos de Francisco Laporta", *op. cit.*, y PÉREZ LUÑO, A. E., "Concepto y concepción de los derechos humanos (Acotaciones a la ponencia de Francisco Laporta)", *Doxa* nº 4, 1987 y ORTÍ VALLEJO, A., *Derecho a la intimidad e informática*, Comares, 1994, p. 48.

MURILLO: "El Estado como organización política jurídicamente organizada tiene su razón de ser en la realización de los derechos fundamentales. Sobre su observancia o, mejor, sobre la satisfacción de las necesidades materiales y morales que con ellos se pretende asegurar descansa el orden político y la paz social como, con expresión, a mi juicio afortunada, dice nuestra Constitución. Hablar del Derecho Constitucional como técnica jurídica de la libertad o recordar el artículo 2º de la Declaración de Derechos del Hombre y del Ciudadano, de 26 de Agosto de 1789, cuando dice: *La finalidad de toda asociación política es la consecución de los derechos naturales e imprescriptibles del hombre (...)* no es sino insistir sobre lo mismo"[4].

El artículo 18 de nuestra constitución garantiza el derecho a la intimidad en su párrafo primero y en el cuarto[5] la protege, junto al honor, del uso de la informática

1. Se garantiza el derecho al honor, a la **intimidad** personal y familiar y a la propia imagen.

4. La ley limitará el uso de la **informática** para garantizar el honor y la **intimidad** personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos

[4] LUCAS MURILLO, P., El Derecho a la Autodeterminación Informativa, Temas clave de la constitución española, pp. 17 y 18, Tecnos, Madrid, 1990.

[5] BAJO FERNÁNDEZ, M., *Comentarios a la Legislación penal,* Cobo del Rosal, M., (dir.), Bajo Fernández, M., (coord.), *Derecho penal y Constitución: Protección del honor y de la intimidad*, Edersa, Madrid, Tomo I, 1982, p. 121; sobre el debate en relación a la necesidad o no del párrafo cuarto del artículo 18, por entenderse incluidas en el primer párrafo todas las limitaciones necesarias para garantizar el derecho, el autor afirma: "Probablemente el constituyente sólo quiso hacer en el párrafo último una consideración expresa de algo que ya consideraba implícito en el párrafo primero y, en este sentido, le sobra la razón a quien ha realizado esta crítica de innecesariedad. Pero, en los textos jurídicos suele ocurrir que toda expresión innecesaria adquiere de inmediato un sentido y alcance que no estaba en la mente de su autor. Y esto ocurre también con el párrafo último del artículo 18 de la Constitución, en el que no sólo el derecho al honor y a la intimidad se protegen frente al uso indebido de la informática, sino que se añade algo más: se establece una reserva de ley para limitar el uso de la informática y no se limita al reconocimiento de los derechos, sino también al reconocimiento de su ejercicio".

Del enunciado de este artículo 18 ya se pone de manifiesto la preocupación existente en la injerencia que la informática (o la Sociedad actual de la Información) iba a suponer en nuestra intimidad, que la ley debía limitar. El derecho a la protección de datos o a la autodeterminación informativa, nace para proteger toda aquella información relativa a nosotros que no tiene por qué formar parte de nuestro área más íntima y personal. Por ello, es natural pensar que se trate de un *nuevo derecho* que nace de una *nueva situación* caracterizada por *nuevos medios* que pueden suponer un ataque a nuestra libertad en definitiva. Pero tal y como afirma TEJERINA[6], "No estamos ante un derecho nuevo, sino ante una nueva necesidad de protección que demanda la *libertad* del individuo, al ir viéndose menoscabada por nuevas y distintas amenazas como las que implica precisamente el desarrollo de la tecnología en esta *Sociedad de la Información*". No podemos estar más de acuerdo.

Nuestro legislador constitucional pensó en *la informática*, como medio que facilitaba enormemente el tratamiento de datos personales y por tanto, podría entrañar un peligro, pero actualmente este término ha quedado desactualizado, pudiendo bien ser sustituido por *big data* o simplemente, por cualquier técnica que pueda surgir en un futuro. Lo que verdaderamente nos lleva a pensar que el bien jurídico objeto de protección es la **libertad** de la persona, en el sentido de decidir cuándo y hasta cuándo sus datos pueden ser objeto de tratamiento y concretamente, cuáles. En definitiva, la llamada autodeterminación informativa.

A nivel Europeo, fue el Tribunal Constitucional Alemán en 1983[7] quien utilizó por primera vez el término *derecho a la autodeterminación informativa*". Y Portugal[8] el primer país en incluir en su constitución de 1976 el derecho de los ciudadanos a conocer lo que consta acerca de ellos en forma de "registros mecanográficos" así como la finalidad a la que se destinan las informaciones y a exigir la

---

[6] TEJERINA, O., *Seguridad del Estado y Privacidad*, Reus, 2014, p. 20.

[7] Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, relativa a la Ley del Censo de la República Federal Alemana.

[8] Artículo 35 de la Constitución portuguesa de 1976.

rectificación o actualización de la información. También establece determinada protección frente a la informática en relación a determinados datos sensibles y prohíbe atribuir un número nacional único a los ciudadanos.

Bien es cierto que los ordenamientos jurídicos europeos reconocen el derecho a la intimidad tal y como lo entendemos hoy desde el siglo XX, pero no podemos confundir intimidad con protección de datos de carácter personal, privacidad[9], derecho a la autodeterminación informativa o *habeas data*, ya que se tratan de dos derechos fundamentales distintos, y prueba de ello es la configuración del derecho a la protección de datos como derecho fundamental autónomo a finales del siglo XX.
El derecho fundamental a la intimidad supone el derecho de cada individuo a proteger su esfera más íntima, a mantenerla fuera del

[9] Nótese que el término "privacidad" no es utilizado actualmente por ningún texto normativo español, pero su utilización, tanto por los profesionales como por la ciudadanía, es una realidad.
Personalmente considero que el término "privacidad", al ser una traducción literal del término "intimidad", no es adecuado ni correcta su utilización como comprensivo del derecho a la protección de datos de carácter personal u otros significados que actualmente de facto se le están atribuyendo, quizá por la falta de un término específico. El DRAE, 22ª ed. define "privacidad" como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" lo cual apunta directamente hacia el concepto de intimidad. En contra de esta opinión, podemos decir que la Exposición de motivos de la LORTAD habló ya de "privacidad", quizá influenciada por la Doctrina americana, al decir "**Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta**, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado". La Doctrina italiana, muy influenciada por el concepto de *privacy* americano, ha llegado a interiorizar tanto el concepto de privacidad ("*privacy*") que incluso ya prescinde del específico término italiano "*riservatezza*.

alcance del resto de personas o aquellas que estime oportuno. Conforme la sociedad ha ido evolucionando y apareciendo nuevas tecnologías, han aumentado exponencialmente las formas de injerencia hacia los individuos; y no sólo injerencia con respecto a su intimidad, su esfera más privada, sino en conjunto a cualquier información relativa a una persona, lo cual ha hecho necesario la aparición no ya de un nuevo bien jurídico digno de protección, sino de un nuevo mecanismo de protección, frente a injerencias no estrictamente realizadas contra la intimidad de las personas (aunque en última instancia la intimidad siempre puede quedar afectada), en forma de derecho fundamental, pues protege el mismo bien jurídico que otros derechos fundamentales pero manifestado de diferente manera. Es así como surge el derecho a la protección de datos como un derecho fundamental autónomo y diferente al derecho fundamental a la intimidad. Lo cual no quiere decir que estemos ante dos conceptos excluyentes, sino complementarios, es decir, el derecho a la intimidad no se contrapone al derecho a la protección de datos de carácter personal y viceversa, sino que ambos conjuntamente dotan de una protección global a la persona en todas las áreas y facetas de su vida.
Citando a LUCAS MURILLO: "no puede negarse que la cobertura jurídica de la que gozan en la actualidad las personas es más intensa, perfecta y eficaz que la que existía hace un siglo, cuando el catálogo de derechos fundamentales era mucho más reducido[10]". Tan es así, que como muy coherentemente apunta LUCAS MURILLO: "(…) el llamamiento que efectúa el artículo 18.4 de la Constitución es meridiano y (…) sitúa claramente el debate en torno a la regulación de la informática en el terreno del derecho a la intimidad, aunque no haya que excluir otros derechos que se vean también implicados"[11] y puntualiza que no se está refiriendo tanto al derecho al honor y a la propia imagen cuanto a las consecuencias que puede implicar la referencia final del artículo 18.4 al "*pleno ejercicio de sus derechos*".

[10] LUCAS MURILLO, P., *op. cit.*, p. 38.
[11] LUCAS MURILLO, P., *op. cit.*, p. 30.

La Doctrina española no ha sido unánime con respecto a si se trataba de un derecho autónomo creado *ex novo*[12], parte o evolución del derecho a la intimidad o bien una consecuencia natural de la evolución de la realidad social. Y aquí es donde cobra importancia el concepto de los denominados derechos de tercera generación. Como se ha puesto anteriormente de manifiesto, el artículo 18.4 de nuestra Carta Magna no formula directamente el derecho a la protección de datos de carácter personal o el derecho a la autodeterminación informativa, sino que establece un **mandato** para que la ley **limite** el uso de la informática para garantizar el honor, la intimidad y el pleno ejercicio de los derechos.

Como se analizará más adelante en el apartado relativo a la configuración jurisprudencial del derecho a la protección de datos de carácter personal como derecho fundamental autónomo, nuestro Tribunal Constitucional zanja cualquier duda[13] al respecto y en su Sentencia 11/1998 afirma que el artículo 18.4 CE "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, **consagra un derecho fundamental autónomo** a controlar el flujo de informaciones que conciernen a cada

---

12 El catálogo de derechos fundamentales no sigue el esquema de numerus clausus, LUCAS MURILLO, P., señala que "Este proceso de constante actualización o, mejor, ampliación del catálogo de los derechos constitucionalmente garantizados revela que nos movemos en una materia expansiva por naturaleza. En efecto, tanto el concepto de derechos humanos cuanto el de derechos fundamentales son el precipitado de una evolución histórica en cuyo curso queda patente el dinamismo que aquéllos encierran. Estos derechos no pueden concebirse de una forma estática. Al contrario, tienden a desarrollarse adoptando contenidos y pretensiones al principio no conocidos". LUCAS MURILLO, P., *op. cit*., pp. 34 y 35.

13 Cfr. el Voto Particular a la STC 290/2000 realizado por el Magistrado don MANUEL JIMÉNEZ DE PARGA Y CABRERA al que se adhiere don RAFAEL DE MENDIZÁBAL ALLENDE, en el que no se comparte que sea el artículo 18.4 el fundamento único o sobre el que se construya el derecho fundamental a la libertad informática, sino que se trata únicamente de un punto de apoyo para su construcción como tal derecho fundamental. Así, afirma que "la Sentencia convierte en base principal lo que en la Constitución es un simple mandato al legislador para que éste limite el uso de la informática".

persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, **pertenezcan o no al ámbito más estricto de la intimidad**, para así preservar el pleno ejercicio de sus derechos (…)". Ya lo afirmaba así años antes LUCAS MURILLO: "aun a falta de su completa regulación legislativa, se puede considerar que el derecho a la autodeterminación informativa es un derecho fundamental[14]". Defiende este autor que el bien jurídico protegido es independiente, con independencia del carácter instrumental o no del derecho a la autodeterminación informativa con respecto a otros derechos, pues en último término, todos los derechos fundamentales lo son con respecto de la dignidad humana, citando como ejemplo el derecho fundamental a la inviolabilidad del domicilio, que, reconocido como derecho fundamental en la CE y por el propio Tribunal Constitucional, se encuentra al servicio de la intimidad y libertad de la persona, y en última instancia de la dignidad y personalidad humanas.

En la misma línea, PÉREZ LUÑO[15], incide en el carácter dinámico de los derechos humanos, que como categoría histórica, nacieron como libertades *individuales* configurando la primera fase o generación de derechos fundamentales, como derechos de "defensa" frente a las injerencias del poder público. Posteriormente, en el siglo XIX, será necesario completar el catálogo de derechos fundamentales con los denominados derechos de segunda generación, (derechos económicos, *sociales* y culturales), como derechos de "participación" que requerirán un papel activo del Estado en cuanto a su garantía y realización. Como complemento a las fases anteriores, continúa el autor, los denominados derechos de tercera generación "se presentan como una respuesta al fenómeno de la 'contaminación de las libertades' (*liberties' pollution*), término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías. La revolución tecnológica ha redimensionado las

[14] LUCAS MURILLO, P., *op. cit.,* p. 158.
[15] PEREZ LUÑO, A., *op. cit*., pp. 55-57.

relaciones del hombre con los demás hombres, las relaciones entre el hombre y la naturaleza, así como las relaciones del ser humano con su contexto o marco de convivencia". Es por ello que, ante nuevas formas de agresión a los derechos fundamentales, deberán encontrarse nuevos mecanismos de defensa y garantía, y aquí es donde los denominados derechos de tercera generación encuentran su significación y justificación. No obstante, también ha habido autores que se han posicionado contrarios a la configuración del derecho a la autodeterminación informativa como un derecho fundamental autónomo. Cabe citar a LAPORTA, muy crítico con el reconocimiento de las diferentes generaciones de derechos, y por tanto, de ampliar el catálogo de derechos fundamentales, llegando a afirmar[16] que "(…) el ampliar más y más los catálogos de derechos humanos es incompatible con la mayoría de los rasgos que se predican de ellos". Por su parte, ORTÍ VALLEJO, aun admitiendo el carácter abierto del elenco de derechos fundamentales[17], reivindica la máxima cautela para afirmar la existencia de un nuevo derecho de la personalidad, terminando por concluir que "no hay razones suficientes para afirmar que la protección de la persona frente a la utilización de ficheros y tratamientos automatizados de datos personales, comporte la existencia de un nuevo derecho de la personalidad[18]".

Así, para este autor, las leyes de protección de datos no protegen un ámbito distinto de la intimidad, porque "en materia informática no tiene caso distinguir entre informaciones íntimas y las que no lo son, porque esta tecnología posee la capacidad de transformar éstas últimas en informaciones íntimas"[19]. No podemos compartir dicho razonamiento en ningún caso, pues las posibilidades que ofrecen

---

[16] LAPORTA, F., *op. cit.*, p. 44.

[17] ORTÍ VALLEJO, A., Derecho a la intimidad e informática. (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada), Comares, Granada, 1994, p. 34, afirma que "por nuestra parte no dudamos en adherirnos al criterio que considera a los derechos fundamentales una categoría histórica y, por tanto, el tratarse de un elenco que está abierto a nuevos tipos (…)".

[18] ORTÍ VALLEJO, A., *op. cit.*, p. 57.

[19] ORTÍ VALLEJO, A., *op. cit.,* p. 51.

nuevos medios de tratamiento (pensemos en el tratamiento de datos masivos actual), nada tienen que ver ni deben confundirse con la naturaleza misma de los datos. Es decir, un dato de carácter personal no podrá devenir "íntimo" por el hecho de ser objeto de un tratamiento informatizado. Podrán requerirse medidas de seguridad adicionales más elevadas para aquellos tratamientos cuyo objeto sea inferir perfiles psicológicos u otro tipo de consecuencias, pero ello no alterará la naturaleza del dato originario, pues siguiendo el razonamiento de ORTÍ VALLEJO, podríamos llegar a la errónea conclusión de que todos los datos son íntimos. Para ORTÍ VALLEJO, consecuencia del no reconocimiento de un ámbito distinto de protección de ambos derechos, estamos simplemente ante un problema causado por una nueva tecnología, que puede solucionarse reformulando el concepto de intimidad, sin necesidad por tanto de crear un nuevo derecho fundamental o de la personalidad[20], siguiendo a la Doctrina italiana mayoritaria. No podemos compartir esta postura, en primer lugar porque ignora la existencia de datos de carácter personal no íntimos y analiza el problema por tanto, desde la perspectiva del tratamiento automatizado de los datos, y en segundo lugar, porque aunque en un primer momento pueda aparecer lógica la solución de reformular o ampliar en concepto de intimidad, ello supondría ampliar desmesuradamente su objeto de protección, es decir, ese ámbito reservado y más íntimo, siempre será el mismo pues es consustancial a la persona humana, con independencia de las posibilidades de tratamiento que nos brinde la tecnología, y es precisamente por ello que surge una nueva necesidad de protección que antes no existía, que justifica plenamente la creación del derecho fundamental a la protección de datos de carácter personal.

Visto todo lo anterior, y partiendo de un sistema jurídico positivista pero en constante evolución como la sociedad misma, es claro que no cabe realizar objeción alguna a la aparición de nuevos derechos fundamentales, lo cual no significa que cualquier nueva necesidad de protección dé lugar a un nuevo derecho fundamental. A partir del

[20] ORTÍ VALLEJO, A., *op. cit.*, pp. 58 y 59.

derecho a la intimidad, como veremos en el apartado siguiente, surge el derecho a la protección de datos personales, como respuesta a una nueva necesidad de protección provocada por la evolución misma de la sociedad en relación a la tecnología. Y por esta misma razón, quizá en un futuro no muy lejano, nos veamos en la necesidad de proteger, ya no dentro de una esfera individual sino colectiva, otro tipo de agresión contra la libertad de las personas en relación a sus datos.

1.1.2 Derecho a la intimidad

Bien es cierto que el derecho a la protección de datos tiene su origen en el derecho a la intimidad por lo que no puede negarse cierta coincidencia en su ámbito material, pero en ningún modo puede entenderse que el segundo incluya todos los aspectos del primero produciéndose un solapamiento de su ámbito de protección. La afección del derecho a la protección de datos no comportará necesariamente el quebranto del derecho a la intimidad, ya que no todos los datos de carácter personal tienen la condición de "íntimos" y es por ello que se protegen bienes jurídicos diferentes, relacionados por ser ambos derechos de la personalidad, pero diferentes. El derecho a la intimidad, como derecho subjetivo[21], tiene fundamentalmente una vertiente negativa, en el sentido de impedir a terceros conocer el contenido o detalles de la esfera más personal del individuo, y por tanto, el derecho de la persona a desenvolverse libremente. El artículo 18.1 de nuestra carta magna habla de intimidad "personal y familiar", quizá para remarcar el ámbito reducido del concepto de intimidad, como el núcleo más cercano y privado de la persona. Nuestro Tribunal

[21] Cfr. BAJO FERNÁNDEZ, M., *op. cit.*, p. 8, "los llamados derechos de la personalidad son, en realidad, atributos del propio sujeto de derecho, es decir, de la propia persona. De ahí que no quepa hablar de derechos subjetivos, porque los atributos del titular del derecho, o sea, aquello que lo convierte en 'persona' (vida, integridad física, libertad, honor, nombre, intimidad) no puede desvincularse de sí mismo. Los atributos de la personalidad no son derechos subjetivos, ni facultades derivadas de la norma objetiva, porque en realidad integran la propia entidad personal del sujeto, a quien se atribuye la titularidad del derecho subjetivo".

Constitucional ha precisado el contenido del derecho a la intimidad, en diferentes sentencias, quizá porque hasta 1982, año en el que se aprueba la *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen,* el Ordenamiento jurídico español no tuvo una legislación propia en relación al derecho a la intimidad. Así, la STC 231/1988[22] afirma que "Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la C.E. aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la '**dignidad** de la persona', que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás necesario —según las pautas de nuestra cultura— para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como **personalísimos** y ligados a la misma existencia del individuo (…)". La misma Sentencia, precisa que "el derecho a la intimidad personal y familiar se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen".

En cuanto al ámbito de reserva de la vida privada que otorga el derecho a la intimidad, la STC 134/1999[23], recogiendo anterior Jurisprudencia Constitucional, resume que "El art. 18.1 C.E. no garantiza una "intimidad" determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 garantiza es un **derecho al secreto**, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida

[22] STC 231/1988 de 23 de Diciembre, FFJJ 3º y 4º.
[23] STC 134/1999 de 15 de Julio de 1999, FFJJ 5º y 6º.

privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cuál sea lo contenido en ese espacio. Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida, lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos". Además, añade que el hecho de que la información sea o no veraz, es irrelevante para establecer si ha habido o no lesión del art. 18.1 C.E., "ya que, si la información transgrede uno de sus límites (art. 20.4 C.E.), su veracidad no excusa la violación de otro derecho o bien constitucional". Así lo reitera la STC 115/2000, en relación a la STC 172/1990, "el criterio para determinar la legitimidad o ilegitimidad de las intromisiones en la intimidad de las personas no es el de la veracidad, sino exclusivamente el de la relevancia pública del hecho divulgado, es decir, que su comunicación a la opinión pública, aun siendo verdadera, resulte ser necesaria en función del interés público del asunto sobre el que se informa".

En relación al carácter público del titular del derecho a la intimidad, la STC 134/1999 afirma tajantemente que "el riesgo asumido por el personaje con notoriedad pública no implica aminoración de su derecho a la intimidad o al honor o a la propia imagen, cuya extensión y eficacia sigue siendo la misma que la de cualquier otro individuo", teniendo como único límite los actos propios de sus titulares.

Respecto a la mayor o menor gravedad de los hechos potencialmente revelados, la STC 115/2000[24] afirma que "resulta irrelevante desde la perspectiva constitucional que los datos pertenecientes a la esfera de intimidad divulgados sean o no gravemente atentatorios o socialmente desmerecedores de la persona cuya intimidad se desvela, aunque desde la perspectiva de la legalidad puedan servir para modular la responsabilidad de quien lesiona el derecho fundamental (art. 9 de la

[24] STC 115/2000 FJ 8º.

Ley Orgánica 1/1982, de 5 de mayo). Y la razón es, sencillamente, que los datos que pertenecen al ámbito del derecho a la intimidad personal y familiar constitucionalmente garantizado están directamente vinculados con la dignidad de la persona (art. 10.1 CE) (..), y, por tanto, es suficiente su pertenencia a dicha esfera para que deba operar la protección que la Constitución dispensa (…)".

No obstante todo lo anterior, el derecho a la intimidad no resulta un derecho absoluto, sino que deberá realizarse una justa ponderación con otros derechos fundamentales tales como la libertad de expresión o información, o bien con situaciones que supongan una situación de subordinación como la posición de un trabajador frente al empresario[25] o en el ámbito penitenciario.

Visto el contenido que nuestro Tribunal Constitucional hace del derecho a la intimidad personal y familiar, bien es cierto que ambos derechos, como derechos de la personalidad, buscan garantizar la **libertad** del individuo para que pueda desarrollar libremente su personalidad y, por tanto, otros derechos. Será el **objeto** de ambos derechos lo que los diferencie realmente, pues antes de que la informática supusiera una amenaza, la protección de datos de carácter

[25] STC 170/2013, de 7 de octubre de 2013, en la que se desestima el amparo solicitado por el trabajador despedido por haber facilitado información de la compañía a terceros a través del móvil y correo electrónico corporativos. El trabajador alega vulneración de su derecho a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE), al haberse considerado como prueba lícita la aportación por la empresa del contenido de determinados correos electrónicos del trabajador, obtenidos de un portátil propiedad de la empresa. Se produce por tanto una colisión entre el poder de dirección del empresario (art 20.3 ET) y los derechos del trabajador (18.1 y 18.3 CE). El Convenio Colectivo aplicable establecía como falta leve la "utilización de los medios informáticos propiedad de la empresa (correo electrónico, Intranet, Internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral", por lo que "no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa (…)". La expresa prohibición establecida en el Convenio Colectivo del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales conlleva la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

personal no era necesaria debido a que la dimensión social del individuo en sus relaciones con terceros, no era ni con mucho la actual.

1.1.3 Bien jurídico protegido

El bien jurídico protegido por el derecho a la intimidad es el libre desarrollo de la personalidad, la libertad de disposición con respecto al ámbito íntimo de la persona. Mientras que el bien jurídico protegido por el derecho a la protección de datos o *habeas data* es también la libertad de la persona de decidir con respecto a su información no íntima, como una manifestación más de su dignidad.
ÁLVAREZ CIENFUEGOS[26] afirma que, a pesar de que ambos derechos tengan un fundamento común, esto es, la dignidad de la persona humana y los derechos inviolables que le son inherentes en los términos reconocidos en el art. 10.1 de la Constitución y en los Tratados Internacionales, "las diferencias son evidentes: mientras que la protección de la intimidad tiene un carácter «defensivo» excluyendo del conocimiento ajeno la 'vida personal y familiar', vetando incluso las intromisiones de terceros contra la voluntad del titular. En el caso de la Protección de los Datos Personales, aún reconociendo la dinamicidad de su contenido objetivo derivado de los cambios tecnológicos, este derecho fundamental garantiza a la persona un poder de control —de contenido positivo— sobre la captura, uso, destino y posterior tráfico de los datos de carácter personal". De esta manera, ÁLVAREZ CIENFUEGOS[27] sostiene que la diferencia está, en que frente al deber de abstención, de no intromisión en la esfera íntima de la persona, que el derecho a la intimidad puede imponer, "el derecho a la protección de datos añade además a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio

[26]ÁLVAREZ-CIENFUEGOS, J. M., "La libertad informática, un nuevo derecho fundamental en nuestra Constitución (Comentario de las Sentencias 290/2000 y 292/2000)", *La Ley*, n. 5230, 2001.
[27] ÁLVAREZ CIENFUEGOS, J.M., *op. cit.*

impone a terceros deberes jurídicos, no contenidos en el derecho fundamental a la intimidad y que pretenden, en último término, atribuir a la persona afectada un control sobre sus datos personales que, en ocasiones, puede imponer a terceros deberes de hacer, como son, entre otros: el derecho a saber y ser informado sobre el destino y uso de los datos, el derecho a acceder, rectificar y cancelar datos (…)". La STC 290/2000 afirma[28] que "(…) el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que pueda lesionar ciertos derechos fundamentales de los ciudadanos o afectar al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional".

El derecho a la protección de datos opera cuando la intimidad no se ve afectada, pues hablar de ámbitos coincidentes de protección nos obligaría a "penalizar" de igual manera actos con distinta significación, o incluso a llegar a poder elegir la vía procesal más conveniente para la defensa del afectado en lugar de la que correspondería. En este sentido podemos hablar de la *vis atractiva* que actualmente ocurre en sede del derecho de protección de datos, si tenemos en cuenta por ejemplo que la imagen es un dato de carácter personal, por lo que en multitud de ocasiones, conductas que afectan al derecho a la propia imagen (artículo 18.1 CE) son denunciadas por la vía del derecho a la protección de datos dado el menor coste económico inicial para el denunciante junto con la sencillez del procedimiento de denuncia. A diferencia del derecho a la intimidad, el cual se ve afectado por la mera revelación de un dato íntimo, el derecho a la protección de datos no protege toda aquella información, no íntima, relativa al individuo, en sí misma considerada, sino que deberá analizarse la utilización que de dicha información se realice, es decir, para determinar si el derecho a la protección de datos ha sido afectado, será necesario valorar si se ha respetado la finalidad para la cual fueron recogidos los datos, entre otros aspectos, en otras palabras, si se ha respetado el poder de disposición del interesado. Citando a

[28] STC 290/2000, FJ 11º.

LUCAS MURILLO: "el bien que tutelan los sistemas de protección de datos no es la intimidad 'física' o entendida en sentido estricto, sino la intimidad informativa o autodeterminación informativa (…)[29]".

1.1.4 Contenido esencial del derecho a la protección de datos. Configuración jurisprudencial

La Jurisprudencia ha tenido, y tiene, una importancia capital en la configuración de este derecho. En palabras de JIMÉNEZ DE PARGA Y CABRERA[30] "una de las tareas importantes de los Tribunales Constitucionales es extender la tutela a determinadas zonas del Derecho no expresamente consideradas en las correspondientes Constituciones, cuando, como ocurre en el presente caso, es necesario hacerlo para que no queden a la intemperie, sin techo jurídico alguno, intereses esenciales de los ciudadanos".

Desde que en los años 70 se comenzó a positivar el derecho a la protección de datos (aunque no necesariamente con esta denominación) en determinados países europeos, la Jurisprudencia ha jugado un papel esencial. Podemos decir que fue la sentencia del Tribunal Constitucional Alemán sobre la Ley de Censo de Población[31] la que comenzó dicho proceso de configuración, hablando por primera vez del *derecho a la autodeterminación informativa,* como algo independiente y separado del derecho a la intimidad. En dicha

[29] LUCAS MURILLO, P., *op. cit.*, p. 123.

[30] Voto particular que formula el Magistrado D. MANUEL JIMÉNEZ DE PARGA Y CABRERA STC 290/2000, de 30 de noviembre de 2000, al que presta su adhesión el Magistrado D. RAFAEL DE MENDIZÁBAL ALLENDE http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4274#complete_resolucion&votos

[31] Sentencia del Tribunal Constitucional Alemán (Bundesverfassungsgericht) de la República Federal de Alemania de 15 de Diciembre de 1983, consultada en Jurisprudencia del Tribunal Constitucional Federal Alemán Extractos de las sentencias más relevantes compiladas por Jürgen Schwabe, Fundación Konrad-Adenauer-Stiftung, México, 2009, pp. 94-102.

sentencia se afirma "la autodeterminación individual presupone, también bajo las condiciones de la moderna tecnología para el procesamiento de información, que a los individuos se les dé libertad para decidir sobre qué actividades emprender y cuáles omitir, incluyendo la posibilidad de comportarse efectivamente de conformidad con esa decisión. (…) Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer *quiénes*, *cuándo* y *en qué circunstancias* saben *qué* sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información. (…) Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar. De esto se deduce lo siguiente: el libre desarrollo de la personalidad presupone en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. Esa protección se contempla en los derechos fundamentales previstos en el Art. 2, párrafo 1, en relación con el Art. 1, párrafo 1 de la ley Fundamental. El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales".

No obstante, en aquellas Constituciones en las que no se recoge expresamente el derecho a la protección de datos como derecho fundamental, su configuración como tal por parte de la Jurisprudencia presenta mayor o menor dificultad en función de la existencia o no de una cláusula abierta[32] que permita precisamente completar ese

[32] *Op. cit*. JIMÉNEZ DE PARGA Y CABRERA, M., en el voto particular a la STC 290/2000, menciona que la Constitución Española, a diferencia de la de Portugal, Argentina o EEUU, no incluye ("se olvidó o no quiso recogerse") una "cláusula abierta" como la existente en EEUU "la enumeración que se hace en esta Constitución no deberá interpretarse como denegación o menoscabo de otros derechos que conserva el pueblo", que permita incluir este tipo de "derechos extraconstitucionales" o "derechos fundamentales atípicos".

"catálogo inacabado" de derechos fundamentales. La Jurisprudencia española, partiendo del concepto de intimidad, ha perfilado el contenido actual del derecho fundamental a la protección de datos de carácter personal, aun no reconociéndolo como un derecho autónomo desde el primer momento. Así, debe citarse en primer lugar la Sentencia 254/1993 del Tribunal Constitucional[33]. Esta Sentencia tiene su origen en la negativa de la Administración del Estado a atender un derecho de acceso. La propia sentencia enmarca el supuesto de hecho[34]: "La cuestión suscitada en el presente recurso de amparo consiste en determinar si la negativa a suministrar la información solicitada, acerca de los datos personales del actor que la Administración del Estado posee en ficheros automatizados, vulnera o no los derechos fundamentales a la intimidad y a la propia imagen que le reconoce el art. 18 de la Constitución, tanto en su apartado 1 como en el 4", o en otras palabras "si el actor tenía o no derecho, en virtud del art. 18 C.E., a que la Administración le suministrase la información que solicitaba".

Y todo ello, como la propia sentencia cita, nuestra Jurisprudencia mantiene que lo esencial es "el derecho fundamental que se defiende, no la cita del art. de la Constitución que lo proclama". La sentencia pone de manifiesto la importancia que tienen las garantías para la defensa de los derechos fundamentales de los ciudadanos, ante los riesgos que su indebido tratamiento puede suponer. Así, afirma "paradójicamente, los riesgos derivados del exceso, de los errores, o del uso incontrolado de información de carácter personal no pueden ser afrontados eficazmente por los particulares afectados a causa de una información insuficiente, pues los ciudadanos se encuentran inermes por la imposibilidad de averiguar qué información sobre sus personas almacenan las distintas Administraciones públicas, premisa indispensable para cualquier reclamación o rectificación posterior. Menos aún pueden conocer y prevenir o perseguir el uso desviado o

---

[33] STC 254/1993, de 20 de julio de 1993, disponible en http://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/1993/254

[34] Fundamento Jurídico 1. STC 254/1993.

la diseminación indebida de tales datos, incluso aunque le causen lesiones en sus derechos o intereses legítimos. De aquí que el Convenio europeo de 1981 no se limite a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11; sino que los complete con unas garantías para las personas concernidas, que formula detalladamente su art. 8".

La importancia de esta sentencia, dictada antes de la entrada en vigor de la LORTAD, radica en el reconocimiento que realiza de una "nueva garantía constitucional" basada en el derecho a la libertad frente a posibles injerencias en la dignidad y libertad de la persona proveniente de un tratamiento ilegítimo de sus datos, no considerando por tanto el elenco de derechos fundamentales como una lista cerrada. Establece la STC 254/1993 que: "Dispone el art. 18.4 C.E. que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". De este modo, nuestra Constitución ha incorporado una **nueva garantía constitucional**, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un **derecho o libertad fundamental,** el **derecho a la libertad frente a la potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos**, lo que la Constitución llama "la informática"[35].
El hecho de que cuando acontecieran los hechos no existiera desarrollo legislativo de todos los derechos fundamentales recogidos en el artículo 18, no supone que éstos no generen derechos y obligaciones para sus titulares, pues tal y como afirma la sentencia

[35] STC 254/1993, FJ 6º.

"Los derechos y libertades fundamentales vinculan a todos los poderes públicos, y son origen inmediato de derechos y obligaciones, y no meros principios programáticos"[36]. Y a partir de aquí, comienza a elaborar en el Fundamento Jurídico 7º ese "contenido mínimo" que puede desprenderse de este derecho o libertad. Pero como veremos a continuación, y a diferencia de lo que pudiera parecer, el TC no configura el mencionado nuevo "derecho o libertad fundamental" sino que lo entiende incardinado en el derecho fundamental a la intimidad, como la facultad del interesado de controlar el uso de los datos relativos a su persona, es decir, como una nueva vertiente positiva de este derecho.

Así, afirma la Sentencia: "Un primer elemento, el más "elemental", de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: El uso de la informática encuentra un límite en el *respeto al honor y la intimidad* de la personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna ***garantía complementaria***, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de *derecho de control sobre los datos relativos a la propia persona*. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)". Es decir, no será esta sentencia la que configure el derecho a la protección de datos

---

[36] Recordemos el artículo 53.1 de la Constitución Española: "Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos (…)" y es doctrina asentada del TC la aplicación directa de los derechos fundamentales y libertades públicas sin que su efectividad dependa de un posterior desarrollo legislativo (vid STC 75/1982 y STC 39/1983), aunque como precisa SOLOZÁBAL ECHAVARRÍA J. J., "Los derechos fundamentales en la Constitución Española", *Revista de Estudios Políticos (Nueva Época)*, n, 105, julio-septiembre 1999, p. 14, dicha doctrina constitucional es perfectamente compatible con su afirmación "el régimen de los derechos fundamentales requiere de completamiento o acabamiento, de modo que el mero reconocimiento constitucional no basta para garantizar un verdadero disfrute de los derechos fundamentales".

como derecho fundamental autónomo, pero reconoce y configura su contenido esencial, aunque en forma de garantía *complementaria* del derecho a la intimidad.

Un año después nos encontramos con la STC 143/1999, que viene a resolver la alegación de vulneración del derecho a la intimidad personal y familiar, por parte del Real Decreto 338/1990, de 9 marzo, y la Orden Ministerial de 14 marzo 1990, reguladoras del Número de Identificación Fiscal, no en cuanto a la existencia misma de un Número de Identificación Fiscal, sino por ser éste un instrumento a través del cual se recaba información que puede ser utilizada de forma desviada, incidiendo en la esfera de reserva personal que aquel derecho garantiza.

En su Fundamento Jurídico 6º el TC pone de manifiesto la existencia de un interés legítimo en salvaguardar del conocimiento de terceros determinadas informaciones de la persona, pero ya no dentro del derecho a la intimidad para luego decir en el Fundamento Jurídico 7º, siguiendo la línea marcada por la sentencia comentada anteriormente, que es necesaria la ampliación del ámbito de juego del derecho a la intimidad. Así afirma primeramente que "el derecho a la intimidad en cuanto derivación de la dignidad de la persona, implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 209/1988, Fundamento Jurídico 3º). Dada la conexión necesaria que ha de existir entre el derecho en cuestión y la esfera reservada para sí por el individuo, en los más básicos aspectos de su autodeterminación como persona, *resulta,* por lo menos, *cuestionable que en abstracto pueda entenderse vulnerada su intimidad* por la exigencia de transmitir información sobre actividades desenvueltas en el tráfico económico y negocial. Unas actividades que tienden a desarrollarse en el ámbito de relación con terceros, y a estar sometidas a fórmulas específicas de publicidad, en aras de la seguridad jurídica y de la transparencia en el tráfico económico, de ahí que *sólo con extremada dificultad puedan calificarse como reservadas*, en el sentido antes descrito típico del juego del derecho a la intimidad. No cabe duda de que puede existir

un interés legítimo en mantener resguardadas del conocimiento de terceros estas actividades, pero dicho interés desborda el ámbito de estricta constitucionalidad, para introducirse en la esfera de lo puramente económico".

Y en el Fundamento Jurídico 7º se separa de la argumentación jurídica comenzada diciendo "Desde luego, es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información puede ocasionar este efecto y, correlativamente, **se hace precisa la ampliación del ámbito de juego del derecho a la intimidad**, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho (STC 254/1993)".

Así, y aun reconociendo la diferencia entre intimidad y datos de carácter personal, el TC se esfuerza en integrarlo dentro del derecho a la intimidad. "(…) se ha afirmado que, ya que "los datos personales que almacena la Administración son utilizados por sus autoridades y servicios", no es posible "aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión" (STC 254/1993, fundamento jurídico 7º). En consecuencia con ello, habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente inversor de la vida privada del ciudadano, a través de su tratamiento técnico, *vulneraría el derecho a la intimidad* de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta".

Será en la STC 11/1998[37] cuando se hable por primera vez de un derecho fundamental autónomo. En esta sentencia se analiza la

[37] Sentencia 11/1998, de 13 de enero de 1998 (BOE núm. 37, de 12 de febrero de 1998), disponible en http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=20139

vulneración del derecho de libertad sindical por la utilización ilegítima de datos personales por parte de una empresa, ya que se utilizaron para una finalidad completamente distinta para la cual fueron proporcionados. Partiendo del argumento comenzado por la STC 254/1993 que defendía la existencia de una garantía complementaria ("libertad informática") como manifestación de la vertiente positiva del derecho a la intimidad, la STC 11/1998 habla ya de la protección de los datos informáticos en relación al artículo 18.4 C.E.: "En efecto, el art.18.4 en su último inciso establece las limitaciones al uso de la informática para garantizar el pleno ejercicio de los derechos, lo que significa que, en supuestos como el presente, el artículo citado es, por así decirlo, *un derecho instrumental ordenado a la protección de otros derechos fundamentales*, entre los que se encuentra, desde luego, la libertad sindical, (…) porque es, en definitiva, el derecho que aquí se ha vulnerado (…)".

Pero va más allá de concebirlo como un mero derecho instrumental para la protección de otros derechos fundamentales al afirmar que "no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, **consagra un derecho fundamental autónomo** a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, **pertenezcan o no al ámbito más estricto de la intimidad**, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho de libertad sindical".

A continuación analizaremos la STC 290/2000[38] originada por cuatro recursos de inconstitucionalidad interpuestos contra la LORTAD, que

[38] Sentencia 290/2000, de 30 de noviembre de 2000 (BOE núm. 4, de 4 de enero de 2001), disponible en

a raíz de una cuestión competencial, entre otras cosas, analiza el contenido del derecho fundamental a la protección de datos de carácter personal. Esta sentencia, junto con la STC 292/2000 que analizaremos posteriormente, determinarán el contenido esencial del derecho a la protección de datos de carácter personal.

Así, la STC 290/2000 cita[39] el Fundamento Jurídico 6º de la STC 254/1993 (que no el Fundamento Jurídico 7º), en el que se sostiene que el art 18.4 CE además de ser una garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos, es, además, en sí mismo, "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama 'la informática'". Así, se establece que: **"**En efecto, ha de tenerse presente, como ya se anticipaba en la decisión de este Tribunal que se acaba de mencionar, que el **derecho fundamental** al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un *haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales*, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos".
En este punto debe hacerse referencia al Voto Particular realizado por el Magistrado D. Manuel JIMÉNEZ DE PARGA Y CABRERA al que presta su adhesión el Magistrado D. Rafael DE MENDIZÁBAL ALLENDE, ya que entiende que "la Sentencia convierte en principal lo que en la Constitución es un simple mandato al legislador para que éste limite el

---

http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=13749

[39] Fundamento Jurídico 8 de la STC 290/2000.

uso de la informática". Es decir, no considera que el artículo 18.4 de la CE contenga un derecho fundamental en sí mismo, sino que es un punto de apoyo, entre otros, para la pertinente construcción del derecho fundamental. Así, JIMÉNEZ DE PARGA Y CABRERA sostiene que "los cimientos constitucionales para levantar sobre ellos el derecho de libertad informática son más amplios que los que proporciona el artículo 18.4 CE", citando como fundamento principal el artículo 10.1 CE, el cual recoge, en su opinión, unos principios constitucionales (la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás) que, además de ser directamente vinculantes, han de regir la interpretación de todo el Ordenamiento Jurídico. Así, afirma "con estos principios constitucionales, de aplicación directa, y el apoyo de determinados derechos expresamente recogidos en la Constitución de 1978, así como en Textos internacionales, es posible extender la tutela a ciertos derechos de singular relieve e importancia en el actual momento de la historia".

El TC afirma que la LORTAD desarrolla un derecho fundamental específico, el derecho a la protección de los datos personales, y deja a un lado la concepción de garantía instrumental haciendo valer su sustantividad propia al decir que la protección de los datos personales "mal puede estar al servicio de otros fines que los constitucionales en relación con la salvaguardia de los derechos fundamentales, ni tampoco puede ser medio o instrumento de actividad alguna". Por su parte, la STC 292/2000[40] , recoge la Jurisprudencia del TC acaecida hasta la fecha, en su afirmación de la sustantividad propia del derecho a la protección de datos de carácter personal, destacando dos peculiaridades con respecto al derecho a la intimidad, en relación a su diferente objeto y contenido. Así, afirma[41] que "La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la

[40] Sentencia 292/2000, de 30 de Noviembre de 2000, disponible en http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4276

[41] STC 292/2000, FJ 5º.

intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona". Asimismo, sostiene que el derecho a la intimidad y el derecho a la protección de datos comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, pero el derecho a la protección de datos, además, "atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

El TC afirma[42] que el contenido del derecho fundamental a la protección de datos consiste en un "poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

En resumen, podemos ver cómo desde un inicio, la Jurisprudencia del TC ha concebido como necesaria la existencia de un conjunto de facultades en relación a áreas no necesariamente pertenecientes al ámbito de lo íntimo, que permitan a los ciudadanos el libre ejercicio de sus derechos y el libre desarrollo de la personalidad, aunque en un inicio se denominase garantía complementaria al derecho a la intimidad para acabar asentando después el derecho a la protección de datos como un derecho fundamental autónomo con sustantividad propia.

---

[42] STC 292/2000, FJ 7º.

1.2 Reconocimiento normativo y principios

En el apartado siguiente se analizará el marco jurídico existente en sede internacional y europea, por lo que ahora nos referiremos exclusivamente a la normativa española en materia de protección de datos.

1.2.1 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, (LORTAD)

La primera plasmación normativa del derecho a la protección de datos de carácter personal, la realizó la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, en adelante, LORTAD. La LORTAD desarrolla por primera vez, dieciséis años después, el mandato constitucional establecido en el artículo 18.4 de nuestra Carta Magna y ocho años después de la ratificación[43] del Convenio 108 del Consejo de Europa, según el cual los Estados ratificantes se obligaban a adaptar su legislación al respecto. No obstante lo anterior, fue la adhesión de España al Convenio de Schengen el 25 de Junio de 1991, la que empujó a legislar en materia de protección de datos, ya que adecuar el Derecho interno a lo establecido en el Convenio 108 del Consejo de Europa de 1981, era *conditio sine qua non* para poder participar en el Convenio de Schengen. La LORTAD tiene la oportunidad, por tanto, de recoger toda la Doctrina y Jurisprudencia desarrollada hasta entonces y así asienta conceptos tales como qué consideramos "datos de carácter personal", "tratamiento" de datos, los principios rectores en la materia y las garantías de defensa de los interesados. Su artículo 1 establece el objeto de la ley, consistente en desarrollar lo previsto en el artículo 18.4 de la Constitución Española, limitando el uso de la informática y otras técnicas y medios de tratamiento *automatizado* de

[43] España firmó el Convenio 108 del Consejo de Europa el 28 de Enero de 1982 pero no lo ratificó hasta el 27 de Enero de 1984.

los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos. Destacar que se refiere exclusivamente al tratamiento "automatizado" de datos, como el propio nombre de la ley establece, si bien en el artículo siguiente[44], al establecer el ámbito de aplicación, incluye el tratamiento no automatizado como una modalidad de uso posterior protegida.

La LORTAD fue criticada y de hecho, fue objeto de diferentes recursos[45] ante el TC por parte del Defensor del Pueblo, el Consejo Ejecutivo de la Generalidad de Cataluña, el Parlamento de Cataluña y el Grupo Parlamentario Popular, que dieron lugar a las anteriormente mencionadas STC 290/2000 y STC 292/2000. La STC 290/2000 no declara la inconstitucionalidad de precepto alguno, ya que durante la tramitación del recurso se produjo la derogación de la LORTAD, y por tanto, la pérdida sobrevenida del objeto de los recursos de inconstitucionalidad interpuestos, en palabras del propio TC.

No obstante, resulta interesante conocer los preceptos objeto de impugnación; así, se impugnan los siguientes artículos:

- artículo 6.2 LORTAD: establece la posibilidad de no recabar el consentimiento por parte de la Administración para el tratamiento de los datos personales del administrado, lo cual entienden los recurrentes infringe los límites impuestos por el artículo 18.4 CE
- artículo 19.1: se alega inconstitucionalidad por infracción del principio de reserva de ley, ya que permite a las Administraciones la cesión de datos para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, cuando dicha cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición de igual o superior rango que regule su

[44] Artículo 2.1 LORTAD: "La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado".

[45] La STC 290/2000 resuelve los recursos de inconstitucionalidad acumulados 201-93, 219-93, 226-93, 236-93 y la STC 292/2000, el recurso de inconstitucionalidad 1463/2000.

uso. El Defensor del Pueblo entiende que, por un lado se vulnera el requisito del consentimiento previo necesario para la cesión de datos establecido por el artículo 11 de LORTAD y un límite al derecho fundamental a la intimidad establecido en el artículo 18.1 CE, y además, el artículo 53.1 CE, que requiere una norma con rango de ley para el desarrollo de los derechos fundamentales. Asímismo, considera que establece una remisión en blanco a favor del ejecutivo.

- artículo 20.3, permite la recogida y tratamiento de datos especialmente protegidos por las Fuerzas y Cuerpos de seguridad del Estado, "exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta". Se alega vulneración del artículo 16 (libertad ideológica, religiosa y de culto), pues se vulnera el derecho a no declarar sobre las propias creencias o ideologías, pero los recurrentes ponen de manifiesto el problema que surge con respecto al almacenamiento y tratamiento de estos datos sensibles, ya que al estar al margen del ámbito protegido por el artículo 16.2 CE, cabe aplicar la excepción del artículo 20.3 LORTAD. También se alega vulneración del artículo 18.4 CE, ya que la creación de ficheros con datos sensibles contradeciría el propio artículo 20.3 que únicamente permite la existencia de dichos ficheros en el marco de una investigación concreta, lo cual a su vez, es del todo ilógico pues no cabe crear ficheros para un único supuesto y uso, como ponen de manifiesto los recurrentes.
- artículos 22.1 y 2, establecían la no aplicación del artículo 5 LORTAD (párrafos 1 y 2) relativo al derecho de información, cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad Pública o a la persecución de infracciones penales o administrativas. Se alega vulneración del artículo 18.1 CE, por considerar que dichas excepciones contradicen el artículo 9.2 del

Convenio 108 del Consejo de Europa[46] y que la habilitación que se realiza a la Administración constituye un apoderamiento en blanco.

- Los artículos 24, 31, 40.1 y 2, son impugnados por el Parlamento de Cataluña y el artículo 39, que también es impugnado por la Generalidad de Cataluña, en relación a las competencias de la comunidad autónoma para crear y mantener sus propios ficheros. El TC desestima las alegaciones por entender que se reclaman competencias propias del Estado[47].
- DF 3 LORTAD, la cual establecía el carácter de ley ordinaria de determinados artículos y Disposiciones Adicionales y Finales.

Una vez aprobada la Ley Orgánica 15/1999 de Protección de Datos de Carácter personal, en adelante, LOPD, el Defensor del Pueblo presentó un nuevo recurso de inconstitucionalidad contra los artículos 21.1 y 24. 1 y 2 de la LOPD (artículos 19 y 22 LORTAD), por considerar que la nueva Ley Orgánica seguía vulnerando la Constitución Española. El TC estima el recurso de inconstitucionalidad reconociendo la vulneración de reserva de ley de lo establecido en el artículo 21.1 LOPD, y respecto al artículo 24 LOPD, afirma que la utilización de cláusulas en blanco a favor de la Administración, supone la desprotección del contenido esencial de los derechos fundamentales establecidos en el artículo 18 CE.

---

[46] Artículo 9.2 Convenio 108: "2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:
a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;
b) para la protección de la persona concernida y de los derechos y libertades de otras personas.

[47] Aunque cabe destacar que la LOPD recogerá parcialmente las alegaciones planteadas por la Generalidad y el Parlamento de Cataluña, cuando por ejemplo el artículo 32 LOPD relativo a los códigos tipo incluye la posibilidad de registro en los registros creados al efecto por las Comunidades Autónomas.

1.2.2 Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de carácter personal, (LOPD)

Consecuencia de la aprobación de 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, era necesario introducir modificaciones en la LORTAD para adecuarla a lo establecido en ella, por lo que en un primer momento, el objetivo no fue aprobar una nueva Ley Orgánica de Protección de Datos, sino introducir las modificaciones necesarias en la existente LORTAD[48].
En la Exposición de Motivos de este proyecto de ley orgánica, se afirma que, a pesar de que la LORTAD se promulgase antes de la aprobación de la Directiva 95/46, los contenidos de la misma ya se tuvieron en cuenta por el legislador español a la hora de su aprobación, afirmando que ello significa que la LORTAD "se ajusta en la mayoría de sus previsiones a las disposiciones contenidas en la Directiva 95/46 siendo necesario únicamente introducir en aquélla las precisas reformas que den como resultado la total adecuación entre dicha ley y la Directiva comunitaria". La Exposición de Motivos no hace referencia alguna a los recursos de inconstitucionalidad presentados contra la LORTAD y por aquel momento todavía pendientes de resolución, y cuyos artículos cuestionados son reproducidos en este proyecto de ley. Ante las numerosas enmiendas presentadas al proyecto de ley, al final verá la luz una nueva ley orgánica que derogará la LORTAD, la Ley 15/1999 de Protección de datos de carácter personal, en adelante, LOPD.

---

[48] Así, se publicó en el BOCG, VI legislatura, Serie A, n. 135-1, de 31 de Agosto de 1988, el Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 5/1992 de 29 de Octubre de regulación del tratamiento automatizado de los datos de carácter personal, disponible en http://www.congreso.es/public_oficiales/L6/CONG/BOCG/A/A_135-01.PDF

La LOPD se publica el 13 de Diciembre de 1999, y por tanto, incumpliendo el plazo de transposición[49] marcado por la Directiva 95/46, cuyo límite era el 24 de Octubre de 1998. La LOPD, a diferencia de la LORTAD y del proyecto de ley orgánica de reforma de la LORTAD, carece de Exposición de Motivos, quizá dado el apremio temporal por encontrarnos fuera del plazo de transposición, aunque su estructura y extensión es bastante similar. También llama la atención que no se haga referencia alguna al artículo 18.4 de la CE, fundamento primigenio del derecho a la protección de datos de carácter personal en nuestra Carta Magna.

1.2.2.1 Objeto

En su artículo 1 la LOPD establece que "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".
Vemos cómo el objeto de la LOPD difiere del consignado por la LORTAD pues ésta tenía por objeto desarrollar el mandato establecido el artículo 18.4 de nuestra CE, y así establecía "*La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".*
El objeto establecido por la LOPD trae causa del establecido por la Directiva 95/46 "Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las

[49] El artículo 32.1 de la Directiva 95/46 aprobada el 24 de octubre de 1995 establece "Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción (...)".

libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales" aunque ésta última no hace referencia al honor ni a la intimidad "personal y familiar".

1.2.2.2 Ámbito de aplicación

Uno de los principales mandatos de la Directiva 95/46 era extender la protección de datos de carácter personal, no sólo a los tratamientos automatizados como hacía la LORTAD, sino también a los no automatizados. El ámbito de aplicación de la Directiva se refiere "*al **tratamiento** total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero"* (art 3.1). Mientras que la LOPD "*será de aplicación a los datos de carácter personal **registrados en soporte físico**, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado*".

Nótese la diferencia entre ambos preceptos, ya que mientras la Directiva 95/46 habla genéricamente de "tratamiento" de datos, con independencia por tanto de si forman parte de un fichero o no, la LOPD parece presuponer que para que sea posible la realización de un tratamiento, automatizado o no, de datos, éstos deben formar parte de un fichero, por lo que así establece su ámbito de aplicación.

Y así parecía entenderlo también la Agencia Española de Protección de datos[50], recogiendo la jurisprudencia de la Audiencia Nacional, (sentencia de 16 de febrero de 2006), cuando se refiere al tratamiento de datos personales, poniendo en relación este concepto con el de fichero, al que configura como un *prius* necesario para la aplicación

[50] Informe 0573/2009 del Gabinete Jurídico de la AEPD disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2009-0573_Necesidad-de-existencia-de-fichero-para-la-aplicaci-oo-n-LOPD-al-tratamiento-manual-de-datos-personales.pdf

de la Ley Orgánica 15/1999, si bien es cierto que en el contexto de un tratamiento manual. La mencionada sentencia afirma "para que una actuación *manual* sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizados de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "tratamiento de datos personales" según el concepto normativo que la ley proporciona.

En realidad la existencia del 'fichero' en el sentido legal es siempre precisa para que un tratamiento de datos personales esté sujeto al sistema de protección de la ley. En los casos de tratamiento *automatizado* de datos-siempre sometidos a la ley- es difícil imaginar la inexistencia de un fichero (aunque no se exija expresamente) puesto que los datos que se tratan mediante sistemas automatizados lo son siempre bajo unos criterios de estructura u organización previa".

A nuestro juicio esto supone una incorrecta trasposición de la Directiva 95/46, ya que en el Considerando 12 de la misma, se establece que "que los principios de la protección deben aplicarse a todos los **tratamientos** de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario (…)" y el 14, "Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los **tratamientos** que afectan a dichos datos"; aclarando el Considerando 15, "que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están **automatizados o** cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos **en un archivo estructurado** según criterios específicos

relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata".

Consecuencia de lo anterior, quizá es la ampliación, de la definición de la figura del Responsable del Fichero, añadiendo, "o **tratamiento**", como "la persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del **tratamiento**", pero lo que está claro es que el contenido del artículo 2.1 de la LOPD dice lo que dice, y contradice lo establecido por la Directiva, aunque a efectos prácticos, acudiendo al Efecto Directo de la Directiva por una deficiente trasposición, dicho obstáculo quedaría salvado, y actualmente la AEPD[51] no tiene en cuenta la literalidad del mencionado artículo 2.1 LOPD

Asimismo, el artículo 2.1 de la LOPD concreta (casi reproduciendo literalmente el artículo 4 de la Directiva 95/46[52]) que se regirá por la presente ley todo tratamiento de datos de carácter personal:

---

[51] Así, en el Informe Jurídico 0279/2009 se afirma "(…) la Ley Orgánica 15/1999, establece en su artículo 2.1 que "La presente Ley Orgánica será´ de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". En consecuencia, la Ley Orgánica 15/1999 resultará de aplicación a todos los supuestos en los que exista un tratamiento de datos de carácter personal, definidos por el artículo 3 a) de la misma como "Cualquier información concerniente a personas físicas identificadas o identificables." En este sentido, si se produce un tratamiento de datos con información concerniente a personas físicas identificadas e identificables, que según se desprende del contenido de la consulta, parece que efectúa la consultante, con independencia de si se crea o no un fichero, sí resulta de aplicación las previsiones de la Ley Orgánica 15/1999 y su Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre". Informe disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/naturaleza_pub_pri_ficheros/common/pdfs/2009-0279_Constituci-oo-n-y-creaci-oo-n-de-ficheros-en-soporte-papel-y-automatizados.pdf

[52] El artículo 4.2 de la Directiva 95/46 establece que "En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento", y dicho requisito no ha sido recogido por la LOPD.

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.
Por otro lado, quedan fuera del ámbito de la LOPD (artículo 2.2 LOPD):
a) los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) los ficheros sometidos a la normativa sobre protección de materias clasificadas
c) los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.
La primera exclusión es la conocida como "**ámbito doméstico**", relativa a los "tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares"[53] llevadas a cabo que el Tribunal de Justicia tuvo ocasión de precisar en la conocida sentencia Bodil Lindqvist[54]. Han de darse dos requisitos cumulativos para la aplicación de dicha excepción; en primer lugar que se trate de ficheros mantenidos por personas físicas y en segundo

[53] Artículo 4 del RD 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
[54] Sentencia del Tribunal de Justicia de 6 de noviembre de 2003, en el asunto prejudicial C101/01, disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=183168

lugar, que el tratamiento se realice en el ámbito exclusivo de una actividad personal o doméstica. La Sra Lindqvist, catequista, creó en su domicilio varias páginas web para que los feligreses de la parroquia pudieran disponer de información que les fuera de utilidad. En dichas páginas se publicó información sobre la Sra. Lindqvist y sus compañeros, incluyendo el nombre de pila y el algún caso el nombre completo, la situación familiar y número de teléfono e incluso señaló que una de sus compañeras se había lesionado un pie y que se encontraba en situación de baja parcial por enfermedad. Fue condenada a pagar una multa por haber tratado datos personales sin comunicación a la Autoridad de protección de datos sueca, por transferencia internacional sin autorización, y por tratamiento de datos sensibles sin consentimiento. Con ocasión del recurso presentado, se plantearon diversas cuestiones prejudiciales que arrojaron las siguientes conclusiones:

- la conducta de publicar información personal en una página web constituye un tratamiento total o parcialmente automatizado de datos, y por tanto, no queda amparada por la exención doméstica.
- que es preciso dar una interpretación al concepto de datos relativos a la salud utilizada por la Directiva, por lo que la publicación del hecho de que una persona se ha lesionado un pie y está en situación de baja, debe considerarse un dato personal relativo a la salud,
- la publicación de datos personales en una página web, accesible desde cualquier país, incluidos países terceros, no supone una transferencia internacional de datos en el sentido del artículo 25 de la Directiva 95/46.

En sede nacional, la AN en Sentencia de 15 de Junio de 2006 tuvo ocasión de precisar el concepto de ámbito doméstico. El supuesto de hecho consistía en la organización de una celebración (bodas de plata) por parte de una promoción de la Academia General Militar, lo cual implicó la creación de un fichero con los datos de todos los antiguos alumnos por parte de la comisión organizadora y su comunicación a una agencia de viajes, la cual comunicó con los antiguos alumnos que figuraban en dicho fichero para enviar información sobre el evento.

La AEPD consideró que cuando los datos de las agendas personales salen de la esfera personal y forman parte de un conjunto de datos recogidos para la promoción de un evento, nos encontramos ante un tratamiento de datos sujeto al ámbito de aplicación de la LOPD, y por tanto, sancionó dicha actuación. Por su parte, la AN, partiendo de la afirmación de que no es tarea fácil dilucidar qué ha de entenderse por "personal" o "doméstico", ya que en algunos casos lo personal y profesional aparecen entremezclados, afirma que:

- la utilización del adverbio "exclusivamente" en el art. 2.2.a) apunta a que los ficheros mixtos, en los que se comparten datos personales y profesionales, quedarían incluidos en el ámbito de aplicación de la ley al no tener como finalidad exclusiva el uso personal.
- El hecho de que el tratamiento lo realice un único individuo no es indicativo de que el tratamiento se desarrolla en un ámbito exclusivamente personal, pues actividad individual no debe identificarse con actividad "personal".
- Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos.

En relación al caso concreto, la AN concluye que no se pretendía una finalidad profesional ya que la finalidad del tratamiento no excedía del ámbito íntimo y privado, aunque implicase la participación de un colectivo numeroso de personas. Así, afirma[55] que "La pretensión de que tales actividades, en cuanto al tratamiento de datos, debieran quedar sujetas a los principios de protección contemplados en la ley 15/1999, con fundamento en una concepción maximalista del principio del consentimiento, como parece expresar la Agencia de Protección de Datos, conllevaría una desnaturalización de las relaciones sociales, sometiéndolas a unos rigores formales en cuanto al manejo de datos personales totalmente ajenos al sentir social y en modo alguno exigidas por el derecho fundamental a la

[55] SAN 3077/2006 de 15 de Junio de 2006, FD 3.

autodeterminación informativa, derecho que no es absoluto y que debe ser interpretado en cuanto a sus manifestaciones y exigencias partiendo de su contraposición con otros derechos y valores constitucionales, como el libre desarrollo de la personalidad, y de la realidad social a la que está dirigido".

La redacción dada por la LOPD a la exclusión del ámbito doméstico, varía de la anteriormente establecida por la LORTAD ("*ficheros mantenidos por personas físicas con fines exclusivamente personales*"), ya que introduce el término utilizado por la Directiva 95/46[56] "*actividades exclusivamente personales o domésticas*" y por tanto, no refiriéndose únicamente a los fines, lo cual viene a concretar el ámbito de aplicación de la excepción, que bajo la vigencia de la LORTAD dio lugar a interpretaciones extensivas[57] de la misma.

El RD 1720/2007 que desarrolla la LOPD, no se limita sólo a los "ficheros" sino que hace referencia también a los "tratamientos" y además, añade un párrafo aclaratorio, "*sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares*".

La segunda exclusión establecida por el artículo 2.2 b) de la LOPD es la relativa a *los* ***ficheros sometidos a la normativa sobre protección de materias clasificadas***. En su desarrollo reglamentario, el artículo 4 b) del RD 1720/2007 se limita a reproducir lo establecido por la LOPD.

Para aclarar el concepto de "materias clasificadas" hemos de acudir a la Ley de Secretos Oficiales[58] que establece que podrán ser declaradas materias clasificadas "*los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado*". Tal y

---

[56] Art. 3.2 de la Directiva 95/46 "(...) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

[57] Cfr. Protección de Datos. Comentarios al Reglamento, LEX NOVA, 2008, pp. 81 y 82.

[58] Artículo 2 de la Ley 9/1968, de 5 de abril, sobre secretos oficiales, en su redacción dada por la Ley 48/1978, 7 octubre.

como se indica en la propia Exposición de Motivos, en la denominación de "materias clasificadas", también utilizada en otros países, se comprenden los dos grados de secretos oficiales generalmente admitidos, es decir, secreto y reservado, en atención al grado de protección que requieran[59] correspondiendo dicha calificación, sin que pueda ser transferida o delegada, exclusivamente, en la esfera de su competencia, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor[60] o bien, sean así declaradas por una ley.

En este punto debe tenerse en cuenta el Acuerdo del Consejo de Ministros de 28 de Noviembre de 1986, el cual otorga a determinadas materias el carácter de "secreto" o "reservado"[61].

Así, se otorga con carácter genérico la clasificación de "secreto" a:

-Las claves y material de cifra criptográfico.

---

[59] Artículo 3 de la Ley 9/1968 sobre Secretos Oficiales.

[60] Artículos 4 y 5 de la Ley 9/1968 sobre Secretos Oficiales.

[61] Destacar la STS de 4 abril de 1997 sobre los papeles del CESID, que sienta las bases jurisprudenciales sobre la desclasificación de documentos. Recomendamos la lectura del resumen que de dicha sentencia realiza TORRES VENTOSA, J. J., "La regulación legal de los Secretos Oficiales". *Anuario de la Facultad de Derecho*, 1998, n. 16, pp. 382-388. Suscribimos plenamente las conclusiones del autor, el cual aboga por la aprobación de una nueva legislación "plenamente acorde con los principios del Estado social y democrático de derecho que la *Lex Suprema* proclama, y ello por más que tanto el T.C.J. como el T.S. manifestaran en su día, *expressis verbis*, la conformidad de aquélla con la Constitución" para evitar lo sucedido en la desclasificación de los papeles del CESID "(…) un juez penal lo solicita del Ministerio de Defensa, éste se niega y plantea un conflicto de jurisdicción, un Tribunal especial, el T.J.C., falla a favor de la administración, el juez pide de nuevo los documentos al Gobierno, que se los deniega, y las partes de ese proceso penal interponen recurso Contencioso-Administrativo, que es resuelto por el T.S. a favor de los particulares-, no es viable en el futuro". Defiende que sea un único órgano el que conozca de la clasificación de una materia reservada o secreta, el Consejo de Ministros, de la misma manera que el control de sus decisiones, no ha de atribuirse a "órganos híbridos de naturaleza jurídica indeterminable". También aboga por la inclusión de un criterio de desclasificación automática por el mero transcurso del tiempo.

-El despliegue de unidades y orden de batalla; el Centro de Conducción de Operaciones Estratégicas (CECOE) y, en general, todos los sistemas de mando, control y comunicaciones, incluidas las redes militares permanentes.
-Las deliberaciones de la Junta de Defensa Nacional, de la Junta de Jefes de Estado Mayor, de los Consejos Superiores de los tres ejércitos y de la Comisión Delegada del Gobierno para Situaciones de Crisis.
-La estructura, organización, medios y procedimientos operativos específicos de los servicios de información, así como sus fuentes y cuantas informaciones o datos puedan revelarlas.
-Los estados de eficacia operativa y de moral de las unidades.
-Los informes y datos estadísticos sobre movimiento de fuerzas, buques o aeronaves militares.
Y el carácter de "reservado" a:
-Los destinos de personal de carácter especial.
-Los planes de seguridad de Instituciones y organismos públicos así como de las Unidades, Centros u Organismos de las Fuerzas Armadas y de los Centros de Producción de Material de Guerra.
-Los planes de protección de todas aquellas personas sometidas a la misma, específicamente de las autoridades y de los miembros de las Fuerzas Armadas.
-Las investigaciones y desarrollos científicos o técnicos de carácter militar realizadas por industrias militares o de interés para la defensa.
-La producción, adquisición, suministros y transportes de armamento, munición y material bélico.
-Las conceptuaciones, informes individuales y sanciones del personal militar.
-Las plantillas de persona y de medios y de equipo de las Unidades.
Y todos aquellos documentos necesarios para el planeamiento, preparación o ejecución de los documentos, acuerdos o convenios a que se refieren los apartados anteriores, tendrán también a su vez el carácter de secreto o reservado, según corresponda.
El tercer grupo de ficheros (o tratamientos, como precisa el RD 1720/2007 en su artículo 4), excluidos del ámbito de aplicación de la

LOPD son los "*establecidos para la investigación del* ***terrorismo y de formas graves de delincuencia organizada****. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos"*. El desarrollo reglamentario se limita a reproducir lo establecido en la LOPD. La LORTAD no hacía referencia alguna a este tipo de ficheros entre las materias excluidas[62] de su ámbito de aplicación, por lo que *a sensu contrario* se encontraban incluidos, aunque pudiera haber ciertas matizaciones, como las aplicables a los ficheros policiales. A primera vista, la lectura del precepto no parece entrañar ninguna dificultad interpretativa, pero como señala PUENTE ESCOBAR[63] caben dos posibles interpretaciones:

1) atendiendo a la finalidad del fichero, tal y como establece el precepto. No obstante, este criterio presenta el problema de que si realizamos una interpretación literal, nos llevaría a excluir del ámbito de aplicación de la LOPD aquellos ficheros que, aun no teniendo como finalidad principal la investigación del terrorismo u otras formas graves de delincuencia organizada, contengan datos

---

[62] Artículo 2.2. LORTAD "El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:
-A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.
-A los ficheros mantenidos por personas físicas con fines exclusivamente personales.
-A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.
-A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.
-A los ficheros mantenidos por los partidos políticos, sindicatos e Iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

[63] PUENTE ESCOBAR, A., *op. cit.* en Protección de Datos. Comentarios al Reglamento, pp. 87-88.

relacionados con estas finalidades. Esta interpretación conllevaría la exclusión del ámbito de la LOPD, de la totalidad del fichero, no sólo de aquellos datos recabados para las finalidades que el precepto excluye, lo cual supone al tiempo contradecir la propia LOPD que no pretende en ningún momento dicha solución, pues establece normas específicas en relación a los ficheros policiales.

2) Interpretación objetiva, es decir, quedarían excluidos aquellos ficheros que, teniendo dichas finalidades, hubieran sido previamente notificados a la AEPD, con independencia de la finalidad del fichero. Esta interpretación presenta el problema de que la aplicación del régimen de protección de datos dependerá de un trámite meramente formal como es el registro de un fichero ante la AEPD, quedando por tanto todos aquellos ficheros no comunicados a la AEPD, sometidos al régimen de protección de datos. Podría rebatirse a su vez que este problema parte de un incumplimiento de la normativa general de protección de datos (obligación de registro de ficheros), y que por tanto, este criterio no presenta ninguna objeción.

No obstante, este ha sido el criterio acogido, pero atendiendo únicamente a la finalidad del fichero, y no al cumplimiento o incumplimiento del trámite formal del registro del fichero ante la AEPD.

Respecto a los ficheros creados para la investigación de "formas graves de delincuencia organizada", surge el problema de qué delitos entendemos incluidos en esta expresión. Es el mismo problema que ocurre cuando la *Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas* utiliza[64] la expresión "delitos graves" en la descripción del objeto de la Ley.

---

[64] Artículo 1.1 Ley 25/2007 de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*: Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y*

Podría acudirse a textos internacionales como cita[65] PUENTE ESCOLAR, la Directiva 2006/24 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones que menciona como "asuntos de gravedad" la delincuencia organizada y el terrorismo; o el Convenio de Creación de Europol, que menciona en su Preámbulo "los problemas urgentes que plantean el terrorismo, el tráfico ilícito de drogas y otras formas graves de delincuencia internacional" o en su artículo 2.2 donde precisa los delitos que comportarán la actuación de Europol, "(…) tráfico ilícito de estupefacientes, de material nuclear y radiactivo, las redes de inmigración clandestina, la trata de seres humanos y el tráfico de vehículos robados".

No obstante lo anterior, no consideramos que puedan tomarse estos textos como criterio para determinar el alcance de la expresión "formas graves de delincuencia organizada". En primer lugar, porque no aportan la seguridad jurídica que la definición de la expresión precisa, ya que son meras enumeraciones no exhaustivas. En segundo lugar, porque la LOPD habla de "formas graves de delincuencia organizada", lo que dejaría dentro del ámbito de aplicación de la LOPD a delitos graves que no entren dentro del concepto de delincuencia organizada[66].

---

*enjuiciamiento de **delitos graves** contemplados en el Código Penal o en las leyes penales especiales*".

[65] PUENTE ESCOBAR, A., *op. cit.*, p. 89.

[66] El artículo 282 bis 4. de la Ley de Enjuiciamiento Criminal establece "4. A los efectos señalados en el apartado 1 de este artículo, se considerará como **delincuencia organizada** la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

Entendemos que el criterio que más seguridad jurídica aporta para establecer el contenido de la expresión "delitos graves" es, siguiendo a MAEZTU LACALLE[67], acudir al artículo 33.2 de nuestro Código Penal que establece como pena grave la prisión superior a cinco años.

1.2.2.3 Definiciones

Tras analizar el Objeto y Ámbito de aplicación, el Título I de la LOPD termina incluyendo diez definiciones[68] de los términos más utilizados

---

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.
f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.
g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.
h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.
i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.
j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.
k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.
l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.
m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.
n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.
o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando.

[67] MAEZTU LALLE, D., en su blog *"El TS ratifica la Ley de Conservación de datos"* http://derechoynormas.blogspot.com.es/2010/02/el-tribunal-supremo-ratifica-la-ley-de.html

[68] Artículo 3 de la LOPD: A los efectos de la presente Ley Orgánica se entenderá por: a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables. b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. c) Tratamiento de datos: operaciones y

en la normativa de protección de datos. A las definiciones de dato de carácter personal; fichero; tratamiento de datos; Responsable del fichero o tratamiento; Afectado o interesado y procedimiento de disociación, se añaden **cuatro nuevos conceptos** que no aparecían en la LORTAD: Encargado del tratamiento; Consentimiento del interesado; cesión o comunicación de datos; Fuentes accesibles al público.

Destacar que en la LOPD se omite la constante referencia a los ficheros automatizados, ya que se incluyen también los ficheros realizados sobre ficheros manuales o no automatizados. También se denomina al "afectado" como "interesado".

---

procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo. f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable. g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen. i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado. j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

1.2.2.4 Principios

En el Título II de la LOPD, al igual que en la LORTAD, se establecen los "Principios de la protección de datos". Dichos Principios se manifiestan en el Título III (igual que en la LORTAD), estableciendo los correspondientes derechos de los interesados. Estos Principios vienen a seguir los establecidos a nivel internacional[69] y en sede comunitaria y su objetivo es preservar el derecho fundamental a la protección de datos, estableciendo unas obligaciones para todos los agentes involucrados en el tratamiento de datos así como los derechos que a los titulares de los datos objeto de tratamiento les competen.
Haremos hincapié y profundizaremos en los Principios que rigen la normativa de protección de datos actual, ya que será importante a la hora de comparar otros sistemas legislativos así como para valorar la evolución de la normativa.

1.2.2.4.1 Principio de Calidad de los datos

El Principio de Calidad ocupa un lugar muy importante entre los Principios que rigen la normativa de protección de datos ya que recoge las bases que han de regir todo tratamiento de datos, bien sea por el sector privado o público. Nuestra LOPD[70] recoge aquí las bases y principios establecidos por el Convenio 108 del Consejo de Europa

[69] En el apartado relativo al Marco Jurídico del presente capítulo profundizaremos en dichos instrumentos internacionales y comunitarios, pero básicamente ahora nos referimos al Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984 y a la Directiva 95/46, 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.

[70] El artículo 4 de la LOPD y el artículo 8 del RD 1720/2007, recogen lo establecido por el Considerando 28 y artículo 6 de la Directiva 95/46 y artículo 5 del Convenio 108 del Consejo de Europa.

y que posteriormente fueron recogidos por la Directiva 95/46, los cuales analizaremos en el apartado siguiente.

Si acudimos a la Exposición de Motivos de la derogada LORTAD, podemos ver el lugar preeminente del Principio de Calidad,

"Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, se pretende limitar". El Principio de Calidad se recoge en el artículo 4[71] de la LOPD, y supone que

[71] Artículo 4 LOPD Calidad de los datos:

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

únicamente podrán recogerse y someterse a tratamiento[72], aquellos datos de carácter personal que sean adecuados, pertinentes y no excesivos, en relación con el ámbito y finalidades para las que fueron recogidos, las cuales además deberán ser determinadas, explícitas y legítimas[73]. Es por ello que se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos, es decir, mediante engaño o de cualquier forma no lícita, constituyendo en su caso una infracción muy grave (artículo 44.4 a) LOPD). Así, vemos cómo el Principio de Calidad recoge a su vez los **Principios de Proporcionalidad y Finalidad**, de una importancia capital en la recogida y tratamiento de datos de carácter personal. Tan es así que la falta de concreción de las finalidades en el momento de la recogida, puede hacer que el consentimiento devenga nulo. De esta manera, el Principio de Finalidad se aplica no solamente en la recogida y tratamiento de los datos, sino también en la cesión[74] de los mismos.

Asimismo, los datos deberán ser *exactos* y *puestos al día (**Principio de Veracidad o exactitud**)*, de modo que sean veraces por responder a

---

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

[72] Se distingue entre recogida y tratamiento de datos, lo cual, según LESMES SERRANO, C. y otros, en *La Ley de Protección de Datos. Análisis y comentario de su Jurisprudencia*, LEX NOVA, Valladolid, 2008, p. 142, supone "una distinción que desde un punto de vista jurídico resulta difusa, ya que el art 3c) de la LOPD al definir el tratamiento de datos, incluye en dicho concepto las operaciones y procedimientos técnicos de carácter automatizado o no que permitan la recogida de los datos".

[73] La LORTAD sólo hablaba de "finalidades legítimas", por lo que la LOPD ha querido acentuar el Principio de Finalidad.

[74] En el caso de la cesión de datos, el art 11.3 LOPD y el 12.2 del RD 1720/2007, el cual establece que "cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo".

la situación *actual*[75] del afectado. De hecho el propio artículo 4 LOPD señala que si los datos resultasen inexactos, en todo o en parte, deberán ser cancelados y sustituidos de oficio por los datos rectificados o completados.

Por tanto, el Principio de Veracidad y exactitud supone la imposición de una obligación al Responsable de actualizar o cancelar los datos, sin necesidad de que el interesado realice ninguna solicitud, cuyo incumplimiento puede derivar en la imposición de una sanción grave[76]. Destacar que el Reglamento, a diferencia de la LOPD, establece una presunción *iuris tantum* a favor del Responsable, de que los datos recogidos directamente del interesado se considerarán exactos. Corolario del Principio de Veracidad y exactitud, se establece la *obligación del Responsable de cancelar o sustituir*, aquellos datos que, respectivamente, resulten inexactos (total o parcialmente) o incompletos, con independencia de los derechos de rectificación y cancelación de que disponen los interesados. El Reglamento nos concreta que dicha cancelación de datos inexactos o sustitución de los incompletos, deberá realizarse en un plazo de diez días a contar desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o plazo específico para ello. Asimismo, si los datos hubiesen sido comunicados previamente, el Responsable deberá notificar al cesionario, también en un plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido, el cual deberá, en un plazo de diez días desde la recepción de la notificación, proceder a la rectificación o cancelación notificada. En este caso, el cesionario no deberá comunicar al interesado la actualización realizada. Quizá pueda parecer que el Principio de Veracidad y exactitud no es tan

---

[75] El art. 4.3 de la LORTAD empleaba la expresión situación "real" en lugar de "actual" como hace la LOPD en su artículo homónimo.

[76] Art. 44.3 LOPD "son infracciones graves: c) tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave". Para casos concretos en los que se produce (y no se produce) vulneración del Principio de Veracidad, Vid. LESMES SERRANO, C., *op. cit.*, pp. 156-158.

importante como los Principios de Finalidad y Proporcionalidad, pero en realidad, sin el cumplimiento del Principio de Veracidad, probablemente viéramos conculcados el resto de principios, tal y como afirma[77] LESMES SERRANO.

Una variación bastante discutida con respecto a la redacción de la LORTAD, es el párrafo segundo del presente artículo 4 LOPD (y del mismo modo el RD 1720/2007 en su artículo 8.3), el cual establece que "*los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos"* (excluyendo el tratamiento posterior con fines históricos, estadísticos o científicos, que el artículo 9.1 declara expresamente no incompatibles). Con respecto a esta excepción al Principio de Finalidad para el tratamiento posterior con fines históricos, estadísticos o científicos, la LOPD viene a recoger lo establecido en la Directiva 95/46[78]. La propia LOPD en su artículo 4.5 *in fine* se remite al Reglamento para determinar el "procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos". Así, el Reglamento establece en su artículo 9.1, que para determinar los fines históricos, estadísticos o científicos, deberá atenderse a la legislación que en cada caso resulte aplicable, y en particular a la Ley 12/1989 de 9 de Mayo Reguladora de la función estadística pública, la Ley 16/1985 de 25 de Junio, del Patrimonio Histórico español y la Ley 13/1986 de 14 de Abril de Fomento y coordinación general de la investigación científica y técnica, sus respectivos reglamentos así como a la normativa autonómica en la materia. Además, se añade la posibilidad de que la AEPD o autoridad autonómica de control, previa solicitud del

---

[77] LESMES SERRANO, C., *op. cit*, p. 154 i.f.

[78] El Considerando 29 de la Directiva 95/46 establece "considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona".

Responsable del tratamiento, puedan acordar[79] el mantenimiento íntegro de determinados datos, en razón de su valor histórico, estadístico o científico. La LORTAD, además de no hacer mención a la exclusión del tratamiento posterior con fines históricos, estadísticos o científicos, utiliza la expresión "finalidades distintas" mientras la LOPD habla de finalidades "incompatibles". Al utilizar el vocablo "incompatible", permite la utilización de los datos para finalidades *diferentes* para las que fueron recogidos, siempre que sean *compatibles*, lo cual podemos entender choca de plano con la exigencia de que las finalidades sean determinadas, explícitas y legítimas, suponiendo por tanto una ampliación del ámbito de aplicación.

En este punto cabe recordar la literalidad del Considerando 28 de la Directiva 95/46 que establece "Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal, con respeto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención de los datos no pueden ser *incompatibles* con los objetivos originariamente especificados".
Podemos entender por tanto, que existe una diferencia entre las finalidades especificadas en el momento de la recogida de los datos (que recordemos, ha de ser explícitas, determinadas y legítimas) y las finalidades de los tratamientos posteriores (las cuales no podrán ser incompatibles con las establecidas en el momento de la recogida); o bien, podemos entender que se trata de una traducción literal de los términos utilizados por la Directiva 95/46 y que debe realizarse una interpretación sistemática del precepto, no ampliando por tanto el ámbito objetivo de tratamiento con finalidades compatibles pero no determinadas previamente en el momento de la recogida de datos. Así opina VIZCAÍNO CALDERÓN: "probablemente la cuestión deriva de una

[79] Siguiendo el procedimiento establecido en el art 157 del RD 1720/2007, Sección 2ª.

adaptación excesivamente apresurada del texto del artículo 6.1b) de la Directiva. (…) parece que la Ley utiliza el término "incompatibles" como sinónimo de "distintas" o "diferentes" partiendo de la concreción finalista de la recogida y tratamiento que constituye la base de la Ley"[80]. Esta segunda interpretación es la acogida por la AN en su Sentencia de 11 de Febrero de 2004[81] la cual establece (la negrita es nuestra): "*En relación con la interpretación de la expresión "finalidades incompatibles" que establece el artículo 4.2 de la Ley Orgánica 15/1999, esta Sala no puede compartir el criterio que postula la recurrente, pues aunque el artículo 4.2 de la Ley 15/99, en contraposición con el artículo 4.2 de la Ley 5/92, ya no se refiere a "finalidades distintas", sino a "finalidades incompatibles", revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto y la ambigüedad del término "finalidades incompatibles" avalan la interpretación realizada en el acto administrativo impugnado. En efecto, según el diccionario de la Real Academia "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre sí", por tanto****, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades****, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo y como tal ha de rechazarse", como hemos declarado en Sentencia de 8 de febrero de 2002. Teniendo en cuenta, además, que dicho término se introduce en la Ley de 1999, como ha declarado la doctrina, por una traducción poco precisa del artículo 6 de la Directiva 46/1995, de 24 de octubre.*
Conclusión igualmente avalada por la **interpretación sistemática** aludida, pues como señalamos en la citada Sentencia de 8 de febrero de 2002, <<semejante prescripción no puede ser entendida sino como

[80] VIZCAÍNO CALDERÓN, M., Comentarios a la Ley Orgánica de protección de datos de carácter personal, Civitas, 2001, 1ª ed., pp. 94 y 95.
[81] SAN 845/2004, de 11 de Febrero de 2004, Rec Núm 119/2002, FD 4. Para más información sobre Jurisprudencia de la AN en dicha materia, Vid. LESMES SERRANO, C., *op. cit.*, pp. 148-152.

un enunciado de carácter general, que no puede prevalecer sobre la regulación específica de una materia>>, citando al efecto el artículo 6 de la citada Ley, y añadiendo que la interpretación de dicho artículo 6.2, a sensu contrario, impone <<que cuando los datos se usen con otra finalidad distinta se precisará el consentimiento del afectado. **Y no parece que el art. 4.2, venga a efectuar una ampliación sobre la posibilidad de utilización de los datos, como entiende el actor, porque ello supondría dejar sin contenido el art. 6.2**, cuya redacción en este punto es igual a su homónimo de la Ley 5/92".

Por tanto, hemos de entender, tal y como lo hace la AEPD[82] y la AN, que la expresión finalidades "incompatibles" es sinónima a "diferentes".

Se establece en el párrafo quinto del artículo 4 LOPD, la ***obligación de cancelar*** **los datos una vez dejen de ser necesarios o pertinentes** para la **finalidad** para la cual hubieran sido recabados, por lo que, como dice el propio artículo, "no serán conservados" de manera que se permita la identificación del interesado por un tiempo superior al necesario para el cumplimiento de las finalidades del tratamiento. Por tanto, es la finalidad la que determina si los datos deben ser o no cancelados, partiendo de la base de que todo tratamiento tiene una duración determinada.

Como excepciones a esta obligación general de cancelación de los datos, el RD 1720/2007 en su artículo 8.6 menciona dos supuestos: durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Una vez cumplidos los plazos provenientes de estos dos

---

[82] Tratamiento de datos para fines incompatibles. Informe 0078/2005, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2005-0078_Tratamiento-de-datos-para-fines-incompatibles.pdf donde recoge la interpretación dada por el TC en la STC 292/2000, de 30 de Noviembre, que identifica el término "incompatibles" con "distintos", ver FFJJ 5º y 13º.

supuestos, los datos sólo podrán ser conservados previa disociación[83] de los mismos, o bien, dando lugar, ahora sí, a la obligación de bloqueo derivada de la cancelación. Es por ello que entre los supuestos en que cabe denegar el derecho de cancelación[84] se encuentran precisamente la obligación de conservar los datos durante los plazos previstos en las disposiciones aplicables[85] o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado. Destacar, que en la práctica, pocos Responsables de ficheros proceden a la cancelación de los datos una vez cumplidos los fines del tratamiento.

1.2.2.4.2 Deber de información en la recogida de los datos

El artículo 5 LOPD, derivado del artículo 10 de la Directiva 95/46, recoge el "derecho de información en la recogida de datos" que se traduce en un deber de informar del Responsable del fichero o tratamiento[86]. El artículo 18 del RD 1720/2007[87], anulado por la

[83] Artículo 3 f) LOPD "Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable".

[84] Artículo 33 LOPD.

[85] Por ejemplo, la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 17.1 establece un plazo de conservación de la documentación clínica "para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial".

[86] Artículo 3 d) LOPD "Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

[87] Artículo 18 RD 1720/2007: Acreditación del cumplimiento del deber de información

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre , deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

Sentencia TS Sala 3.ª 15 Jul. 2010, establecía en el Responsable la carga de la prueba respecto del cumplimiento del deber de información, mediante la conservación del medio o soporte que permitiera acreditar su cumplimiento, debiendo conservarlo mientras persistiera el tratamiento de los datos del afectado. La razón de la anulación de este artículo, según el TS, es que si la LOPD no especifica nada en cuanto a la forma en la que debe cumplirse con el derecho de información, el Reglamento estaba creando una obligación adicional (y nueva) respecto al propio deber de informar, obligando a la forma en que debe conservarse la acreditación del deber de informar. Cabría pensar que la anulación de este precepto supondría para los Responsables la no necesidad de acreditar el cumplimiento de la obligación de informar, pero si acudimos al artículo 12.3 del RD 1720/2007, el cual establece que corresponde al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho, vemos cómo sigue recayendo en éste la carga de la prueba con respecto a la obligación de informar y recabar el consentimiento. Por tanto, con respecto a la forma mediante la que se ha de llevar a cabo el deber de información por parte del Responsable, rige el Principio de Libertad de forma, pero siempre teniendo en cuenta que ha de poder acreditar su cumplimiento. Si el derecho fundamental a la protección de datos parte de la premisa del poder de disposición de las personas con

---

2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Artículo 18 anulado por Sentencias TS (Sala 3.ª, Sección 6.ª) de 15 julio de 2010; Recursos 23 y 25/2008 (B.O.E. 26 octubre).; TS, Sala Tercera, de lo Contencioso-administrativo, Sección 6ª, S, 15 Jul. 2010 (Rec. 23/2008); TS, Sala Tercera, de lo Contencioso-administrativo, Sección 6ª, S, 15 Jul. 2010 (Rec. 25/2008); Sentencia TS Sala 3.ª 15 Jul. 2010 (declara nulo el art. 18 del RD 1720/2007 de 21 Dic., Reglamento de desarrollo de la LO 15/1999 de 13 Dic., sobre Protección de Datos de Carácter Personal).

respecto a sus datos personales, el derecho de información se configura como requisito indispensable para que este poder de disposición tenga lugar, pues si no se facilita la información mínima necesaria, el interesado no podrá prestar un consentimiento previo (pudiendo dar lugar a un vicio del consentimiento), ni mucho menos ejercitar sus derechos. A diferencia de la LORTAD que únicamente preveía el deber de información cuando los datos se obtengan directamente del interesado, la LOPD incluye el deber de información también en aquellos supuestos en que los datos no hayan sido recabados directamente del interesado. El artículo 5 LOPD establece:

"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".

Destacar el énfasis que se realiza en que el interesado sea informado de los extremos anteriormente mencionados, con carácter previo y de modo expreso, preciso e inequívoco. Y ello es así porque es la única manera de que el interesado pueda dar un consentimiento real y plenamente consciente sobre la trascendencia e implicaciones que conlleva ese concreto acto de facilitar sus datos.

Todo tratamiento de datos requiere el *consentimiento inequívoco* del afectado, pero incluso cuando no sea preciso dicho consentimiento porque va implícito, por ejemplo, en la firma de un contrato, deberá cumplirse siempre con el deber de información. La ya mentada STC 292/2000, establece en su FJ 7º que "De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. **Y resultan indispensables para hacer efectivo ese contenido** el reconocimiento del **derecho a ser informado** de quién posee sus datos personales y con qué fin, y el

derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

Por tanto, el contenido mínimo del deber de información deberá incluir la identidad y dirección del Responsable del fichero o tratamiento a quien estamos facilitando los datos; la finalidad de la recogida de datos y los destinatarios de la información; del carácter obligatorio o facultativo de las solicitudes de información así como de las consecuencias de la obtención de dichos datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Con respecto a la obligación de informar sobre la identidad y dirección del Responsable del tratamiento, señalar también que deberá informarse en el caso de producirse una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, tal y como establece el artículo 19 del RD 1720/2006, no considerando este supuesto constitutivo de una cesión de datos.

La información, como hemos mencionado anteriormente, ha de proporcionarse de modo expreso, preciso e inequívoco, por lo que a la hora de describir la finalidad del tratamiento, no podrán utilizarse expresiones vagas o que de cualquier manera no permitan al interesado ser consciente de la concreta finalidad para la que se van a utilizar sus datos. Así, la Sentencia del Tribunal Supremo 2141/2005[88], ante la alegación de la empresa demandada de que los datos sobre los que se informa "se deducen de los que se solicitan o de las circunstancias que se recaban a los clientes", recoge los

[88] STS 2141/2005 de 11 de Abril de 2005 (Rec 4209/2001), FD 4.

argumentos dados por la sentencia recurrida: "Esta información, sin embargo, **omite un dato esencial exigido en el art. 5.1.a) que es el relativo a la finalidad** de la incorporación de los datos en el fichero **y los destinatarios** de tales datos, sin que la alusión que en la circular remitida por Telefónica a sus clientes, en orden a esa finalidad como la de 'proporcionarles los mejores servicios' suponga poner en conocimiento de los afectados —como exige la Ley— **el concreto destino que se persigue con la incorporación del dato en el fichero**, por lo que, a juicio de esta Sala y Sección, el contenido de dicha circular no cumple las exigencias de ese deber información establecido en el art. 5.1 y ese incumplimiento, acreditado, del deber de información que inexcusablemente recae sobre la actora integra el ilícito administrativo tipificado como infracción grave en el art. 43.3.c) de la LORTAD".

Respecto a la obligación de informar sobre el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas y de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, el párrafo tercero del artículo 5 LOPD exime de informar sobre ello si el contenido de la información proporcionada "se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban". En muchas ocasiones será fácilmente deducible la obligatoriedad de proporcionar determinada información, por ser necesaria para la finalidad para la cual se facilitan los datos (como por ejemplo, para la contratación de un servicio), por tanto, podemos afirmar que esta obligación de informar sobre el carácter obligatorio o no respecto de proporcionar determinada información, está directamente relacionada con la finalidad para la cual se recaban los datos, y por tanto, con el Principio de Calidad.

Cabría argumentar que la literalidad del artículo 5.3 LOPD utiliza conceptos genéricos y abiertos por tanto a la interpretación, en la definición del presupuesto para eximir del deber de informar sobre dichos extremos, generando cierta inseguridad jurídica, pero lo que en cualquier caso siempre podremos valorar es si los datos solicitados

son excesivos o no necesarios para la finalidad del tratamiento y por tanto, para juzgar si debería haberse cumplido con el deber de informar sobre el carácter voluntario o no de facilitar dichos datos y de las consecuencias de facilitar dichos datos o negarse a ello y si el interesado ha recibido la información de un modo preciso e inequívoco, como exige el mismo precepto.

El artículo 5.3 LOPD también incluye, entre los extremos sobre los cuales puede prescindirse de la obligación de informar, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Personalmente, no entendemos cómo puede haberse incluido esta posibilidad, por varios motivos, en primer lugar porque siempre será necesario informar sobre la posibilidad de ejercitar dichos derechos, que el interesado no tiene por qué saber de su existencia, y en segundo lugar, porque no se entiende en qué casos sería aplicable dicha excepción, es decir, cuándo podría deducirse esta información de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Si acudimos al artículo 10[89] de la Directiva 95/46, vemos cómo se incluyen todos los extremos obligatorios sobre los que debe informarse al interesado, y no sólo los que el 5.3 LOPD menciona, "salvo que se hubiera informado previamente", y además, con respecto a los extremos sobre los que se puede prescindir de informar (letras b), c) y d) del artículo 5 LOPD), la Directiva exige que deberá facilitarse dicha información

[89] Artículo 10 Directiva 95/46 "Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:
a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- los destinatarios o las categorías de destinatarios de los datos,
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen,
en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado".

suplementaria siempre resulte necesaria para garantizar un tratamiento de datos *leal* respecto del interesado. Además, destacar que la Directiva sólo habla de los derechos de "acceso y rectificación".

El párrafo segundo del artículo 5 LOPD establece que "cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior". Del presente apartado destacar la exigencia del carácter legible de la información proporcionada, con independencia del medio por el cual se recaben los datos.

La exigencia de la legibilidad no hace sino redundar en la importancia de que el consentimiento prestado sea inequívoco y por tanto, consciente.

Cuando la información no haya sido proporcionada directamente por el interesado, el párrafo cuarto del artículo 5 LOPD establece que *"éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo"*.

En primer lugar, podemos observar cómo el precepto en este caso sí incluye la posibilidad de haber informado anteriormente, como hacía el artículo 10 de la Directiva 95/46 en el caso de que los datos son recogidos del interesado directamente. No entendemos cómo en este caso sí se recoge esta posibilidad, cuando en realidad es menos probable que se produzca, dado que los datos no han sido recogidos directamente del interesado.

Dejando a un lado cuestiones sobre la correcta trasposición o no de la Directiva en este punto, resulta interesante el planteamiento que realiza LESMES SERRANO[90] sobre la excepción a este deber de informar cuando los datos no son recabados del interesado, establecida por el artículo 5.5 *in fine* con respecto a datos procedentes de fuentes accesibles al público y el apartado anterior cuando los datos procedan

[90] LESMES SERRANO, C., *op. cit.*, p. 183.

y se destinen a la actividad de publicidad o prospección comercial en cuyo caso, este deber de comunicación difiere y en lugar de realizarse en un plazo de tres meses desde la recogida de datos, se realizará en cada comunicación que se dirija al interesado, y deberá informar sobre el origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten. Dicho autor plantea la posibilidad de que en el caso de que los datos obtenidos de fuentes accesibles al público no se destinen a una actividad de publicidad o prospección comercial, se aplicaría la obligación de informar en el plazo de tres meses no estando incluídos por tanto, en la excepción de este deber de información ya que al fin y al cabo se trata de datos no recabados directamente del interesado. No obstante, el propio autor sostiene que es una cuestión que no está clara ya que el artículo 6.2 de la LOPD incluye dentro de los supuestos excepcionados de la obligación de recabar consentimiento, cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero, de la misma manera que el artículo 11.2 LOPD excepciona también del deber de obtener el consentimiento para la cesión de estos mismos datos.

Coincidimos con LESMES SERRANO en que cuando los datos sean recogidos de fuentes accesibles al público y no se destinen a actividades publicitarias o de prospección comercial, se aplicará la obligación de información establecida en el párrafo cuarto del artículo 5, y por tanto, deberá informar en el plazo de tres meses. Pero el hecho de que no sea necesario el consentimiento para el tratamiento de estos datos ni para su cesión, no es un argumento contrario a dicha postura, sino precisamente complementario, pues ya que se trata de un tratamiento no consentido a priori por el interesado, mediante el cumplimiento del deber de información, se le hace partícipe de la existencia del tratamiento y de la identidad del responsable, entre otros aspectos, de modo que en caso de no consentir a dicho tratamiento, pueda ejercitar el derecho de cancelación.

Junto al supuesto de tratamiento de datos obtenidos de fuentes accesibles al público para finalidades publicitarias, excepcionado del

deber de informar en el plazo de tres meses, el párrafo quinto del artículo 5, también excepciona de este deber cuando expresamente así una ley lo prevea, cuando el tratamiento tenga fines históricos estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. En estos casos, no hay una modificación del deber de informar como en el supuesto de tratamiento de datos obtenidos de fuentes accesibles al público para finalidades publicitarias, sino que directamente, no hay obligación de informar.

Cuando el tratamiento de datos estuviera expresamente previsto en una ley, no debemos olvidar que estamos dentro del supuesto en que los datos no han sido obtenidos del interesado, por lo que en el caso de obtenerse directamente de éste, sí deberemos informar, aunque el tratamiento o cesión vengan establecidos por una ley.

Cuando el tratamiento tenga fines históricos, estadísticos o científicos, tampoco será necesario cumplir con el deber de información establecido en el artículo 5.4 LOPD.

Con respecto a qué podamos entender como datos históricos, la AEPD en un Informe del año 2000[91] acude al artículo 57.1 c) de la Ley 16/1985 del Patrimonio histórico, que establece que "Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o *hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años a partir de la fecha de los documentos.* Por tanto, en los casos en los que no se cumplan estos

[91] Informe disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2000-0000_Alcance-del-concepto-del-tratamiento-de-datos-hist-oo-ricos-con-fines-cient-ii-ficos-o-de-investigaci-oo-n.pdf

plazos, no podemos considerar a estos documentos como de interés histórico, por lo que será necesario recabar el consentimiento para su tratamiento y publicación.

Cuando el tratamiento tenga fines estadísticos, tampoco será necesario cumplir con el deber de información establecido en el artículo 5.4 LOPD. En este caso acudimos a la Ley 12/1989, de 9 de Mayo, de la Función Estadística Pública, que establece se aplicará a todas las Administraciones Públicas en relación a las estadísticas con fines estatales.

El artículo 5.5 de la LOPD también excepciona del deber de información establecido en el párrafo anterior del mismo artículo, a los tratamientos con fines "científicos". La AEPD ha tenido ocasión de pronunciarse en relación al concepto de "fines científicos" en un Informe del año 2002[92]. Así, la AEPD afirma "El término científico, desde un punto de vista semántico implica pertenencia a una ciencia. Tal expresión, entendida literalmente, tiene una amplitud omnicomprensiva que implicaría la posibilidad de conectar prácticamente cualquier tratamiento de datos personales con una especialidad científica, tanto referida a las ciencias sociales como a las naturales. Así, incluso un estudio de mercado, de publicidad o de técnicas comerciales o publicidad tendría o podría establecérsele una conexión con una especialidad o rama del conocimiento (ciencias económicas, ciencias de la información etc.). Parece en consecuencia lógico que la interpretación auténtica de tal precepto deba efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la LOPD".

El artículo 5.5 LOPD en su segundo párrafo, también excepciona del deber de información al interesado en el plazo de tres meses, cuando los datos no hayan sido recabados del interesado, el supuesto que la información al interesado resulte imposible o exija esfuerzos

[92] Informe AEPD "Cesión de datos para la realización de un estudio sociológico" 2002
https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2002-0000_Cesi-oo-n-de-datos-para-la-realizaci-oo-n-de-un-estudio-sociol-oo-gico.pdf

desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. En relación al gran número de interesados, un Informe de la AEPD del año 2002[93] precisa cuestiones en relación al procedimiento a seguir en relación a la aplicación de esta excepción.

En primer lugar, el procedimiento deberá ser iniciado a petición del interesado, por lo que no será necesaria la adopción de un acuerdo de iniciación de oficio. No obstante, la apreciación de la excepción sólo será posible a través de un acto administrativo de la Agencia que decida sobre la procedencia o no de la excepción alegada. Dicho acto administrativo implicará la tramitación del correspondiente procedimiento administrativo, con todas las garantías establecidas en la Ley 30/1992 de 26 de Noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo, Común, sometiéndose por tanto a las reglas generales que rigen el procedimiento administrativo, dada su aplicación supletoria en virtud del artículo 35.2 de la LOPD[94]. El solicitante deberá acreditar la desproporcionalidad del esfuerzo que conllevaría la realización de la notificación. El propio artículo 5.5 LOPD aporta los criterios que deberá tener en cuenta la Agencia para valorar la procedencia o no de la aplicación de la excepción; dichos criterios son la antigüedad de los datos, el número de afectados así como las medidas compensatorias que se adopten por el Responsable del Tratamiento. La AEPD concreta que en la fase probatoria del procedimiento, será necesario

---

[93] Informe AEPD "Procedimiento para la exención del deber de informar (artículo 5.4 LOPD) Año 2002
http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/deber_informacion/common/pdfs/2002-0000_Procedimiento-para-la-exenci-oo-n-del-deber-de-informar.pdf

[94] Artículo 35.2 LOPD "En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado".

que se cuantifique realmente el coste que conllevaría realizar la notificación a los afectados, así como las medidas compensatorias que en su caso se adoptarán. Según el Informe de la AEPD, la Agencia se limitará a determinar en cada caso si, la realización de la notificación a los interesados implica un esfuerzo desproporcionado, por lo que la actuación de la Agencia se limitará a establecer si procede la aplicación de la excepción o no al concreto supuesto, no entrando a resolver sobre las medidas compensatorias propuestas, sino sobre su suficiencia o no. No obstante lo anterior, la propia AEPD parece contradecirse cuando tras afirmar que la Agencia únicamente se pronunciará sobre la suficiencia o no de las medidas compensatorias propuestas, establece que, en caso de no estimarlas suficientes, en la Propuesta de resolución la Agencia "podrá señalar cuál es su criterio para delimitar las medidas compensatorias que, en su caso, pudieran ser suficientes para estimar la solicitud planteada, a fin de que el interesado pudiera, en el trámite de audiencia concedido por el artículo 84 de la Ley 30/1992 aclarar, si lo estima necesario, las medidas compensatorias propuestas o si procede proponer nuevas medidas".

Con posterioridad a la emisión de dicho Informe, dicho procedimiento aparece regulado en el RD 1720/2007 (artículos 153 a 156). El procedimiento sigue la línea del Informe mencionado, y añade que en el escrito de solicitud del interesado, además de identificar claramente el tratamiento al que pretende aplicarse la exención, motivar las causas en que fundamenta la imposibilidad o esfuerzo desproporcionado del cumplimiento del deber de informar y las medidas compensatorias propuestas, deberá aportar una cláusula informativa que, mediante su difusión, en los términos que se indique en la solicitud, permita compensar la exención del deber de informar.

En relación al hecho que comentábamos anteriormente sobre que la Agencia únicamente se pronunciaría sobre la suficiencia o no de las medidas propuestas, el Reglamento concreta que, en caso de considerarlas insuficientes, la Agencia "podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud", tanto durante el procedimiento como en la resolución

que ponga fin al mismo. El procedimiento tendrá una duración máxima de seis meses, finalizado el cual sin resolución expresa, el solicitante podrá considerar estimada su solicitud por silencio administrativo positivo.

1.2.2.4.3 Principio de Consentimiento

El Principio del consentimiento tiene una importancia capital en la normativa de protección de datos, ya que permite al interesado ejercer el control sobre sus datos (autodeterminación informativa), pero no es menos cierto que para poder hablar de consentimiento, es requisito *sine qua non* que se haya cumplido correctamente con los principios de calidad, información y finalidad, pues en caso contrario, éste podría considerarse nulo, o como mínimo, viciado. Así, en la mentada STC 292/2000 el TC afirma que "(…) De suerte que sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) **quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales**, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia". Y la Sentencia de la AN de 9 de Octubre de 2007[95], "La exigencia de esta información en la recogida de datos que reconoce el Art. 5 LOPD constituye un derecho del afectado que es objeto de protección por sí mismo, aunque también es, lógicamente, un complemento previo de la prestación del interesado sea informado previamente, **su omisión puede determinar un vicio del consentimiento**. El derecho a la información constituye el pilar necesario para el ejercicio de otros derechos que la Ley reconoce".
Realizada esta precisión, es claro que el consentimiento es el instrumento que permite al interesado ejercer el control sobre sus

[95] SAN 4625/2007, Rec num 213/2006, FJ 5º.

datos personales, el cual constituye precisamente el contenido básico del derecho a la protección de datos, tal y como se mencionó en apartados anteriores y así ha quedado definido por la STC 292/2000, (FJ 6º), cuando afirma "Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (…), el derecho a la protección de datos atribuye a su titular un **haz de facultades** consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un **poder de control sobre sus datos personales**, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el **poder de disposición sobre los datos personales".**

Llama la atención que el Convenio 108 no lo establezca expresamente, aunque implícitamente se infiere la necesidad del mismo. Es la Directiva 95/46 la que define y exige el consentimiento del interesado, como presupuesto necesario para el tratamiento de datos. Así, define el consentimiento (art 2 h) como "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan". Y en su artículo 7 establece que "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma **inequívoca** (…)".

La LOPD establece el Principio del consentimiento del interesado en su artículo 6, al igual que la antigua LORTAD. Fruto de la

trasposición de la Directiva, se incorpora a la LOPD el adjetivo "inequívoco". Asímismo, se añade un nuevo párrafo (el cuarto), relativo al derecho de oposición del interesado en los casos exceptuados de la obtención del previo consentimiento. El artículo 6 de la LOPD establece:

1. El tratamiento de los datos de carácter personal requerirá el **consentimiento inequívoco** del afectado, salvo que la ley disponga otra cosa.
2. **No será preciso el consentimiento** cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado.

1.2.2.4.3.1 Características del consentimiento: inequívoco e informado

La LOPD define el consentimiento en su artículo 3 h) como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". Tal y como se ha comentado anteriormente, el adjetivo "inequívoco" proviene de la trasposición del artículo 7 de la Directiva 95/46. La LORTAD en su artículo 3 donde ofrece una serie de definiciones, no incluye la relativa al consentimiento, y en su artículo 6 donde regula el Principio del consentimiento, no incluye dicho término. El término "inequívoco" no equivale a expreso o cualquier otra forma en la que deba prestarse el consentimiento.

La SAN de 27 de Abril de 2006[96] afirmaba la importancia de la introducción de dicho término (FJ 4º) "Uno de los pilares básicos de la normativa reguladora del tratamiento automatizado de datos es como ya hemos señalado el principio del consentimiento o autodeterminación, principio cuya garantía estriba en que el afectado preste su consentimiento consciente e informado para que la recogida de datos sea lícita y que se plasmaba ya en el artículo 6.1 de la LORTAD de 1992, a cuyo tenor el "tratamiento automatizado de datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa" precepto reproducido en el nuevo artículo 6.1 de la Ley Orgánica 15/99, **que para resaltar la importancia del consentimiento del afectado, califica la prestación del consentimiento añadiendo la expresión "inequívoco".**

La propia AEPD concreta en un Informe del año 2000[97], los caracteres del consentimiento definido por la LOPD. Para ello, parte de la definición de consentimiento establecida por la propia LOPD, requiriendo por tanto la concurrencia de cuatro características para considerar válidamente prestado el consentimiento: libre, específico,

---

[96] SAN de 27 de Abril de 2006, Sala de lo Contencioso Administrativo, Sección Primera, FJ 4º.

[97] "Caracteres del consentimiento definido por la LOPD" disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Caracteres-del-consentimiento-definido-por-la-LOPD.pdf

informado e inequívoco. En relación al requisito de inequívoco, afirma que "implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto) siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento". Afirmación de la que claramente se deduce que no admite el consentimiento presunto como válido, en materia de protección de datos. No obstante, el mismo informe sí considera válido, y por tanto, inequívoco, el consentimiento tácito. Así afirma "el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la LOPD) si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo". Por tanto, a pesar de que la existencia del consentimiento presunto no puede ser ignorada en Derecho Español, por ser una de las formas en que éste puede manifestarse, además de haber sido admitido por la propia AEPD con anterioridad a la emisión del citado Informe, podemos concluir que a partir del mismo (año 2000) el consentimiento presunto a criterio de la AEPD no es inequívoco, y por tanto, en materia de protección de datos no es válido. No hay una opinión unívoca al respecto en la Doctrina y la propia AEPD, incluso con posterioridad a su propio informe del año 2000, llega a admitir la validez de la prestación del consentimiento implícito o presunto[98].

En nuestra opinión, si tomamos en cuenta los conceptos de consentimiento tácito y presunto, siendo el primero el que se entiende prestado a partir de la inactividad del interesado (bien por silencio o

[98] Ver Resolución de archivo de la AEPD en el Expediente No E/01225/2009, disponible en https://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2009/common/pdfs/E-01225-2009_Resolucion-de-fecha-09-12-2009_Art-ii-culo-6.1-y-11-LOPD.pdf tal y como muy acertadamente pone de manifiesto GONZÁLEZ CALLEJA, D., en http://descargalegal.blogs.lexnova.es/2011/12/05/el-consentimiento-presunto-no-es-valido-en-proteccion-de-datos-excepto-para-ccoo/

bien por falta de oposición) siendo éste perfectamente conocedor de las consecuencias y por tanto, efectos jurídicos derivados de su silencia o inactividad, y el segundo, permite deducir la voluntad del sujeto a partir de su actuación, no vemos ningún obstáculo a que el consentimiento presunto puede llegar a ser inequívoco, y por tanto, perfectamente válido en materia de protección de datos. A mayor abundamiento, y siguiendo el argumento dado por la AEPD según el cual es necesario "que exista expresamente una acción u omisión que implique la existencia del consentimiento", no entendemos por qué el consentimiento presunto, basado precisamente en actos (acciones) del interesado, no resulta, o no puede resultar, en ningún caso "inequívoco" para la AEPD, a diferencia del tácito, que sí puede ser considerado válido y por tanto, inequívoco. En este sentido, APARICIO SALOM afirma que "El consentimiento tácito es una forma más del consentimiento presunto o implícito, que se diferencia por el hecho de que la deducción del contenido de la voluntad no se obtiene de actos del interesado, sino de su falta de actuación, de su silencio"[99]. Entendemos que no se trata de excluir unas u otras formas de prestación del consentimiento, sino que con independencia de las mismas, siempre se trate de un consentimiento inequívoco, tal y como exige la propia LOPD. Precisamente por ello, la propia AEPD afirma[100] que para que el consentimiento tácito pueda ser considerado inequívoco, (por lo que *a sensu contrario,* habrá consentimientos tácitos que no serán considerados inequívocos), "será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo, no existiendo al propio tiempo duda alguna de que el interesado ha tenido conocimiento de la existencia del tratamiento y de la existencia de ese plazo para evitar que se proceda al mismo".

---

[99] APARICIO SALOM, J., Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, Pamplona, 2000, p. 59.

[100] En su propia página web https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/tratamiento_cesion/tratamiento/index-ides-idphp.php

En el mismo sentido, la SAN 2632/2000, de 14 de abril, afirma (FD 6º): "Tampoco puede admitirse, como razona el Abogado del Estado, la existencia de un consentimiento tácito o un impropiamente llamado "silencio positivo" del afectado para admitir la cesión de sus datos, pues tal forma de obtener el consentimiento requeriría, en la mejor de las hipótesis, una rigurosa constancia documental de que la entidad cedente había informado y conservaba el escrito, con constancia de la recepción por el interesado, en el que tales extremos quedaban claramente expuestos".

En relación al consentimiento tácito, APARICIO SALOM afirma[101] que "conforme se deduce de la doctrina (jurisprudencial) citada, sólo puede aceptarse el silencio como forma de otorgamiento del consentimiento cuando así lo dispone una norma jurídica, cuando existe una costumbre a tal efecto, o cuando se establece así en un contrato aceptado por las partes". Así, este autor afirma que la LOPD regula, sin mencionarlo de forma expresa, el silencio como expresión del consentimiento en diversos preceptos (artículo 6.2 inciso tercero, 11.2b) cuando se trate de datos recogidos de fuentes accesibles al público, artículo 5.4), en los que se afirma que no es preciso el consentimiento, pero exige que se informe al interesado. Concluye que "En todos estos casos, aunque la Ley afirma, o en algún caso se apoya en la idea de que no es preciso el consentimiento, en realidad está estableciendo el sistema del consentimiento tácito, ya que, al exigir que se informe al interesado respecto del tratamiento, se permite a éste que se oponga al tratamiento, de modo que, si no ejerce el derecho de cancelación u oposición, consiente tácitamente el tratamiento, y el responsable puede continuar sirviéndose de los datos".

Retomando el tema de la no aceptación del consentimiento presunto como inequívoco por la AEPD en el mencionado informe del año 2000, ¿acaso el consentimiento para la instalación de cookies no

[101] APARICIO SALOM, J., *op. cit.*, pp. 63 a 69.

podríamos considerarlo presunto? La AEPD afirma[102], con respecto al consentimiento para la instalación y utilización de cookies no exceptuadas "También podrá obtenerse (el consentimiento) **infiriéndolo de una determinada acción** realizada por el usuario, en un contexto en que a éste se le haya facilitado información clara y accesible sobre las finalidades de las cookies y de si van a ser utilizadas por el mismo editor y/o por terceros, de forma que quepa entender que el usuario acepta que se instalen cookies. En todo caso **la mera inactividad del usuario no implica la prestación del consentimiento por sí misma**". Tal y como afirma APARICIO SALOM: "deben distinguirse tres formas posibles de expresar la voluntad, expresa, presunta y tácita. La diferencia entre las dos primeras está en el hecho de que la forma presunta es meramente deductiva, se desprende del comportamiento del interesado que, si bien no es una declaración de voluntad, permite que dicha voluntad se deduzca de su comportamiento. Constituye una manifestación de la voluntad, se basa, pues, en una deducción de la voluntad implícita en los actos del interesado"[103]. Así, la SAN 866/2007, de 28 de Febrero de 2007 establece (FD 5º) "Por lo demás, los requisitos del consentimiento se agotan en la necesidad de que este sea "inequívoco", es decir, que no exista duda alguna sobre la prestación de dicho consentimiento, de manera que en esta materia el legislador, mediante el artículo 6.1 de la LO de tanta cita, acude a un criterio sustantivo, esto es, nos indica que **cualquiera que sea la forma que revista el consentimiento —expreso, presunto o tácito— éste ha de aparecer como evidente, inequívoco** —que no admite duda o equivocación—, pues éste y no otro es el significado del adjetivo utilizado para calificar al consentimiento, de manera que el establecimiento de presunciones, como la falta de denuncia de los hechos por el afectado o las demás circunstancias a las que se alude en la demanda, equivaldría a establecer un sistema de suposiciones que

[102] Página 19 de la Guía de la AEPD sobre el uso de las cookies, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

[103] APARICIO SALOM, J., *op. cit.*, p. 59.

pulverizaría esta exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser "equívoco", es decir, que su interpretación admitiría varios sentidos y, por esta vía, se desvirtuaría la naturaleza y significado que desempeña como garantía en la protección de los datos, e incumpliría la finalidad que está llamado a verificar, esto es, que el poder de disposición de los datos corresponde únicamente a su titular.

Por todo ello, entendemos que, partiendo del Principio de Libertad de forma que rige la prestación del consentimiento, éste podrá ser tanto tácito como presunto, y por supuesto expreso, siempre y cuando pueda predicarse la característica de inequívoco, lo cual podría ser un problema de prueba en algunos casos.

Por último, el art 14 del RLOPD establece expresamente la forma en que puede utilizarse el consentimiento tácito, siempre y cuando la ley no exija el consentimiento expreso. Así, se establece que el Responsable podrá solicitar el consentimiento del interesado, informándole sobre los extremos especificados en el artículo 5 LOPD y 12.2 del RLOPD (el cual establece que cuando se solicite el consentimiento para la cesión de datos deberá informarse inequívocamente de la finalidad a la que se destinarán los datos y el tipo de actividad desarrollada por el cesionario), concediéndole un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. No obstante, se concreta que el responsable del tratamiento deberá conocer si la comunicación ha sido objeto de devolución por cualquier causa, ya que en dicho supuesto, no podrá proceder al tratamiento, pues no se podrá entender prestado el consentimiento. Asimismo, se establece que el Responsable deberá facilitar al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos, citando como ejemplos los procedimientos en que tal negativa pueda efectuarse mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público del Responsable.

En cuanto al carácter **informado** del consentimiento, implica necesariamente que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce, requisito *sine qua non* para poder prestar el consentimiento.

El art 12 del RLOPD establece que:

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser **informado** de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será **nulo**.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

En relación a la literalidad del párrafo primero de este artículo, en el que se afirma que el consentimiento deberá ir referido a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, siguiendo a ZABÍA DE LA MATA, podría pensarse, partiendo de la definición de tratamiento dada por la LOPD, que el consentimiento ha de solicitarse para cada concreta operación en que consista el tratamiento. Siguiendo a este autor, cuando se habla de "un tratamiento o serie de tratamientos concretos", a lo que parece referirse es a las concretas finalidades de dichos tratamientos, las cuales han de ser consentidas, pues el contenido del deber de información viene delimitado perfectamente por el artículo 5 LOPD, "sin que sea necesario que, una vez que se ha prestado el

consentimiento, el mismo sea reiterado en cada supuesto de recogida de datos, a no ser lógicamente que concurran circunstancias nuevas en la relación jurídica[104]".

Por tanto, y como decíamos al comienzo de este epígrafe, es de capital importancia el deber de información, ya que legitimará el consentimiento que el interesado preste, pues un defecto en la información previa proporcionada, puede hacer que el consentimiento devenga nulo, tal y como se establece en el párrafo segundo del citado artículo 12 RLOPD. En cuanto al concreto contenido del deber de información, nos remitimos al epígrafe anterior en el que se aborda en profundidad el deber de información en la recogida de datos.

1.2.2.4.3.2 Excepciones al Principio del consentimiento

La SAN de 27 de abril de 2006, anteriormente mencionada, sitúa al interés general, como fundamento de las excepciones al Principio del Consentimiento, siempre que éstas sean establecidas por una norma con rango de Ley. La sentencia establece que "Se trata de una garantía fundamental legitimadora del régimen de protección establecido por la Ley, en desarrollo del artículo 18.4 de la Constitución, dada la notable incidencia que el tratamiento automatizado de datos tiene sobre el derecho a la privacidad en general y que sólo encuentra como excepciones al consentimiento del afectado, aquellos supuestos que, por lógicas razones de interés general, puedan ser establecidos por una norma de rango de ley".

El artículo 6 de la LOPD recoge los siguientes supuestos en los que podrá prescindirse del consentimiento "inequívoco" del interesado:

-que la ley disponga otra cosa:

queda fuera de toda duda que, siguiendo el Principio de reserva de Ley, como no podía ser de otra manera ante la exceptuación o restricción de un derecho fundamental, ha de ser por una ley en

---

[104] ZABÍA DE LA MATA, J., *op. cit.,* Protección de Datos. Comentarios al Reglamento, p. 174.

sentido formal y no una disposición reglamentaria, las excepciones a la prestación del consentimiento por parte del interesado.

El RLOPD por su parte concreta en su artículo 10 que será posible el tratamiento o la cesión[105] de los datos de carácter personal sin necesidad del consentimiento del interesado *cuando lo autorice una norma con rango de ley o una norma de derecho comunitario* y, en particular, cuando concurra uno de los supuestos siguientes:

"El tratamiento o la cesión tengan por objeto la satisfacción de un *interés legítimo del responsable* del tratamiento o del cesionario amparado por dichas normas, *siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados* previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas".

La AEPD en Informe de 6 de marzo de 2001[106] concretó en relación al Principio de reserva de Ley que, para que una cesión de datos pueda considerarse amparada en el artículo 11.2 a) de la Ley Orgánica 15/1999 será necesario que una norma con rango de Ley perfile el alcance y finalidad de dicha cesión, sin perjuicio de que la misma pueda, siempre dentro del marco perfilado, aclararse mediante el desarrollo reglamentario de dicha Ley. Por el contrario, no bastaría que la Ley se limitara a establecer una regla general de cesión sin aclarar su finalidad, su alcance o los destinatarios de la misma,

---

[105] Nótese que la LOPD en su artículo 6 solamente habla de "tratamiento", mientras que el artículo 10 del RLOPD distingue en sus párrafos segundo y cuarto supuestos en que cabe la *cesión* sin consentimiento, y en el párrafo tercero, los casos en que cabe el *tratamiento* sin consentimiento del interesado. No obstante dicho matiz, carece de trascendencia práctica ya que atendiendo a la definición de tratamiento dada por la propia LOPD (art 3 c) y por el RLOPD (art 5 t), las cesiones quedan englobadas dentro del concepto de tratamiento.

[106] Según se menciona en el Informe 0307/2008 disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0307_Comunicaci-oo-n-de-informaci-oo-n-para-verificar-la-calidad-del-servicio-por-parte-de-la-Inspecci-oo-n-de-Hacienda-a-la-Inspecci-oo-n-de-servicios.pdf

quedando dicha delimitación, en su totalidad, pendiente de lo que dispusiera la norma reglamentaria. Así, en el citado Informe la AEPD afirma "Respecto de la cesión o comunicación de datos, y siguiendo en este punto la referencia que la consultante efectúa de la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, rige (salvo en la cesión entre administraciones públicas para el desempeño de competencias similares) el principio de reserva de Ley, de tal modo que será necesario que, a falta de consentimiento, expreso o tácito cuando la Ley lo permita, del afectado, será necesaria la existencia de una habilitación legal que dé cobertura a la comunicación, pudiendo dicha habilitación incluso traer su causa de lo establecido en la propia Ley Orgánica 15/1999, tal y como sucede en los supuestos incluidos en los apartados b) a f) del artículo 11.2 de la misma. Esta reserva de Ley debe ser interpretada, a la luz de lo indicado en la propia Sentencia citada (FJ 11º), en el sentido de que el legislador no podrá, sin más, efectuar una delegación genérica de los límites del derecho fundamental a la protección de datos en favor de otro de los poderes del Estado (en este caso el ejecutivo, como titular de la potestad reglamentaria). De este modo, cualquier norma reglamentaria que habilite una comunicación de datos deberá traer su causa de lo establecido en una disposición con rango de Ley que delimite claramente qué puede y qué no puede permitir o autorizar esa norma reglamentaria. En consecuencia, no se consideraría suficiente una cobertura general a la cesión que previera la posibilidad de cesión "en los términos que reglamentariamente se determinen", es decir, en los supuestos en que el ejecutivo tuviese por conveniente. Del mismo modo, y aunque el supuesto excede del ámbito de la presente consulta, no sería admisible una cesión de datos entre Administraciones Públicas amparada simplemente en el cumplimiento del principio de colaboración interadministrativa, diseñado en términos genéricos por el artículo 4.1 c) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Sin embargo, sí cabría considerar respetado el principio de reserva de Ley en aquéllos supuestos en que una norma con dicho rango establezca los requisitos generales de la cesión o dé

cobertura a la misma, sin perjuicio de que dicha cesión sea posteriormente concretada, en cuanto a los aspectos procedimentales, en una norma con rango reglamentario. Como sería conforme a la doctrina del Tribunal Constitucional la concreción por una norma reglamentaria del deber específico de colaboración entre dos Administraciones Públicas para el ejercicio por una de ellas de una determinada competencia si ese deber es delimitado claramente por una norma con rango de Ley".

-cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias:
El artículo 10.3 a) del RLOPD concreta que dichas funciones han de venir atribuidas por una norma con rango de ley o una norma de derecho comunitario. Este supuesto regula los casos en que para el ejercicio de las funciones propias de la Administración, atribuidas por una Ley, sea necesaria la inclusión de sus datos en un fichero de la Administración u otras operaciones de tratamiento, en cuyo caso no será necesaria la obtención del consentimiento previo del interesado. En el supuesto de datos no facilitados por el propio interesado, la AEPD afirma[107] que "debe recordarse que es constante el criterio mantenido por esta Agencia a partir de la publicación de la Sentencia del Tribunal Constitucional 292/2000, según el cual la primera de las causas legitimadoras del tratamiento, previstas en el artículo 6.2, es decir, la vinculada a funciones propias de las Administraciones Públicas debe entroncarse con el principio de reserva de Ley consagrado por dicha Sentencia, de forma que sólo será posible encontrar cabida en dicha excepción en los supuestos en que sea la propia Ley la que atribuya las competencias que justifiquen el tratamiento". Por tanto, habrá que estar a la existencia de concretas

[107] Informe 0253/2010, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2010-0253_Tratamiento-de-datos-por-la-Administraci-oo-n-P-uu-blica.pdf

normas que habiliten dichos tratamientos sin consentimiento del interesado.
En dicho Informe, también se hace referencia al supuesto en que el interesado solicite recursos ajenos a los prestados por esa concreta Administración a la que dirige su solicitud, afirmando la AEPD que "En estos supuestos en que se recibe por el consultante una solicitud dirigida a otras entidades prestadoras de servicios sociales, debe igualmente tenerse en cuenta lo indicado respecto a la excepción al consentimiento del interesado prevista en el primer inciso del artículo 6.2 de la Ley. Cabe a este respecto señalar que la habilitación legal para dicho tratamiento se encuentra contenida en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común cuyo artículo 38 prevé lo siguiente: "*1. Los órganos administrativos llevarán un registro general en el que se hará el correspondiente asiento de todo escrito o comunicación que sea presentado o que se reciba en cualquier unidad administrativa propia. También se anotarán en el mismo, la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares.*
2.Los órganos administrativos podrán crear en las unidades administrativas correspondientes de su propia organización otros registros con el fin de facilitar la presentación de escritos y comunicaciones. Dichos registros serán auxiliares del registro general, al que comunicarán toda anotación que efectúen".
Todo ello, con independencia de la obligación de cumplir con el deber de información, informando por tanto de los extremos exigidos por el artículo 5 LOPD.

-cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento:
En muy similares términos se recoge por el artículo 10.3 b) RLOPD.
Es lógico que no se exija el consentimiento del interesado para el tratamiento de datos que implica el desarrollo de una relación contractual o precontractual aceptada previamente por el interesado.

Únicamente debe tenerse en cuenta que debe cumplirse con el deber de información establecido en el artículo 5 LOPD y que el tratamiento debe limitarse a la ejecución de dicho contrato, por lo que en caso de utilizar los datos para finalidades distintas, deberá requerirse el consentimiento del interesado. De hecho, el propio RLOPD (artículo 15) prevé el supuesto en que durante el proceso de formación de un contrato se solicita el consentimiento del afectado para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual. En este caso, el responsable del tratamiento deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos, en ese momento. Concreta el RLOPD que se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

-cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley:
El artículo 7.6 mencionado, establece que no será necesario el consentimiento cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos mencionados, continúa el artículo 7.6 LOPD, cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento. Queda fuera de toda necesidad de explicación adicional, el fundamento que justifica la no exigencia de consentimiento previo ante la necesidad de protección de un interés vital, entendido este concepto en un sentido amplio. Cierto sector

doctrinal, como ZABÍA DE LA MATA critica[108] el hecho de que se contemple esta previsión, relativa a datos especialmente protegidos, entre los supuestos del artículo 6 LOPD que se refieren a datos de nivel básico, y no se incluya en los artículos 7 y 8 LOPD, que regulan las especialidades en el tratamiento y cesión de los datos especialmente protegidos.

-cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado:
El RLOPD reproducía literalmente lo establecido por la LOPD y decimos reproducía pues el artículo 10.2b) fue derogado por la Sentencia de la Sala Tercera del Tribunal Supremo de 8 de febrero de 2012[109] por entender que el Reglamento se excedía de lo establecido por la Directiva 95/46 en su artículo 7 f), ya que en ningún momento se exigía que los datos figurasen en fuentes accesibles al público, no pudiendo los estados miembros establecer requisitos adicionales ya que podrían modificar el alcance de los principios establecidos por la Directiva en dicho artículo. No obstante, no se declaró la nulidad del precepto de la LOPD del que traía causa el artículo 10.2b) del Reglamento, ya que el Tribunal entendió que la Jurisdicción Contencioso-Administrativa no puede llegar a conocer de disposiciones con rango de ley. En cualquier caso, y teniendo en cuenta el Principio de Efecto Directo, expresamente afirmado por el

[108] ZABÍA DE LA MATA, J., *op. cit.*, p. 165.
[109] En relación a la cuestión prejudicial planteada ante el Tribunal de Justicia de la Unión Europea (sentencia de 24 de noviembre de 2011, asuntos acumulados C-468 y 469/10, disponible en http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=ES). El impacto de dicha Sentencia en el régimen establecido por la LOPD es analizado por la AEPD en su Informe 0111/2012, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2012-0111_INTER-EE-S-LEG-II-TIMO.-TRANSMISIONES-DE-MARCA-A-CONCESIONARIOS..pdf

Tribunal de Justicia en la sentencia, debe entenderse no aplicable la referencia realizada por el artículo 6.2 de la LOPD a las fuentes accesibles al público.
Por tanto, no será necesario el consentimiento del interesado para el tratamiento de datos que responda a la satisfacción de un interés legítimo del Responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos y además, que no prevalezcan los derechos y libertades fundamentales del interesado. Se trata de dos requisitos cumulativos, por lo que además de analizar qué se entiende por "interés legítimo", deberá realizarse un análisis de los derechos y libertades de los interesados, para ponderar si el tratamiento de datos ha de primar sobre éstos o no. Queda claro que estamos ante un supuesto de excepción del consentimiento previo que requiere valorar las circunstancias concretas de cada caso, además de realizar un análisis de conceptos jurídicos indeterminados como ("interés legítimo") y una ponderación de los intereses puestos en juego por cada parte.

1.2.2.4.3.3 Revocación del consentimiento

El consentimiento, como manifestación de la voluntad, ha de ser esencialmente revocable. Así, el artículo 6.3 de la LOPD establece que "el consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos". La revocación del consentimiento se refiere a aquellos casos en que el interesado lo haya prestado previamente y no a aquellos tratamientos en que el consentimiento no era necesario por encontrarse en cualquiera de los supuestos exceptuados analizados en el epígrafe anterior. No obstante, debe matizarse que se exige "justa causa", por lo que, a pesar de que interpretemos ampliamente este concepto, no se establece una revocación en principio libre, sin necesidad de justificación alguna.
El artículo 17 del RLOPD, dedicado íntegramente a la revocación del consentimiento, no alude en ningún momento a la necesidad de alegar

justa causa a la hora de revocar el consentimiento. Es por ello que en este punto coincidimos con ZABÍA DE LA MATA, que estima que el artículo 6.3 LOPD induce a confusión entre el concepto de revocación, para el que no es necesario alegar causa alguna, y el de oposición, en el que en los casos en que el consentimiento no es preceptivo para el tratamiento, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho (Art 35.1 RLOPD). No obstante, cabe alegar en contra de dicha supuesta confusión que precisamente en el párrafo siguiente (art 6.4 LOPD) se regula el derecho de oposición, estableciendo que "En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado". Además, carece de sentido que quien voluntariamente consintió un determinado tratamiento, deba alegar "justa causa" para revocar el consentimiento que libremente prestó en su momento.

El procedimiento establecido en el artículo 17 del Reglamento, no tiene las formalidades propias de un ejercicio de derecho de acceso, rectificación, cancelación u oposición. Así, el procedimiento de revocación deberá realizare a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. El único plazo temporal establecido por el artículo, es el de 10 días (a contar desde el de la recepción de la revocación del consentimiento) para que el responsable cese en el tratamiento de los datos, sin necesidad de que el responsable conceda o no la petición de revocación, ni deba notificar su realización al interesado, salvo que éste hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, en cuyo caso, deberá realizar dicha comunicación. Por otro lado, si los datos hubieran sido cedidos anteriormente, el Responsable deberá, en un plazo también de 10 días,

notificarlo a los cesionarios para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran.
El artículo 6.3 de la LOPD también alude a que la revocación del consentimiento no tendrá efectos retroactivos, lo cual es bastante obvio, pues si un tratamiento se realizó legítimamente con el debido consentimiento, la revocación del mismo no puede condicionar el sentido de los tratamientos pasados realizados. Existe también la posibilidad de que el interesado ejercite el derecho de cancelación.

1.2.2.4.3.4. Datos especialmente protegidos

Los datos especialmente protegidos o datos sensibles, como su propio nombre indica, son aquellos datos de carácter personal *que revelen* la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual (artículo 7 LOPD) y por ello, se exigen especiales medidas de seguridad en su tratamiento, además de un consentimiento reforzado para poder recabarlos. El artículo 7 de la LOPD comienza recordando que de acuerdo con lo establecido en el artículo 16.2 de la Constitución Española, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias, y si se procediera a recabar el consentimiento para su tratamiento, deberá advertirse al interesado acerca de su derecho a no prestarlo. El consentimiento para el tratamiento de estos datos ha de ser expreso y en el caso de los datos personales que revelen la ideología, afiliación sindical[110], religión y creencias, el consentimiento, además de expreso, ha de constar por escrito. Para el resto de datos especialmente protegidos, es decir, los que hagan referencia al origen racial, a la salud y a la vida sexual, se

[110] Nótese que los datos relativos a afiliación sindical no se mencionan en el párrafo primero del artículo 7 LOPD, quizá porque no se incluyen en el artículo 16.2 de la CE, pero está claro que su tratamiento es el de los datos relativos a la ideología, religión o creencias. La categoría de datos relativos a la afiliación sindical, fue introducida por primera vez por la LOPD, en congruencia con lo establecido en la Directiva 95/46, pero ello no quiere decir que no se dotara a estos datos de la especial protección antes de la aprobación de la LOPD, pues se relacionaban con datos relativos a la ideología, y por tanto, merecedores de su misma protección.

exige únicamente el consentimiento expreso del interesado, mencionando también el artículo 7.3 LOPD que podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley. Para ambos grupos de datos especialmente protegidos, se establece en el párrafo 6 del artículo 7 LOPD, que podrán ser objeto de tratamiento, cuando éste resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento sin consentimiento expreso del interesado, cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Se exceptúan del requisito del consentimiento expreso y por escrito, los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. En el Informe de la AEPD 44/2004[111]se plantea la interesante cuestión de si el dato relativo a la profesión de una persona solicitado para su inclusión en los Registros Oficiales de altos cargos de entidades inscritas en el Banco de España, puede constituir un dato especialmente protegido, pues en determinados casos como por ejemplo, la profesión de sacerdote, alcalde o representante sindical puede revelar ideología o creencias.

El consultante alega que no deberían aplicarse las medidas de seguridad de nivel alto, ya que la finalidad del fichero "no es el

[111] Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2004-0044_Car-aa-cter-del-dato-de-profesi-oo-n-de-sacerdote.pdf

tratamiento de datos que revelen ideología, afiliación social, religión o creencias y que además, "el contenido del campo es decidido de forma voluntaria, libre y autónoma por el interesado, sin intervención alguna por parte del Banco de España". La AEPD concluye que, "la finalidad del tratamiento habrá de ser siempre distinta al mero conocimiento de estas circunstancias de la persona, no afectando dicha finalidad en el carácter especialmente protegido que tendrán en todo caso, y de modo absolutamente objetivo, los datos relacionados con la ideología, afiliación sindical, religión y creencias de los afectados". Conclusión muy lógica, ya que recordemos el artículo 7.4 LOPD prohíbe expresamente la creación de ficheros con la finalidad exclusiva de almacenar este tipo de datos. Con respecto al carácter voluntario del contenido del campo destinado a la profesión, la AEPD precisa muy correctamente que, en el caso de que la cumplimentación del dato de la profesión fuese libre para el interesado, su omisión no implicaría ninguna vulneración de las normas reguladoras de las competencias del Banco de España y de la obligación de comunicación de los datos de los miembros de los órganos de gobierno sometidos a su función supervisora. Pero si por el contrario, es obligatorio facilitar el dato relativo a la profesión por parte de los miembros de los órganos de gobierno, no puede considerarse que la cumplimentación del campo sea enteramente libre en cuanto a su contenido, dado que habrá de referirse estrictamente a dicha profesión, o como mínimo, a la condición por la que el interesado es miembro del correspondiente órgano de gobierno.

Por tanto, respecto a la profesión de sacerdote, la AEPD concluye que "no existiría libertad alguna para indicar otra profesión, dado que es esta y no otra la que ostenta" de modo que "no cabe ninguna duda que la condición de sacerdote del afectado revela su pertenencia a la Iglesia Católica y en consecuencia sus creencias". Con respecto a otras profesiones como alcalde, representante de los trabajadores o representante de una comunidad autónoma, la AEPD afirma que puede que no revelen de modo directo la ideología o afiliación sindical de los afectados, "si bien esta circunstancia podría resultar discutible". En cualquier caso, la AEPD concluye que deberán adoptar

las medidas de seguridad de nivel alto sobre los ficheros que contengan datos profesionales de los afectados.

Resulta muy interesante la cuestión, también mencionada en el Informe comentado, de si un dato especialmente protegido podría no considerarse tal por el hecho de que el mismo se ejerza de forma pública y notoria. Así, la AEPD menciona la doctrina sentada por el TC en su Sentencia 292/2000 y reproducida por la AN en su Sentencia de 28 de Septiembre de 2001, en la que el TC recuerda que la protección de este derecho fundamental a la protección de datos "alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de los datos (…) el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de una persona". No obstante la conclusión anterior, la AEPD en un Informe posterior (0293/2013[112]), donde se plantea si resulta conforme a la LOPD la publicación por parte de una Cofradía, en la revista anual dirigida a los hermanos o en su web/blog, de un listado con los nombres y antigüedad de sus miembros de pleno derecho, con la finalidad de que puedan confirmar su estado en activo dentro de la hermandad, llega a otra conclusión. Se señala también que los miembros de la junta de gobierno participan en programas de radio, prensa etc siendo común mencionar el nombre, cargo, antigüedad de los hermanos, por distintas causas. La AEPD afirma que, como datos relativos a la condición de miembros de una Hermandad, se trata de datos especialmente protegidos y por tanto, su tratamiento y cesión queda sometido a lo establecido en el artículo 7.2 LOPD, es decir, consentimiento expreso y por escrito. No obstante, y tras afirmar que no cabría la obtención de un consentimiento tácito para la cesión de

[112] Informe 0293/2013 disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2013-0293_Publicaci-oo-n-de-listado-de-cofrades.pdf

datos, la AEPD analiza si cuando se trate de datos que el interesado haya hecho manifiestamente públicos podría prescindirse del consentimiento expreso y por escrito, tal y como señala el artículo 8.2e)[113] de la Directiva 95/46. Para ello, reproduce los argumentos deducidos en informe emitido relativo al Proyecto de Real Decreto por el que se regula el Reglamento del Registro de Entidades Religiosas, en el que se cita la doctrina del TC (Sentencia 85/2003, de 8 de mayo), que se considera que la utilización de los datos relacionados con la condición de candidatos en comicios electorales y su tratamiento posterior, no vulnera su derecho a la protección de datos de carácter personal, porque "la adscripción política de un candidato es y debe ser un dato público en una sociedad democrática y por ello no puede reclamarse sobre él ningún poder de disposición". Así, la AEPD afirma que "de lo citado en el artículo 8.2d) de la Directiva y en la doctrina del TC parece deducirse que la limitación establecida por el artículo 7.2 de la Ley Orgánica 15/1999 no puede entenderse como absoluta, sino que deberá quedar modulada por la garantía de otros derechos fundamentales, tomando en particular en consideración el hecho de que la vinculación del interesado con el dato esencialmente protegido es públicamente conocida". La AEPD concluye para el supuesto objeto de consulta que "cabe entender, siempre que así se justifique, que es manifiestamente pública la condición de hermano de aquéllos miembros de la junta de gobierno de la Hermandad que, en calidad de tales, participan en programas de radio o entrevistas con la prensa".

En nuestra opinión, no se da una respuesta completa al supuesto objeto de la consulta, pues únicamente se llega a la conclusión de que se considerará que la condición de hermano de aquéllos que participan

[113] El artículo 8.2 e) de la Directiva 95/46 establece que "1. Los Estados miembros **prohibirán** el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. 2. Lo dispuesto en el apartado 1 no se aplicará cuando: e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

en eventos públicos en calidad de tales, se podrá considerar manifiestamente pública. Nada se dice acerca de la publicación de los datos en internet, que entendemos supone una cesión de datos que requeriría consentimiento del interesado, expreso y por escrito por tratarse de datos especialmente protegidos. Pero además, los argumentos utilizados no parecen justificar la excepción a un supuesto en que, además, debe realizarse una interpretación restrictiva, porque en el caso objeto de consulta, no se trata de un candidato a comicios electorales, sino de miembros de la junta de gobierno de una Hermandad a la que voluntariamente pertenecen y que ningún interés tiene para el resto de personas, a diferencia de lo que podría ocurrir en el caso de candidatos electorales. Pero además, la Directiva lo que establece en el artículo 8.2, son las excepciones a la prohibición de tratamiento de datos, es decir, en el caso de datos que el interesado haya hecho manifiestamente públicos, podrá realizarse su tratamiento, pero obviamente, con las exigencias establecidas para ello, en este caso por la LOPD. Es decir, no se configura una excepción a los requisitos para el tratamiento de datos especialmente protegidos, sino que se permite su tratamiento.

Por todo ello entendemos que el criterio sentado en este Informe carece de fundamento jurídico suficiente, sobretodo teniendo en cuenta que estamos ante datos sensibles que requieren una interpretación restrictiva en lo que a las posibles excepciones en los requisitos para su tratamiento y cesión se refiere. En el Informe 0205/2013[114] se ahonda en estos argumentos, al analizar el tratamiento sin consentimiento de los datos referidos a los cargos electos de los miembros de las corporaciones locales, con indicación de su grupo político de pertenencia, existentes en un determinado ámbito territorial. Así, cita otros Informes previos en los que se sigue el mencionado criterio, como el Informe de 4 de agosto de 2009, en el que se vierten los siguientes argumentos: "(…) el régimen establecido

[114] Informe 0205/2013 disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2013-0205_Publicaci-oo-n-de-datos-de-concejales-electos.pdf

en el artículo 7.2 parece traer su causa directa de lo dispuesto en el artículo 7.1 de la propia Ley Orgánica que establece que "De acuerdo con lo establecido e el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias". Después cita los párrafos 1 y 2 del artículo 8 de la Directiva 95/46, y afirma que "como puede comprobarse el artículo 8.2 de la Directiva establece un principio claro, preciso e incondicional referido a la posibilidad de tratamiento de los datos en caso de que así se consienta por el derecho interno o, sin ningún tipo de consideración adicional, respecto de los datos que el interesado hubiera hecho manifiestamente púbicos. Esta excepción contenida en el artículo 8.2 e) de la Directiva aparece vinculada a lo dispuesto en el artículo 7.1 de la LOPD en el sentido de que el carácter de especialmente protegido del dato y la exigencia de un consentimiento reforzado, expreso y por escrito del afectado guarda relación directa con el derecho a la libertad ideológica consagrado en el artículo 16.1 de la CE. De este modo, los datos referidos a la ideología del afectado deberán quedar restringidos en su tratamiento a menos que el propio interesado levante esta restricción, renunciando a su derecho a no declarar acerca de su ideología política, pudiendo esta circunstancia derivarse de una manifestación explícita del consentimiento, referido a un determinado responsable que vaya a proceder al tratamiento y cesión de los datos de carácter personal, o a una manifestación pública del interesado, dirigido a una pluralidad indeterminada de destinatarios pero en ningún caso limitada a un ámbito concreto, en que aquél pone de manifiesto al común los datos referentes a su ideología política". Así, la AEPD concluye que la limitación establecida en el artículo 7.2 de la LOPD ha de ser interpretada congruentemente con el derecho consagrado en el artículo 16.1 de la CE y con el artículo 8.2 e) de la Directiva 95/46 la cual tiene efecto directo, y establece una excepción incondicionada de la regla general de limitación del tratamiento establecida en el artículo 8.1.

Por tanto, respondiendo a la consulta planteada, la AEPD sostiene que quien se presenta como candidato en unas elecciones generales, "pone de manifiesto con absoluta publicidad su adscripción política, que

pasa a convertirse en un dato hecho manifiestamente público", por lo que el tratamiento y divulgación del dato de ideología (grupo parlamentario de pertenencia) se encuentra legitimado por la normativa de protección de datos por haberse hecho manifiestamente público por el propio interesado al concurrir a las elecciones y posteriormente, en su condición de electo.

Con respecto a las medidas de seguridad aplicables, en el propio Informe 0205/2013, la AEPD concluye que podrán aplicarse las medidas de seguridad de nivel básico, a pesar de tratarse de un dato especialmente protegido. El argumento sostenido por la AEPD para llegar a tal conclusión, a pesar de la literalidad del artículo 81.3 del RLOPD que establece que deberán aplicarse las medidas de seguridad de nivel alto a los ficheros o tratamientos que se refieran a datos de ideología, se basa en una interpretación teleológica de las normas de protección de datos apoyándose en el artículo 3.1 del Código Civil, la cual "parece conducir a la implantación en los ficheros que contengan datos que revelen la ideología de quienes ocupan un cargo de representación política de las medidas de seguridad de nivel básico".

En el párrafo cuarto del artículo 7 LOPD se establece la prohibición sin contemplar ninguna excepción, de la creación de ficheros con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. Lógicamente esta prohibición no abarca a los datos de salud, ya que por razones obvias y legítimas, éstos pueden resultar imprescindibles para la prevención de enfermedades por ejemplo. En el párrafo quinto se establece que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Cabe citar el Informe de la AEPD 0267/2011[115] en el que se resuelve la consulta sobre si el Tablón e Edictos de la Seguridad Social y otros

[115] Informe de la AEPD 0267/2011 disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conce

Tablones Electrónicos de anuncios similares, tienen el carácter de fuente accesible al público y por tanto, puede realizarse un tratamiento de los datos en ellos publicados. La AEPD puntualiza que para poder realizar un tratamiento se necesitará el consentimiento inequívoco del interesado en los términos del artículo 6 LOPD. En relación a si podría ser de aplicación alguno de los supuestos del artículo 6.2 LOPD que exceptúan del requisito del consentimiento, la AEPD matiza que la naturaleza de la información publicada es referida a la comisión de infracciones administrativas en materia de tráfico, circulación de vehículos de motor y seguridad vial, disponiendo el artículo 7.5 de la Ley Orgánica 15/1999 que "los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras" y que precisamente por este motivo, la Orden INT 3022/2010 (artículo 4) establece que "la conservación y almacenamiento de la información obtenida como consecuencia de la consulta del Tablón Edictal de Sanciones de Tráfico, únicamente le estará permitida al propio interesado, a la persona a la que éste hubiera autorizado y a las Administraciones Públicas que por Ley lo tengan autorizado, resultando en los restantes casos contraria a lo dispuesto en el artículo 7.5RCL 1999\3058 de la Ley Orgánica 15/1999, de 13 de diciembre".

En dicho Informe se cita la sentencia de la Audiencia Nacional de 6 de octubre de 2010[116] que analiza el supuesto en que una empresa mantenía un fichero, denominado "potenciales clientes", con el contenido de los edictos publicados en los distintos boletines oficiales en materia sancionadora de tráfico y seguridad vial, considerando dicha conducta contraria a lo dispuesto en la Ley Orgánica 15/1999. Así, la sentencia afirma que "(...) no es posible y está prohibida la

---

ptos/common/pdfs/2011-0267_R-ee-plica-de-tablones-edictales-electr-oo-nicos-contraria-al-art-ii-culo-7.5-LOPD..pdf

[116] SAN 4531/2010, FD 4º, disponible en http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=5764038&links=&optimize=20101104&publicinterface=true

creación de ficheros como el que aquí nos ocupa, relacionados con infracciones administrativas de tráfico, por entidades distintas de la Administración Pública competente. Téngase en cuenta, que en el sitio web desde el que se accede a los datos recogidos en el fichero "Potenciales Clientes" se invita a realizar una "búsqueda entre más de 2,5 millones de multas" o lo que es igual de sanciones impuestas por la comisión de otras tantas infracciones administrativas, por lo que el tratamiento de los mencionados datos personales recogidos en el citado fichero y a los que se accede por cualquier persona a través del sitio web www.autoplus.es utilizando los criterios de búsqueda más arriba expuestos es un tratamiento que vulnera el citado artículo 7.5 LOPD. A lo anterior no obsta que dichos datos procedan o hayan sido recogidos de boletines oficiales que tienen la consideración de fuentes accesibles al público, según el artículo 3 j) de la LOPD. En efecto, si bien el artículo 6.2 de la LOPD excepciona de la necesidad de recabar el consentimiento del afectado para el tratamiento de sus datos, cuando procedan de fuentes accesibles al público, dicha excepción no entra en juego en supuestos como el presente, a la vista de la regla específica del artículo 7.5 LOPD para ese tipo de datos, por lo que el origen público del dato resulta irrelevante en casos como el de autos en que una entidad privada se dedica a recopilar infracciones administrativas en un fichero (más de 2,5 millones de multas de tráfico) y tratar los datos personales de las mismas, lo que sólo puede llevarse a cabo por las Administraciones Públicas cuando esté previsto en su normativa reguladora".

En cuanto a otro tipo de tablones edictales y excluyendo el supuesto de que se traten datos relativos a infracciones administrativas o penales, la AEPD concluye que no cabe entender que los tablones edictales encajen en ninguno de los supuestos del párrafo segundo del artículo 6 de la LOPD ya que no pueden considerarse éstos fuentes accesibles al público, como los diarios o boletines oficiales, pues la finalidad de su acceso universal no es permitir el acceso indiscriminado de datos sino garantizar el acceso a los mismos de los ciudadanos destinatarios de la notificación, y además no se cuenta con

el consentimiento del interesado para la introducción de los datos en el tablón.

Especial referencia a los datos genéticos

La Declaración Internacional sobre los Datos Genéticos Humanos de la UNESCO (2003)[117], define los datos genéticos humanos como "la información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos"; por su parte, la Ley española 14/2007, de 3 de julio, de Investigación biomédica, define en su artículo 3j) "Dato genético de carácter personal", como aquella "información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científico".

Ya en el año 2000 la AEPD tuvo la oportunidad de pronunciarse respecto al tratamiento de datos genéticos, en su informe 2000/0000[118].

En primer lugar, siempre que los datos se refieran a personas identificadas o identificables (como por ejemplo las muestras obtenidas en el escenario de un crimen que *a priori* no identifican a su titular pero que fruto de un posterior cotejo con otros datos, pueden resultar identificables), el fichero se encontrará sometido a la normativa de protección de datos de carácter personal. En segundo lugar, manifiesta que en todo caso los datos genéticos son datos relacionados con la salud de las personas[119].

---

[117] artículo 2 de la Declaración Internacional sobre los Datos Genéticos Humanos, de16 de octubre de 2003, disponible en http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html

[118] Informe 2000/0000 sobre "Tratamiento de datos genéticos para la localización de personas desaparecidas o en investigación criminal" disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protegidos/common/pdfs/2000-0000_Tratamiento-de-datos-gen-ee-ticos-para-la-localizaci-oo-n-de-personas-desaparecidas-o-en-investigaci-oo-n-criminal.pdf

[119] La AEPD precisa que "prescindiendo aquí de la discusión acerca de los efectos del análisis de ADN codificante o expresivo y no codificante, debe señalarse que, si

En tercer lugar, la AEPD manifiesta que en el ámbito de los datos genéticos, resultan especialmente importantes los Principios de Calidad y Finalidad de los datos. Es por ello que no podrán conservar los datos genéticos para otros fines distintos a los que motivaron su recogida, y en palabras de la AEPD "mucho menos para elaborar perfiles genéticos de la población (la llamada codificación genética) o mantener bancos de ADN obtenidos sin consentimiento del afectado para la investigación de futuras conductas criminales" y esta conservación sólo sería posible si existiera una norma con rango de ley que así lo permitiese. Se recalca en el mencionado informe que, cualquier tratamiento que afecte a datos relacionados con la huella genética, deberá realizarse con suma precaución y cautela, respetando siempre escrupulosamente la normativa de protección de datos, evitando en la regulación de estos ficheros términos genéricos, ambiguos o imprecisos que permitan esquivar la normativa aplicable.
Posteriormente, en sede europea, el Grupo de Trabajo del Artículo 29, confeccionó el Documento de Trabajo sobre los datos genéticos (2004)[120], preocupado por las nuevas cuestiones en materia de protección de datos que los progresos tecnológicos y científicos habían motivado en el ámbito de los datos genéticos. Dicho Documento perseguía un doble fin, por un lado, identificar los ámbitos donde el tratamiento de los datos genéticos pueda resultar

---

bien es posible que del resultado del análisis de ADN no codificante no se deriven directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con su salud". En apoyo de esta conclusión se cita la Recomendación (97)5 del Comité de Ministros del Consejo de Europa relativa a la protección de datos médicos, que en la definición de "dato médico" incluye las informaciones genéticas. Además, aporta una definición de datos genéticos, "todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no".

[120] Disponible en
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp91_es.pdf

preocupante en términos de protección de los datos de carácter personal, y por otro, establecer un acuerdo común sobre las distintas cuestiones relacionadas con el tratamiento de los datos genéticos, para dotar a la materia de un enfoque uniforme. Dicho Documento de trabajo pone de manifiesto los avances existentes en la legislación americana mientras que la situación en Europa no es homogénea. Mientras en algunos Estados miembros la legislación sobre la protección de datos otorga a los datos genéticos un carácter sensible, y por tanto dotado de garantías reforzadas, en la mayoría de los Estados miembros no existe legislación específica sobre el tratamiento de datos genéticos, salvo alguna legislación relativa a los derechos de los pacientes que cuenta con determinadas disposiciones sobre el tratamiento de los datos genéticos.

El único instrumento vinculante internacional que existe actualmente es el Convenio sobre los Derechos Humanos y la Biomedicina, adoptado en Oviedo, que prohíbe toda forma de discriminación contra una persona por razón de su patrimonio genético y sólo autoriza las pruebas predictivas con fines médicos. Anteriormente la UNESCO, en la Declaración Universal sobre el Genoma Humano y los Derechos Humanos[121] de 1997 (art 7), estableció que se deberá proteger la confidencialidad de los datos genéticos asociados con una persona identificable, conservados o tratados con fines de investigación o cualquier otra finalidad. No obstante, no debe pasarse por alto su valor no vinculante.

No pretendemos ahora ahondar en la problemática de los datos genéticos, pero sí poner de manifiesto su importancia y los diversos puntos de vista existentes en cuanto a su clasificación. Queda fuera de toda discusión su carácter de datos de carácter personal, y su tratamiento como datos especialmente protegidos o sensibles, a pesar de que ni la Directiva 95/46 ni la LOPD mencionen específicamente la categoría de "datos genéticos". Así, el GT29 en su Documento sobre los datos genéticos (2004), afirma que "Considerando la extrema singularidad de los datos genéticos y su relación con la información

[121] Disponible en http://portal.unesco.org/es/ev.php-URL_ID=13177&URL_DO=DO_TOPIC&URL_SECTION=201.html

susceptible de revelar el estado de salud o el origen étnico, conviene tratarlos como datos especialmente sensibles, conforme a la definición del apartado 1 del artículo 8 de la Directiva y, en este sentido, deben ser objeto de la protección reforzada prevista por la Directiva y por las leyes nacionales de transposición". De este modo, a través de su asimilación a los datos relativos a la salud, se consigue su protección reforzada como datos especialmente protegidos. Compartimos la postura de GÓMEZ SÁNCHEZ la cual afirma[122] que "Sin duda, la asimilación de los datos genéticos al grupo de datos de salud o datos médicos persigue reconocerles un estatus de datos especialmente protegidos, lo cual resulta adecuado a efectos de su protección pero no lo es, sin embargo, a efectos de su naturaleza, pues tal ubicación elude un reconocimiento general de la naturaleza específica de los datos genéticos que reclama una protección singular en todos los casos". Como afirma esta autora, ello conlleva la paradoja de que no todos los datos genéticos reciban la misma protección, en función de la aplicación que se realice de los mismos, como es el caso de su aplicación al ámbito de la seguridad, la prevención y la persecución de delitos, en cuyo caso, se aplicará la legislación interna correspondiente. En apoyo de esta tesis, GÓMEZ SÁNCHEZ cita el artículo 2.2c) de la LOPD que excluye de su régimen a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada y el artículo 2.3 de la LOPD, el cual remite a su propia legislación y a lo dispuesto, en su caso, en la propia LOPD, los siguientes tratamientos de datos: los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; los derivados del Registro Civil y del Registro Central de penados y rebeldes; Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia. Como puntualiza GÓMEZ SÁNCHEZ, la Ley 14/2007

[122] GÓMEZ SÁNCHEZ, Y., "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *Revista Derecho y Salud*, vol. 16, número extra 1, 2008, *XVI Congreso Derecho y Salud*, p. 65.

de Investigación Biomédica no modifica la situación, ya que al delimitar su ámbito de aplicación[123] incluye a los datos genéticos como datos de salud.

1.3 Marco jurídico

En este apartado realizaremos un recorrido cronológico por los diferentes textos legales en sede internacional, que determinan la configuración actual del derecho a la protección de datos personal.

1.3.1 Internacional

En **1948** la **ONU** promulgó la **Declaración Universal de los derechos humanos** y en su artículo 12 establece **"**Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques", incardinando así a la "privacidad" como un derecho humano. La redacción del artículo 12 recuerda bastante al concepto dado por el Juez Thomas M. Cooley[124] en EE.UU., "the right to be let alone", al centrarse en la vertiente negativa del derecho a la privacidad, es decir, la protección frente a cualquier injerencia o

[123] Artículo 1.2 de la Ley 14/2007 establece "asimismo y exclusivamente dentro del ámbito sanitario, esta Ley regula la realización de análisis genéticos y el tratamiento de datos genéticos de carácter personal".

[124] Expresión utilizada por primera vez por el Juez Cooley en *A Treatise of the Law of Torts by Thomas McIntyre Cooley* (Callaghan, 1888) pero reformulada, ya que el contexto en el que se acuña dicha expresión no es exactamente el mismo en ambos casos, limitándose Cooley al ámbito de la indemnidad física, por SAMUEL D. WARREN y LOUIS D. BRANDEIS en "The Right to Privacy", *Harvard Law Review*, vol. IV, 15 de diciembre, 1890, n. 5 http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

ataque en su vida privada o reputación. El concepto americano de "privacidad" será analizado en profundidad en el siguiente capítulo. Bien es cierto que no reconoce expresamente el derecho a la protección de datos de carácter personal, pero lo verdaderamente importante es que se positiviza el derecho a la privacidad, como un derecho fundamental.

Así, corolario de la Declaración Universal de los derechos humanos promulgada por la ONU, el Consejo de Europa dos años más tarde aprobará el **Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950.** Dicho Tratado internacional fue suscrito por España el 24 de Noviembre de 1977. Así, su artículo 8 establece, bajo el epígrafe "*Derecho al respeto a la vida privada y familiar:*

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

Recordemos que para garantizar el cumplimiento por parte de los estados parte de lo establecido en el Convenio, en 1959 se crea el **Tribunal Europeo de Derechos Humanos,** con sede en Estrasburgo.

Siguiendo en sede internacional y con el objeto de reforzar el valor meramente declaratorio de la Declaración Universal de Derechos Humanos de 1948, la Asamblea General de las Naciones Unidas adopta dos Pactos el 16 de Diciembre de 1966, el **Pacto Internacional de Derechos Civiles y Políticos** y el **Pacto Internacional de Derechos Económicos, Sociales y Culturales**. Estos tres textos conforman la llamada "Carta de los derechos humanos". El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establece que *"1. Nadie será objeto de injerencias*

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

En **1967** se constituyó una Comisión Consultiva para el estudio del impacto de las tecnologías de la información sobre los derechos de las personas, que dio lugar a la **Resolución 509** de la **Asamblea del Consejo de Europa** sobre "los derechos humanos y los nuevos logros científicos y técnicos", la cual sentará las bases de lo que hoy conocemos como protección de datos personales.

Después de que en 1970 se aprobase en Alemania la primera Ley[125] específicamente sobre esta materia, en relación al tratamiento de datos realizado por organismos públicos, y el 11 de Mayo de 1973, la primera Ley de protección de datos de ámbito nacional por el parlamento sueco, el **Consejo de Europa** aprobó dos importantes Resoluciones, la *Resolución 73 (22) de 26 de Septiembre sobre la protección de la intimidad frente a los bancos electrónicos de datos en el sector privado* y la *Resolución 74 (29) de 20 de Septiembre relativa a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector público*, comenzando así un proceso en el que profundizará sobre las posibles injerencias de la informática en la vida de las personas. Así, durante las décadas posteriores el Consejo de Europa aprobará importantes resoluciones[126], plasmando su patente preocupación por la protección

[125] Ley del Land de Hesse, de 17 de Octubre de 1970.

[126] Recomendación R (80) 3 del Comité de Ministros a los Estados miembros relativa a la enseñanza, la investigación y la formación en materia de "Informática y Derecho"; Recomendación R (80) 13 del Comité de Ministros a los Estados miembros, relativa al intercambio de informaciones jurídicas en materia de protección de datos; Recomendación R (81) 1 del Comité de Ministros a los Estados miembros relativa a la reglamentación aplicable a los bancos de datos médicos automatizados; Recomendación R (81) 19 del Comité de Ministros a los Estados miembros sobre el acceso a la información en poder de las autoridades públicas; Recomendación R (81) 20 del Comité de Ministros a los Estados miembros relativa a la armonización de las legislaciones en materia de exigencia de un escrito y en materia de admisibilidad de las reproducciones de documentos y de registros

de datos personales en diferentes ámbitos y sectores. Es precisamente durante el lustro anterior a 1980 cuando los países europeos comienzan a promulgar sus leyes nacionales de protección de datos,

---

informáticos; Recomendación R (83) 3 del Comité de Ministros a los Estados miembros relativa a la protección de los usuarios de los servicios de información jurídica; Recomendación R (83) 10 del Comité de Ministros a los Estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadísticas; Recomendación R (84) 10 del Comité de Ministros a los Estados miembros sobre el registro de antecedentes penales y la rehabilitación de los condenados; Recomendación R (85) 20 del Comité de Ministros a los Estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de marketing directo; Recomendación R (86) 1 del Comité de Ministros a los Estados miembros relativa a la protección de los datos de carácter personal utilizados con fines de seguridad social; Recomendación R (87) 15 del Comité de Ministros a los Estados miembros dirigida a regular la utilización de datos de carácter personal en el sector de la policía; Recomendaciones R (89) 2 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal utilizados con fines de empleo; Recomendación R (89) 4 del Comité de Ministros a los Estados miembros sobre la recogida de datos epidemiológicos relativos a la atención sanitaria de carácter primario; Recomendación R (90) 19 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal utilizados con fines de pago y otras operaciones asimiladas; Recomendación R (91) 10 del Comité de Ministros a los Estados miembros sobre la comunicación a terceras personas de datos de carácter personal en poder de organismos públicos; Recomendación R (92) 1 del Comité de Ministros a los Estados miembros sobre la utilización de los análisis de ácido desoxirribonucleico (ADN) dentro del marco del sistema de justicia penal; Recomendación R (95) 4 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal en el ámbito de telecomunicación, especialmente en lo que se refiere a los servicios telefónicos; Recomendación R (95) 11 del Comité de Ministros a los Estados miembros relativa a la relación, tratamiento, presentación y archivo de las resoluciones judiciales en los sistemas de documentación jurídica automatizados; Recomendación R (97) 5 del Comité de Ministros a los Estados miembros relativa a la protección de datos médicos; Recomendación R (97) 18 relativa a la protección de datos personales recogidos y tratados con fines estadísticos; Recomendación R (99) 5 relativa a la protección de la intimidad en Internet; Recomendación R (02) 9 relativa a la protección de datos personales recogidos y tratados con fines relacionados con seguros; algunas disponibles en http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (INGLÉS)

proceso que sigue hasta principios de los años 90, como es el caso de España, que en 1992 promulga la LORTAD. Al mismo tiempo, la cuestión tomaba importancia en el seno de la Unión Europea. Siguiendo a GARCÍA-BERRIO HERNÁNDEZ[127], la primera vez que se consideró la cuestión de los datos personales en relación a la libre circulación de la información en el marco de la UE, fue en un Informe de 1973, al que siguieron amplios debates durante los dos años siguientes. En 1976 el Comité de Asuntos legales del Parlamento Europeo, creó un subcomité encargado de velar por cuestiones específicas en materia de protección de datos. Tal y como afirma GARCÍA-BERRIO HERNÁNDEZ [128], la Dirección General para Asuntos Tecnológicos e Industriales de la Unión constituyó un Grupo de expertos en el "Tratamiento de datos e intimidad" que decidiría esperar a la aprobación del proyecto de Convenio 108 del Consejo de Europa, para comenzar a elaborar la legislación comunitaria. Así, vemos cómo a partir de 1976 se producen diferentes actividades en torno a la protección de datos de carácter personal, tanto en el Consejo de Europa, como en sede europea, y también en la **OCDE**, la cual constituye un grupo de expertos sobre los obstáculos al movimiento transfronterizo de datos y la protección de las libertades individuales, con el objetivo de elaborar unas directrices[129], las cuales verán la luz el 23 de Septiembre de 1980 (*directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*). En el Prólogo se afirma que, dado que en ese momento se había aprobado o se iba a aprobar legislación para la protección de la intimidad en aproximadamente la mitad de los países miembros de la OCDE, y teniendo en cuenta el desarrollo del tratamiento automático de datos,

---

[127] GARCÍA-BERRIO HERNÁNDEZ, T., *Informática y libertades: la protección de datos personales y su regulación en Francia y España*, Colección Estudios de Derecho, Universidad de Murcia, 1ª ed., 2003, p. 66.

[128] Para más información sobre las resoluciones aprobadas por el Parlamento Europeo en materia de protección de datos desde 1975 a 1981 Vid. GARCÍA-BERRIO HERNÁNDEZ, T., *op. cit.*, pp. 66-68.

[129] Recomendación del Consejo relativa a las directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, disponible en http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

resulta necesario elaborar unas "Directrices que ayuden a armonizar la legislación nacional relativa a la intimidad y que, a la vez que defiendan tales derechos, impidan interrupciones en la circulación internacional de datos". En relación a su poder vinculante para los estados (partiendo de la base de que las Recomendaciones de la OCDE no son jurídicamente vinculantes), en el Prólogo se afirma que las Directrices, "representan un consenso sobre principios básicos que pueden incorporarse a la legislación nacional existente o servir de fundamento para la legislación en aquellos países que todavía no dispongan de ella", en coherencia con su artículo 6, en el que se establece que "Estas Directrices deberían considerarse como criterios mínimos susceptibles de suplementarse con medidas adicionales para la protección de la intimidad y las libertades individuales". Como afirma GARCÍA-BARRIO HERNÁNDEZ, "en principio las Directrices no son legalmente vinculantes y la mayoría de la doctrina jurídica no muestra escisiones en esta cuestión particular. Sin embargo, no se puede afirmar lo mismo de la cuestión relativa al reconocimiento del valor de las implicaciones legales que de ellas se derivan", señalando la autora que en este aspecto particular la Doctrina se encuentra dividida en sus argumentos[130].

El 11 de abril de **1985** los ministros de la OCDE adoptaron la *Declaración sobre flujos de datos transfronterizos* y en **1998**, la Conferencia de ministros de la OCDE reunida en Ottawa, aprueba la *Declaración sobre la protección de la intimidad en las redes globales.* Retomando la importante labor realizada por el Consejo de Europa, y un año después de que la OCDE aprobase las *Directrices sobre protección de la intimidad y los flujos transfronterizos de datos de carácter persona*l, en **1981** se aprueba el **CONVENIO Nº 108 DEL**

[130] GARCÍA-BERRIO HERNÁNDEZ, T., *Informática y libertades. La protección de datos personales y su regulación en Francia y España*, Colección Estudios de Derecho, Universidad de Murcia, 2003, pp. 54-55.

CONSEJO DE EUROPA, de 28 de Enero[131], para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. La importancia de este Convenio deriva, no sólo por su contenido, el cual podemos calificar como decisivo, sino por ser el primer instrumento jurídicamente vinculante a nivel internacional en materia de protección de datos. Este Convenio busca conjugar la necesidad de la libre circulación de los datos con la protección de los derechos de las personas[132] y se aplica tanto a los tratamientos de datos realizados en el sector público como en el privado. Comentábamos el carácter decisivo de su contenido, pues supone el establecimiento de una base común, sentando los principios y derechos que seguirán las diferentes legislaciones en materia de protección de datos de los Estados Miembros. Reproduciremos los principios sentados por el Convenio, dada su importante trascendencia y valor de efecto directo aun en el caso de no existir normativa interna que los desarrolle. Siguiendo a GARZÓN CLARIANA[133], "los Principios del Convenio aparecen configurados a la vez como unas bases y como unos mínimos". Como unas bases, porque tal y como se establece en el art 4, los Estados se comprometen a adoptar las medidas necesarias en su Derecho interno para que sean efectivos los principios básicos, y como unos mínimos, porque el art. 11 otorga la posibilidad de que los Estados concedan a las personas "concernidas"[134] una protección más amplia que la establecida en el Convenio. Según el mismo autor, esta

---

[131] En 2006 el Consejo de Europa estableció el 28 de Enero como Día de la Protección de Datos, en conmemoración de la fecha en que se aprobó el Convenio 108.

[132] Artículo 1 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal "El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").

[133] GARZÓN CLARIANA, G., "La protección de los datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas*, vol. 8, n. 1, enero-abril 1981, p. 18.

[134] Utilizando la terminología del Convenio para referirse al "sujeto interesado".

doble cualidad de los principios como base y como mínimos, hace que "estén lejos de constituir un Derecho uniforme sobre la materia" por lo que "la entrada en vigor del Convenio no supondrá la eliminación de las diferencias observables entre las leyes de protección de datos en vigor".[135] Quizá dicha apreciación del autor sea fruto del momento en que se escribió el artículo, pues lo que queda claro es que aspirar a que el Convenio 108 del Consejo de Estado constituyese una norma de Derecho uniforme para todos los estados miembros, dista mucho de la realidad. Lo verdaderamente valioso del Convenio es el asentamiento de las bases que regirán, a partir de entonces, la legislación venidera en materia de protección de datos, siendo además, el primer instrumento jurídicamente vinculante a nivel internacional en la materia, como comentábamos anteriormente, aun en el caso de no existir normativa interna que los desarrolle.
Los Principios enunciados por el Convenio son los siguientes:

Principio de Calidad de los datos[136]:
"a) Se obtendrán y tratarán leal y legítimamente;
b) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
c) serán exactos y si fuera necesario puestos al día;
d) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".

Principio de Finalidad[137] :
"se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades".

Principio de Seguridad[138]:

---

[135] *Op. cit.*, p. 20.
[136] Artículo 4 del Convenio 108.
[137] Artículo 4 b) del Convenio 108.
[138] Artículo 7 del Convenio 108.

"se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

Garantías del interesado[139]:
"Cualquier persona deberá poder:
a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y residencia habitual o el establecimiento principal de la autoridad controladora del fichero
b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de los datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;
d) disponer de un recurso si no se ha atendido a una petición de confirmación, o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo".

Prohibición de tratamiento de determinadas categorías de datos[140]:
"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

---

[139] Artículo 8 del Convenio 108.
[140] Artículo 6 del Convenio 108.

Asimismo, se establecen determinadas restricciones y excepciones[141] tasadas, que además, para ser legítimas, deberán haber sido previstas por la ley de la parte y ser una "medida necesaria en una sociedad democrática".

Dichas excepciones podrán darse en los siguientes supuestos:

a) para la protección de la seguridad del Estado o de la seguridad pública;
b) para la protección del propio interesado o de los derechos y libertades de otras personas;
c) para fines estadísticos o de investigación científica, siempre que no existan riesgos de atentado a la vida privada de los interesados y dicha excepción se prevea por ley.

Actualmente, todos los Estados miembros de la UE han ratificado el Convenio; incluso en 1999 se modificó el Convenio para posibilitar la adhesión de las Comunidades Europeas al mismo, reforzando, en palabras de PAVÓN PÉREZ[142], la cooperación con dicha organización internacional y contribuyendo de este modo al afianzamiento de un amplio foro internacional en materia de protección de datos personales, sobre todo, en todo lo relativo a las relaciones con terceros estados.

Posteriormente, en 2001 se aprobó un **Protocolo Adicional**[143] al Convenio, relativo a las Autoridades de control y a los flujos transfronterizos de datos personales. La finalidad principal de este

---

[141] Artículo 9 del Convenio 108.

[142] PAVÓN PÉREZ, J. A., "La protección de datos personales en el Consejo de Europa: el protocolo adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales", *Anuario de la Facultad de Derecho*, ns. 19-20, 2001-2002, p. 241.

[143] Adoptado el 23 de Mayo de 2001 por el Comité de Ministros del Consejo de Europa, disponible en http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=181&CM=2&DF=&CL=ENG (INGLÉS) y traducción al español no oficial realizada internamente por la AEPD http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.29-cp--PROTOCOLO-ADICIONAL-CONVENIO-N-1o-108.pdf

protocolo podemos decir que es cubrir el vacío que respecto a las transferencias internacionales de datos a terceros países (es decir, no parte del Convenio o no sometidos a la jurisdicción de un estado parte) existía[144]. Así, el artículo 2 del Protocolo Adicional[145] regula las transferencias de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio.

---

[144] Así, el art 12 del Convenio 108 establece: "1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.
2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.
3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las *disposiciones del párrafo 2:*
a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;
b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

[145] Art. 2 del Protocolo Adicional al Convenio 108: "1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.
2. Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte.
3. Sin embargo, cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:
a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;
b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

En relación a las autoridades de control, siguiendo a PAVÓN PÉREZ[146] en el Convenio 108, a pesar de que prevé (art 10) la imposición de "sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos" establecidos en el Convenio, no establece la obligación de cada estado de dotarse de una Autoridad de Control. Esta "deficiencia" viene a solventarse mediante el artículo 1 del Protocolo Adicional, el cual establece su existencia obligatoria, además de pretender, en palabras de PAVÓN PÉREZ [147], "como *desiderátum* un tanto ilusorio, lograr una mejor armonización de los regímenes de control en todo lo relativo a la composición, el funcionamiento y las competencias de las autoridades nacionales de control".

En 2010 el Comité de Ministros comenzó un proceso de revisión del Convenio 108. El Comité Consultivo[148] ha trabajado durante dos años remitiendo al Consejo de Ministros a finales de 2012 un documento de propuesta de reforma. Un comité *ad hoc* (CAHDATA)[149], siguiendo el mandato y plazos del Comité de Ministros, está revisando dicho documento[150].

Por su parte, la Asamblea de **Naciones Unidas** aprobó mediante Resolución 45/95 de la Asamblea General, de 14 de diciembre de **1990**, las *Directrices para la regulación de los archivos de datos*

---

[146] PAVÓN PÉREZ, J.A., *op. cit.,* pp. 242 y 243.

[147] *Op. cit.,* p. 243.

[148] El art. 18 del Convenio 108 determina la creación de un Comité Consultivo a la entrada en vigor del Convenio, formado por un representante de cada parte. En el caso de España, la AEPD es miembro del Consejo Consultivo. El art 19 establece sus funciones: "Podrá´ presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio; podrá´ presentar propuestas de enmienda del presente Convenio, con arreglo al artículo 21; formulará su opinión acerca de cualquier propuesta de enmienda al presente Convenio que se le someta, con arreglo al artículo 21, párrafo 3; podrá´, a petición de una Parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del presente Convenio".

[149] Puede seguirse la actividad del Comité ad hoc (CAHDATA) aquí http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp

[150] Para seguir la evolución del proceso de modernización del Convenio 108, puede consultarse la página web http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

personales informatizados, que establecen unas orientaciones en forma de principios, que serán las garantías mínimas que los estados deberán respetar en su legislación nacional.
Por ultimo, destacar las **Conferencias que las Autoridades de protección de datos de todo el mundo** realizan con carácter anual, en las que intercambian experiencias y analizan la evolución de la protección de datos y de las que surgen determinadas resoluciones. En la 35 conferencia celebrada en Varsovia, se adoptó la Resolución "La Protección de Datos y la Privacidad deben asegurarse mediante el Derecho Internacional", en la que constata "la todavía existente necesidad de una convención internacional vinculante sobre protección de datos que salvaguarde los derechos humanos mediante la protección de la privacidad, los datos personales y la integridad de las redes, y que mejore la transparencia en el procesamiento de datos, al tiempo que logre un balance adecuado respecto de la seguridad de los intereses económicos y la libertad de expresión" y resuelve "hacer un llamado a los gobiernos para abogar por la adopción de un protocolo adicional al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), que debería consolidar los estándares que han sido desarrollados y apoyados por la Conferencia Internacional y por las disposiciones del Comentario General No. 16 a ese Pacto, con la finalidad de conformar unos estándares de aplicación global para la protección de datos y la protección de la privacidad de conformidad con el estado de derecho".

1.3.2 Normativa comunitaria

El proceso de aprobación de la Directiva comienza en 1990 con la Comunicación[151] de la Comisión sobre protección de las personas en lo referente al tratamiento de datos personales y a la seguridad de los sistemas de información, que incluye una Propuesta de Directiva.

[151] DOCE 5 de Noviembre de 1990

Tras un largo camino[152], cinco años después finalmente se aprueba la **Directiva 95/46/CE**[153] 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.

Los tratados constitutivos de las comunidades europeas no incluían referencia alguna a los derechos fundamentales. No obstante, a través de la Jurisprudencia del Tribunal de Justicia Europeo (TJE), se interpretó que los Principios generales del Derecho Europeo incluían la protección de los derechos humanos recogidos por los Tratados de derechos humanos y en particular, el Convenio Europeo de Derechos Humanos. En esta línea, en el año 2000 se aprobó la **Carta de Derechos Fundamentales de la Unión Europea**, recogiendo en un único documento los derechos reconocidos por diferentes instrumentos como el CEDH y demás convenios internacionales del Consejo de Europa, ONU y otros organismos internacionales, así como las legislaciones nacionales y comunitarias**.** En 2009, con la entrada en vigor del Tratado de Lisboa, la Carta pasó a formar parte del denominado Derecho primario de la UE. Así, el artículo 7 de la Carta reconoce el derecho al respeto de la vida privada y familiar, del domicilio y comunicaciones de las personas y el artículo 8 reconoce específicamente el derecho a la protección de datos de carácter personal, dotándole por tanto de la protección relativa a cualquier derecho fundamental:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a

---

[152] Para profundizar en los orígenes de la Directiva 95/46, Vid. HERRÁN ORTIZ, A. I., *El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid, 2002, pp. 115-123.

[153]Disponible en http://eur-lex.europa.eu/legal content/ES/TXT/?uri=celex:31995L0046

acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente.
Retomando la **Directiva 95/46**, ésta se adoptó en un momento en que la mayoría de los estados miembros habían aprobado sus propias normas en materia de protección de datos, por lo que uno de los objetivos de la Directiva 95/46, era armonizar dichas legislaciones nacionales para eliminar los posibles obstáculos "para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario[154]".
En un momento en el que el mercado interior y la libre circulación de mercancías hacían necesario el intercambio de datos personales entre estados y éste cada vez se preveía mayor con la evolución de la tecnología, era necesaria una norma que garantizase unas bases

[154] Considerandos 7 y 8 de la Directiva 95/46:
(7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;
(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

comunes, así como el respeto a los derechos y libertades fundamentales.

Cabe destacar que en 1995 todos los estados miembros de la UE habían ratificado el Convenio 108 del Consejo de Europa, por lo que no cabe hablar de contradicciones entre ambos instrumentos jurídicos, siendo precisamente la Directiva 95/46 continuadora de los Principios asentados por dicho Convenio[155]. La Directiva 95/46, veinte años después y con independencia de la necesidad de reforma o actualización de la normativa de protección de datos, ha mostrado con creces su madurez y solidez, constituyendo una base robusta y común que ha facilitado la concepción e interpretación de la legislación posterior. De este modo, se configura como el texto europeo de referencia en materia de protección de datos. Dos años después se aprobaría la **Directiva 1997/66** *del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.* Ambas Directivas tienen un objeto y ámbito común, si bien en el caso de la Directiva 97/66, respondía a cubrir las necesidades específicas en materia de protección de datos y de la intimidad de los usuarios y abonados, creadas por el desarrollo de la Sociedad de la Información y los nuevos servicios de telecomunicación originados (Considerando 3). De este modo, se dice expresamente en el Considerando 11 que en el sector de las telecomunicaciones se aplica la Directiva 95/46/CE, para todas las cuestiones relativas a la protección de los derechos y libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva.

La Directiva 95/46 era del todo necesaria, ya que una base mínima común para todos los Estados miembros era *conditio sine qua non* para posibilitar que el previsible aumento de los flujos transfronterizos

[155] Considerando 11 de la Directiva 95/46 "Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales".

de datos se realizara pacíficamente[156]. Su objeto es garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (artículo 1). En su artículo 2 establece los **conceptos** de datos personales, tratamiento, fichero, responsable del tratamiento, tercero, destinatario, e introduce el concepto de "encargado del tratamiento".

a) "datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
b) "tratamiento de datos personales" ("tratamiento"): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

---

[156] Así lo pone de manifiesto el Considerando 8 de la Directiva 95/46: "Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones".

c) “fichero de datos personales” (“fichero”): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
d) “responsable del tratamiento”: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;
e) “encargado del tratamiento”: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;
f) “tercero”: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;
g) “destinatario”: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;
h) “consentimiento del interesado”: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

En relación al concepto de "dato personal", queda claro que se trata de una definición conscientemente muy amplia[157], casi idéntica a la definición[158] dada por el Convenio 108. En primer lugar, queda claro que se excluye a las personas jurídicas, dado que ha de ser información relativa a personas físicas. En segundo lugar, podemos hablar de datos personales siempre que la información pueda asociarse a una persona física, bien directa o indirectamente, por lo que un dato que aparentemente no hace una referencia directa a una persona, puede constituir un dato personal si podemos llegar a relacionarlo con la persona física a la que se refiere. Es por ello que no compartimos la idea muchas veces mencionada[159] de que un dato personal ha de cumplir dos condiciones, primero, que se trate de un dato personal relativo a una persona física[160], y segundo, que el dato se refiera a una persona identificada o identificable. Pensamos que lo que convierte a

---

[157] El Dictamen 4/2007 del GT29 sobre el concepto de datos personales, en su página 4 afirma "Resulta necesario señalar que esta definición refleja la intención del legislador europeo de mantener un concepto amplio de 'datos personales' a lo largo de todo el proceso legislativo. En la propuesta original de la Comisión se explicaba que "como en el Convenio 108, se adopta una definición amplia para abarcar toda información que pueda vincularse a una persona" (ver COM (90) 314 final de 13.9.1990, p. 19). La propuesta modificada de la Comisión señalaba que 'la propuesta modificada recoge el deseo del Parlamento de que la definición de "datos personales" sea tan amplia como sea posible con el fin de incluir toda información referente a una persona identificable" (ver COM (92) 422 final de 28.10.1992, p. 10), un deseo que también el Consejo tuvo en cuenta en la posición común (ver Posición Común (CE) no 1/95 adoptada por el Consejo el 20 de febrero de 1995, DO C 93 de 13.4.1995, p.25)".

[158] Artículo 2 Convenio 108 "a) 'Datos de carácter personal' significa cualquier información relativa a una persona física identificada o identificable ('persona concernida');

[159] Cfr HERRÁN ORTIZ, A. I., *op. cit.,* p. 126: "(…) para que efectivamente el tratamiento de un dato se encuentre en el ámbito de aplicación de aquélla (la Directiva) deberá reunir dos condiciones: una, que se trate de un dato personal, relativo a la persona física; y dos, que la información o el dato se refiera a una persona identificada o identificable".

[160] Información relativa a un objeto, como por ejemplo el valor de un coche, podríamos entender que no es dato personal a priori, por referirse a un objeto, pero podría llegar a ser un dato personal si lo vinculamos a una persona.

un dato en dato de carácter personal, es precisamente la posibilidad de vincularlo a una persona física, obviamente identificada o identificable, pues una información aislada, a pesar de poder constituir un dato personal (en el sentido de poder referirse a una persona física), si no podemos vincularlo de ninguna manera a una persona identificable, no podemos hablar propiamente de dato de carácter personal. O en otras palabras, si una información no puede vincularse a una persona concreta, no tiene sentido hablar de esa primera condición "que se trate de un dato de carácter personal", pues cualquier dato será personal siempre que lo podamos vincular a una persona, y en caso contrario, no podremos hablar de dato de carácter personal. En este punto, resulta de obligada lectura el Dictamen 4/2007 del GT29[161] sobre el concepto de datos personales, pues como en sus propias conclusiones indica, proporciona una serie de "orientaciones sobre cómo debe entenderse y aplicarse el concepto de datos personales de la Directiva 95/46/CE y de la legislación comunitaria adoptada en aplicación de la misma en diversas situaciones".

En relación a su **ámbito de aplicación** (artículo 3), se aplica tanto a los tratamientos automatizados (total o parcialmente) como a los no automatizados. No se aplicará a los tratamientos realizados por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. En el siguiente capítulo analizaremos la aplicación de la normativa europea de protección de datos fuera de la UE. No obstante, la Directiva también prevé reglas para clarificar cuándo procede la aplicación de la legislación nacional, en relación a tratamientos efectuados en varios estados miembros (artículo 4), pues como se afirma en el Considerando 20 el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la Directiva; y que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios

[161] Dictamen 4/2007 del GT29 sobre el concepto de datos personales, (WP136) de 20 de Junio de 2007, consultable en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la Directiva.
En relación a las **condiciones generales para la licitud del tratamiento** de datos personales, la Directiva permite a los estados establecer las condiciones en que son lícitos los tratamientos de datos personales, siempre dentro de los límites establecidos por la Directiva, que serán los que veremos a continuación:

Principios relativos a la calidad de los datos

El artículo 6 establece que los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

Principios relativos a la legitimación del tratamiento de datos

El artículo 7 establece que el tratamiento de datos personales sólo podrá efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

Como puede apreciarse, no sólo el consentimiento es el único requisito que legitima el tratamiento de datos, pues han de tenerse en cuenta los principios en relación al tratamiento, que pueden hacer que dicho tratamiento inicialmente consentido, devenga ilícito. En este sentido, cabe destacar que la LOPD establece[162] como regla general y

[162] Artículo 6 LOPD: "**1.** El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

principal requisito legitimador del tratamiento el consentimiento, si bien y como no podría ser de otra manera, establece otros supuestos a modo de excepciones en los que no será necesario el consentimiento *inequívoco* del interesado.

Otras Directivas[163] que han completado el marco de tratamiento en relación a la protección de datos personales en ámbitos específicos,

---

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

[163] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica**;** Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (derogada por la Directiva 2002/58); Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)**;** Directiva 2002/19/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso); Directiva 2002/20/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización); Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco); Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal); Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas); Directiva 2004/82/CE del Consejo de 29 de abril de 2004 sobre la

respetando las bases establecidas por la Directiva 95/46, son la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

En el marco exclusivo de las instituciones y organismos comunitarios, nos encontramos con el **Reglamento 45/2001** del Parlamento Europeo y del Consejo, de 18 de Diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. En relación a su ámbito de aplicación, el artículo 3.1 del Reglamento establece que se aplicará al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, "en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario". Tal y como señala ORTEGA ÁLVAREZ, [164] la expresión utilizada advierte de que el ámbito objetivo del Reglamento se refiere únicamente a los "datos procesados por las instituciones u organismos actuando dentro del ámbito del Tratado de la Comunidad Europea, es decir, del primer pilar o pilar comunitario.

---

obligación de los transportistas de comunicar los datos de las personas transportadas**;** Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso publico o de redes publicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (actualmente anulada por Sentencia del TJUE de 8 de Abril de 2014); Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) /2004 sobre la cooperación en materia de protección de los consumidores.

[164] ORTEGA ÁLVAREZ, L. I., y otros, *La seguridad integral europea*, Lex Nova, Valladolid, 2005, p. 18.

El tratamiento de datos que realiza Europol no está sometido al control del Supervisor Europeo".

Paquete sobre telecomunicaciones de 2002: la Directiva 2002/58

Ante la apertura en 1998 del mercado de las redes y servicios telecomunicaciones a la libre competencia, y siguiendo el compromiso adquirido por las Directivas que hicieron posible dicha liberalización de revisar su propio funcionamiento, tras la conocida como Revisión 99, en el año 2002 se aprobó un nuevo marco regulador de las comunicaciones electrónicas (*Telecom Package*) con el objetivo de encauzar y garantizar el desarrollo de una competencia efectiva, estableciendo un marco regulatorio único para todos los servicios y redes de transmisión (excluyendo la regulación de los contenidos[165]).
Dicho paquete se componía de una Directiva marco, la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, y otras cuatro Directivas específicas:
-Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización);
-Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones

[165] Considerando 5 de la Directiva 2002/21 "(…)Es necesario separar la regulación de la transmisión de la regulación de los contenidos. Por consiguiente, este marco no cubre el contenido de los servicios prestados a través de las redes de comunicaciones electrónicas utilizando servicios de comunicaciones electrónicas, tales como los contenidos de radiodifusión, los servicios financieros y determinados servicios de la sociedad de la información y, por tanto, se entiende sin perjuicio de las medidas adoptadas a nivel comunitario o nacional en relación con dichos servicios, de conformidad con lo dispuesto en el Derecho comunitario, con el fin de promover la diversidad cultural y lingüística y garantizar la defensa del pluralismo de los medios de comunicación. (…) La separación entre la regulación de la transmisión y la regulación de los contenidos no es óbice para tener en cuenta los vínculos que existen entre ambas, en particular, con el fin de garantizar el pluralismo de los medios de comunicación, la diversidad cultural y la protección de los consumidores.

electrónicas y recursos asociados, y a su interconexión (Directiva de acceso);
-Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal);
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas);
Cabría añadir otras disposiciones complementarias[166], pero cabe destacar que otro de los objetivos del mencionado paquete fue reducir el número de Directivas, simplificando el marco regulatorio aplicable.
La Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, deroga la Directiva 97/66 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, pues tal y como se establece en su Considerando (4), "debe ser adaptada al desarrollo de los mercados y de las

[166] Decisión 676/2002/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea (Decisión espectro radioeléctrico); Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas; Decisión 2003/548/CE, de 24 de julio de 2003, relativa al conjunto mínimo de líneas arrendadas con características armonizadas y las correspondientes normas a que se refiere el artículo 18 de la Directiva de servicio universal; Decisión de la Comisión de 6 de diciembre de 2007 que modifica la Decisión 2002/627/CE, por la que se establece el Grupo de entidades reguladoras europeas de las redes y los servicios de comunicaciones electrónicas; Recomendación de la Comisión de 17 de diciembre de 2007 relativa a los mercados pertinentes de productos y servicios dentro del sector de las comunicaciones electrónicas que pueden ser objeto de regulación ex ante de conformidad con la Directiva 2002/21/CE del Parlamento Europeo y del Consejo relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas; Directrices de la Comisión sobre análisis del mercado y evaluación del peso significativo en el mercado dentro del marco regulador comunitario de las redes y los servicios de comunicaciones electrónicas publicadas en el Diario Oficial n° C 165 de 11/07/2002 p. 0006-0031.

tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas disponibles al público sea el mismo, *con independencia de las tecnologías utilizadas*". Vemos aquí una manifestación del Principio de Neutralidad Tecnológica, en lo que respecta a la protección de los datos personales y de la intimidad. Esta referencia a la neutralidad de la tecnología en relación a la protección de datos y la intimidad de las personas, es el pilar básico de toda la regulación de protección de datos de carácter personal. Es decir, se aplicará la misma regulación a los servicios de comunicaciones electrónicas, con independencia de la tecnología utilizada para la prestación de los mismos. No quisiéramos pasar por alto la oportunidad de mencionar una cuestión relativa al desconocimiento de este Principio cuando se afirma la falta de regulación en el momento en que una nueva tecnología, y por tanto, una nueva forma de tratamiento de datos, sale al mercado. Sinceramente, no entendemos la razón de esta afirmación ya que de sobra es sabido que sería impensable regular al ritmo que marca la tecnología, además de ilógico, inviable e injusto[167], y lo más importante, innecesario, precisamente por la estructura de nuestro sistema jurídico. Este principio se adoptó por primera vez en el paquete sobre telecomunicaciones de 2002, y así la Directiva marco lo menciona[168] pero aplicado a la tecnología. No obstante, será en la

[167] Resulta interesante mencionar el sistema jurídico establecido en EE.UU., su Constitución no menciona la "privacidad", aunque por vía jurisprudencial se afirma que la 4ª Enmienda lo acoge. En resumen, existe un Derecho sectorial (existen leyes concretas respecto a determinadas tecnologías), no general, no uniforme (recordemos que es un Estado Federal), y por tanto, todo lo contrario a lo que el Principio de Neutralidad Tecnológica supone.

[168] Considerando 31 de la Directiva marco "(…) Es deseable que los consumidores tengan la posibilidad de recibir, independientemente del modo de transmisión, todos los servicios de televisión digital interactiva teniendo en cuenta la neutralidad tecnológica, los avances tecnológicos futuros, la necesidad de impulsar el establecimiento de la televisión digital, y la situación de la competencia en los mercados de servicios de televisión digital (…)".

Directiva 2009/140/CE[169] cuando se adopte como uno de los principios normativos de regulación de la red radioeléctrica y los servicios de comunicaciones electrónicas. Este principio, como uno de los principios básicos de la regulación de las comunicaciones electrónicas, busca la aplicación de la regulación de manera igualitaria a todo tipo de comunicaciones electrónicas, evitando así modificar la legislación en función de la tecnología utilizada, dotando de seguridad jurídica a los agentes intervinientes en el sector y redundando en beneficio de los usuarios y consumidores. En el considerando 5 de la Directiva 2002/58 se afirma que la introducción de nuevas tecnologías digitales avanzadas en las redes públicas de comunicación, crean necesidades específicas en materia de protección de datos y de la intimidad de los usuarios y que el éxito del desarrollo transfronterizo de estos servicios depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad. A su vez, el considerando 6

[169] Considerando 34 de la Directiva 2009/34: "Hay que reforzar la flexibilidad en la gestión del espectro y en el acceso al mismo, al amparo de autorizaciones neutras con respecto a la tecnología y los servicios, para que sus usuarios puedan elegir las mejores tecnologías y servicios aplicables en bandas de frecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en los planes nacionales pertinentes de atribución de frecuencias, de conformidad con el Derecho comunitario ("principios de neutralidad con respecto a la tecnología y al servicio"). La determinación administrativa de las tecnologías y servicios debe aplicarse cuando estén en juego objetivos de interés general, y ha de estar claramente justificada y ser objeto de revisiones periódicas" y el artículo 9.3 de la Directiva marco, modificada por la Directiva 2009/140, establece "(…) los Estados miembros velarán por que se pueda utilizar todo tipo de tecnología utilizada para los servicios de comunicaciones electrónicas en las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en sus respectivos planes nacionales de atribución de frecuencias, de conformidad con el Derecho comunitario" y en su párrafo cuarto, "los Estados miembros velarán por que se pueda prestar todo tipo de servicios de comunicaciones electrónicas en las bandas de radiofrecuencias declaradas disponibles para los servicios de comunicaciones electrónicas en sus respectivos planes nacionales de atribución de frecuencias, de conformidad con el Derecho comunitario".

constata la existencia de nuevos riesgos para los datos personales e intimidad de los usuarios, originados por las nuevas posibilidades que ofrecen los servicios de comunicaciones electrónicas disponibles al público a través de Internet. Queda por tanto patente que el legislador comunitario no consideraba la regulación establecida hasta el momento como "neutralmente tecnológica", pues en caso contrario esos "nuevos riesgos" no serían tales. Efectivamente, se criticaba que la Directiva 97/66 dotaba de gran protagonismo al servicio de telefonía, no teniendo en cuenta el tratamiento de datos a través de internet o los servicios prestados en línea. Esta Directiva generó un gran debate interno, ya que trae causa directa de la Propuesta de Directiva 2000/385, aprobadas en Diciembre de 2001 dentro del nuevo marco regulador en el ámbito de las comunicaciones electrónicas. Cabe destacar que la Directiva de Protección de Datos se descolgó del resto, debido a la dificultad de alcanzar acuerdos en puntos tales como el Spam, (qué papel debía jugar el consentimiento en las comunicaciones no solicitadas: *opt-in vs opt-out*) y los datos de localización. No obstante, es imprescindible tener siempre en cuenta la Directiva 95/46 sobre el tratamiento de datos personales y libre circulación de esos datos, ya que ésta actúa como norma general respecto a la Directiva 2002/58, y por tanto, plenamente aplicable en aquellas materias que esta última no regule específicamente. Así se declara en el Considerando 10 la aplicación subsidiaria de la Directiva 95/46 para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no estén cubiertas de forma específica por la Directiva 2002/58. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.

La Directiva 2002/58 introduce, entre otros, los conceptos[170] de datos de tráfico, datos de localización, comunicación y servicios de valor

[170] Artículo 2 de la Directiva 2002/58: "b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

añadido. Mientras la Directiva 95/46 habla únicamente de datos personales. La Directiva 97/66 introdujo un nuevo concepto, los datos de tráfico y facturación, pero no se mencionan los datos de localización hasta la aprobación de la Propuesta de Directiva 2000/385, que dió lugar a la Directiva 2002/58. Esto no quiere decir que los datos de localización carecieran de cobertura legal, ya que como dato personal, ya gozaban de protección. Con la aprobación de la Directiva 2002/58, es la primera vez que encontramos estos conceptos definidos por un texto legal, ya que la Directiva 97/66 ni siquiera ofrecía una definición de datos de facturación.

En relación a los **datos de tráfico**, si comparamos la redacción dada al artículo 6 por la Propuesta de Directiva, y la final adoptada por la Directiva, observamos que en la Propuesta, no se hacía alusión a la posibilidad del usuario o abonado de retirar su consentimiento para el tratamiento de los datos de tráfico, en cualquier momento. Respecto a la información que el proveedor del servicio debe proporcionar al abonado o usuario, además del tipo de datos de tráfico que son tratados y la duración del tratamiento, la Directiva incluye el hecho de que esta información debe darse antes de obtener el consentimiento. Por último, la Directiva siempre habla de "abonado o usuario", mientras que la Propuesta a veces sólo menciona al "abonado". Por

---

c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

d) "comunicación": cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;

f) "consentimiento" de un usuario o abonado: el consentimiento del interesado, con arreglo a la definición de la Directiva 95/46/CE;

g) "servicio con valor añadido": todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación;

tanto, pocos son los cambios introducidos por la Propuesta de Directiva respecto a los datos de tráfico por lo que su régimen básico continuó siendo similar al establecido por la Directiva 97/66, aunque sí podemos afirmar que con la adopción de la Directiva, se mejoró la regulación de los datos de tráfico.

Por lo que respecta a los **datos de localización**, la Propuesta de Directiva habla de "Datos sobre Localización", mientras que la Directiva 2002/58 habla de "Datos de localización distintos de los datos de tráfico". La única diferencia en la redacción que encontramos, es que la Propuesta, a pesar de que sí establece en su párrafo segundo la posibilidad de, una vez prestado el consentimiento, "seguir contando" con la posibilidad de rechazarlo, no menciona en el párrafo anterior la regla general de que "se deberá ofrecer la posibilidad de retirar en todo momento su consentimiento". Entendemos que los datos sobre posición geográfica de usuarios móviles son datos de localización y no de tráfico. Es más, al revés, los datos de localización serían de tráfico. (Art. 6) "Los datos de localización distintos de los datos de tráfico…" luego queda claro que hay datos de localización que son de tráfico. Esta opinión se refuerza de la lectura del Considerando 14 de la Directiva 2002/58, que expresamente incluye "la identificación de la célula de red en la que está localizado el equipo Terminal (…)" como dato de localización. Estos datos de localización, son considerados como datos de tráfico por la Directiva, y por tanto, se les aplica la regulación establecida para los mismos. De ahí viene la continua afirmación "los datos de localización distintos de los datos de tráfico", pero no por ello dejarán de ser datos de localización. Al principio, los servicios basados en la localización utilizados por los usuarios o abonados, se basaban precisamente en este tipo de localización "por células" y no en localización por GPS. Este es un punto muy importante, ya que la Directiva se dirige, en mayor medida, a la protección de las personas físicas, principales destinatarios de los servicios de valor añadido (VAS[171]). No obstante lo anterior, con la aprobación de la Directiva,

[171] VAS, *Value Added Services*, Servicios de Valor Añadido.

se mejoró sensiblemente la regulación establecida para los datos de tráfico, por lo que será necesario informar con carácter previo al tratamiento, del tipo de datos que son tratados y de la duración del tratamiento; además el usuario o abonado, al igual que en el régimen establecido para los datos de localización, podrá retirar en cualquier momento su consentimiento. Ya el Grupo de Trabajo del Artículo 29 era consciente de la importancia de los datos de tráfico, y menciona que "(…) la sensibilidad de los datos sobre tráfico, que permiten obtener perfiles individuales de comunicación incluyendo fuentes de información y ubicación geográfica del usuario de teléfonos fijos o móviles y a los posibles efectos perniciosos sobre la intimidad resultantes de la recopilación, difusión o uso posterior de dichos datos". En este punto, no sólo nos estamos refiriendo a esos datos de tráfico que en realidad, son datos de localización, sino también, a esos datos de tráfico derivados de la navegación por Internet que, como ya estableció el Grupo de Trabajo del Artículo 29, constituyen datos sensibles, y por ello, dignos de una protección, como mínimo, diferenciada del resto de datos de tráfico, los antiguos datos de facturación[172]. Los datos de tráfico podrán conservarse a efectos de facturación. Esta posibilidad de tratamiento de los datos de tráfico, configura una de las excepciones a la regla general de que los datos de tráfico deberán ser eliminados o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación. Cabe plantearse a este respecto, qué ocurre cuando la factura ha sido puntualmente abonada, no se va a impugnar la misma, y el período de impugnación establecido en el Estado Miembro en concreto es bastante extenso[173]. Lógicamente, a pesar de que la factura se haya pagado, siempre queda el derecho del abonado de impugnar la factura siempre que se halle dentro de plazo. No obstante lo anterior, vemos conveniente la posibilidad de que si el abonado ha satisfecho su factura y se comprometiera a no impugnarla, sus datos de tráfico

[172] Con la Directiva 97/66 desaparece la categoría de datos de facturación, que pasan a englobarse en la general de datos de tráfico.

[173] Los períodos de impugnación oscilan desde los 6 meses a los 6 años, como es el caso de Irlanda y Reino Unido.

puedan ser borrados. Esta es una solución muy coherente, para el caso de aquellos países en los que los períodos de impugnación de las facturas son muy extensos. Por otro lado, y teniendo en cuenta que los datos de tráfico que podrán ser tratados a efectos de la facturación de los abonados y pago de interconexiones serán los "necesarios", en aquellos casos en que para la facturación se almacenen datos no necesarios, como por ejemplo, los relativos a la situación del terminal del usuario, no podrán almacenarse, ni siquiera a efectos de facturación, salvo que la facturación de las llamadas se base en la ubicación geográfica.

En relación a la retención de datos sobre tráfico en el sector de las telecomunicaciones, en España, todavía cuando la LSSI era un proyecto y no existía por tanto la Directiva 2006/24/CE *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes publicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE* , se debatía la posibilidad de añadir la obligación para los prestadores de servicios de conservar los datos de tráfico durante un año por si fueran necesarios para ulteriores investigaciones policiales o judiciales. Se adujo en su momento que las operadoras de telefonía "ya lo venían haciendo" a efectos de facturación, pero son dos supuestos que consideramos, no pueden compararse.

La **Directiva 2006/24 sobre conservación de datos**[174], establecía en su artículo 1 su objeto y ámbito de aplicación, siendo el primero la armonización las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso publico o de una red publica de comunicaciones en relación con la conservación de determinados

[174] Recomendamos la lectura del artículo de VILASAU SOLANA, M., "La Directiva 2006/24/CE sobre conservación de datos del trafico en las comunicaciones electrónicas: seguridad v. Privacidad" [artículo en línea]. I*DP. Revista de Internet, Derecho y Política*. N. 3. UOC. [Fecha de consulta: 04/10/2015]. http://www.uoc.edu/idp/3/dt/esp/vilasau.pdf

datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. En relación a su ámbito de aplicación, en el segundo párrafo se define su aplicación a los datos de trafico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. Concreta también que no se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas. Tal y como se establecía en el artículo 3.1 de la Directiva, dicha obligación de conservación supone una excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE.

Como bien afirmaba, el mismo año que se aprobó dicha Directiva, VILASAU SOLANA, "La conservación de los datos del trafico interfiere con el derecho fundamental e inviolable a la confidencialidad de las comunicaciones y a la protección de datos. Mediante la Directiva 2006/24 se están socavando los principios de protección de datos sentados en la UE. En definitiva, las medidas adoptadas en la presente Directiva superan totalmente los beneficios que se puedan obtener con la misma ya que se instaura una filosofía de sospecha y vigilancia de todos los ciudadanos sin un mínimo indicio". Pero no ha sido hasta Abril de 2014 que el Tribunal de Justicia de la Unión Europea declaró[175] ilegal la Directiva. Se planteó la validez de la Directiva frente a los artículos 7, 8 y 11 de la Carta Europea de Derechos Fundamentales. El TJUE afirma (apartados 26, 27 y 29) que "ha de señalarse que los datos que deben conservar los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, con arreglo a los artículos 3 y 5 de la Directiva 2006/24, son, en particular, los datos necesarios para rastrear e identificar el origen de una comunicación y su destino, para identificar la fecha, hora y duración de una comunicación, el equipo de comunicación de los usuarios y para identificar la localización del

[175] Sentencia de 8 de Abril de 2014 en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros.

equipo de comunicación móvil, datos entre los que figuran el nombre y la dirección del abonado o usuario registrado, los números de teléfono de origen y destino y una dirección IP para los servicios de Internet. Estos datos permiten, en particular, saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que ésta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto. Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan. Así, el TJUE entiende que "la conservación de datos para su eventual acceso por las autoridades nacionales competentes, según se establece en la Directiva 2006/24, afecta de manera directa y específica a la vida privada y, por tanto, a los derechos que garantiza el artículo 7 de la Carta. Además, el artículo 8 de la Carta también es aplicable a dicha conservación de datos, puesto que constituye un tratamiento de datos de carácter personal en el sentido de ese artículo y debe, por tanto, cumplir necesariamente los requisitos de protección de datos que se derivan de dicho artículo (sentencia Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 47)".

El TJUE afirma rotundamente que la Directiva supone una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta puesto que establece un tratamiento de datos de carácter personal y que la obligación impuesta por los artículos 3 y 6 de la Directiva 2006/24 a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar durante un determinado período datos relativos a la vida privada de una persona y a sus comunicaciones, como los que se indican en el artículo 5 de dicha Directiva, constituye en sí misma una injerencia en

los derechos garantizados por el artículo 7 de la Carta. A su vez, el acceso de las autoridades nacionales competentes a los datos constituye una injerencia adicional en ese derecho fundamental. Además, el Tribunal recalca que la Directiva no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido. En especial, el acceso a los datos conservados por las autoridades nacionales competentes no se supedita a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido y se produzca a raíz de una solicitud motivada de dichas autoridades presentada en el marco de procedimientos de prevención, detección o enjuiciamiento de delitos. Tampoco se ha establecido una obligación concreta de los Estados miembros de que se fijen tales limitaciones.

Por todo ello, el TJUE considera que la injerencia que supone la Directiva 2006/24 en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta resulta de gran magnitud y debe considerarse especialmente grave.

En este punto resulta muy interesante traer a colación el Dictamen 5/2002[176] sobre la Declaración de los Comisarios Europeos responsables de protección de datos sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones. En ella, se establece que "*cuando en casos específicos se deban retener datos de tráfico, debe haber una necesidad demostrable, el período de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la ley, de manera que proporcione suficientes salvaguardias frente a un acceso ilegal o cualquier otro abuso. Una retención sistemática de todas las clases de datos de*

[176] Dictamen 5/2002 sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones (11818/02/ES/Final WP 64)

tráfico para un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso".

De gran trascendencia resulta la introducción por parte de la Directiva 2002/58 de un sistema de *opt-in*[177] para la recepción de **comunicaciones comerciales**. Recordemos que la Directiva sobre comercio[178] electrónico dejó a elección de los Estados Miembros la opción por un régimen de inclusión o exclusión voluntaria ("*opt-in* u *opt out*"). España, en la transposición de la Directiva 2000/31, optó

---

[177] El Artículo 13 de la Directiva 2002/50 establece: "Comunicaciones no solicitadas
1. Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.
2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.
3. Los Estados miembros tomarán las medidas adecuadas para garantizar, que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional.
4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.
5. Los apartados 1 y 3 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a las comunicaciones no solicitadas.

[178] Artículo 7 de la Directiva 2000/31/CE sobre comercio electrónico, de 8 de Junio de 2000.

por la versión más restrictiva, a favor de los usuarios o consumidores estableciendo en la LSSI un régimen de inclusión voluntaria ("*opt-in*"), para poder recibir comunicaciones comerciales. De este modo, la LSSI prohibía el SPAM a todos los efectos. Debido a que esta regulación chocaba de plano con la regulación establecida por la Directiva 2002/58, la necesidad de su modificación era evidente. La Directiva se aprobó el 12 de Julio de 2002, día en el cual se publicaba en el BOE la LSSI. El MCYT justificó tal situación diciendo que esta disposición de la Directiva "no pudo incorporarse a la LSSI por falta de tiempo"[179]. Resulta difícil de creer, ya que en la Exposición de Motivos de la LSSI, se hacen continuas referencias a la Directiva que traspone, la Directiva 2000/31 sobre comercio electrónico, de fecha 8 de Junio de 2000, y por tanto, anterior a la Directiva 02/58. Es bien cierto que la Directiva 02/58 no había sido aprobada, pero su Propuesta (COM/2000/0385 final) era bien conocida, al menos por los sectores ajenos al MCYT. Así las cosas, la LSSI es modificada por la Ley 32/2003 General de Telecomunicaciones, en adelante, LGT. La modificación del artículo 21 de la LSSI por la Disposición Final primera de la LGT, recoge lo establecido por la Directiva 2002/58, es decir, que la prohibición de enviar correos publicitarios a personas que no lo hubiesen requerido o solicitado expresamente, no será de aplicación cuando exista una relación contractual previa, y los datos del destinatario hubiesen sido obtenidos de forma lícita, y los utilizara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean "similares". Resaltar que la LGT también introduce una modificación en la LSSI[180] por la que se establece a la Agencia Española de Protección de Datos (A.E.P.D.) como órgano con potestad sancionadora en cuestiones relacionadas

[179] Sin embargo, el Director General para el desarrollo de la Sociedad de la Información, llegó a afirmar durante la presentación de una campaña institucional sobre la LSSI el 25 de Noviembre de 2002 que "en la medida en que por la vía interpretativa ese consentimiento expreso se entienda dado en los términos en los que dice la directiva, así habría que interpretarlo y no tendríamos que acudir a una modificación ejecutiva".

[180] Artículo 43.1 i.f. LSSI.

con el Spam. La Directiva 2002/58 incluye, a diferencia de la Directiva 97/66, una regulación (artículo 5.3) sobre las cookies o chivatos, entendiendo por tales aquellos datos ocultos intercambiados entre un usuario de Internet y un servidor web que quedan archivados en el disco duro del usuario. Su finalidad inicial era conservar datos entre dos conexiones, pero también son un medio de control de las actividades del usuario así como de captación de datos. También habla[181] de los programas espía (*spyware*), y de los identificadores ocultos o *web bugs*. Cabe destacar que una de las enmiendas introducidas por el Parlamento Europeo a la Propuesta de Directiva de la Comisión, consistía en la obligación de obtener el permiso de previo de los usuarios antes de remitir cookies al navegador; pero finalmente el Consejo de Ministros la eliminó. No obstante, lo anterior denota la importancia o la concienciación que en torno al tema de las cookies ya existía. En aquel momento, la Directiva no establecía una regulación exhaustiva ni mucho menos; se limitaba a decir que siempre que la cookie tenga un fin legítimo, cabrá supeditar el acceso a una web o apartado de la misma, a la aceptación de la cookie. No obstante, sí que especificaba que se debía facilitar una información clara y precisa a los usuarios y éstos debían tener la oportunidad de impedir que se almacene en su web. No se distingue entre cookies fijas o temporales (técnicamente, "duraderas" o "de sesión", respectivamente). El GT29[182] había realizado diversos estudios sobre la privacidad e internet en aquel momento, por lo que llama la atención, la escasa o deficiente, regulación que de estos temas se hace en la Directiva en un primer momento. Como veremos más adelante, la Directiva 2009/136 modifica el régimen aplicable a las cookies.

En relación a la confidencialidad de las comunicaciones, la Directiva 58/2002[183] amplía la regulación de la confidencialidad. La novedad más importante es que amplía la extensión de la confidencialidad,

---

[181] Considerando 24 de la Directiva 2002/58.

[182] Vid. "Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea", del Grupo de Trabajo del Articulo 29, 5063/00/ES/final, WP 37.

[183] Artículo 5, Directiva 2002/58 y 97/66, "Confidencialidad de las comunicaciones".

abarcando no sólo a las "comunicaciones", sino también a "los datos de tráfico asociados a ellas". En el primer párrafo del artículo 5, se establece, tras afirmar la regla general de la confidencialidad de las comunicaciones, que ello "no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad". Con esta afirmación, se pretende diferenciar el almacenamiento técnico realizado por los proveedores de Internet por motivos estrictamente técnicos y de servicio, del almacenamiento con vistas a una posible reproducción. Pero ello ya se tuvo en cuenta en Directivas anteriores, como la Directiva sobre comercio electrónico, al establecer las responsabilidades de los Prestadores de Servicios. Se añade un nuevo párrafo (tercero) en el que se establece que únicamente se permitirá el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el terminal de un usuario o abonado, siempre que se le informe previamente del tratamiento y fines del mismo, y se le ofrezca la posibilidad de negarse a dicho tratamiento. Resulta muy clarificador el Considerando 21 de la Directiva, ya que una cosa es prohibir únicamente el acceso no autorizado, y otra cosa, que todos los accesos sean autorizados, tal y como se desprende del artículo 5 de la Directiva. Se trata de dos maneras de manifestar la prohibición de accesos no autorizados, pero con una gran diferencia de matiz, ya que poniendo en conocimiento del usuario el hecho del tratamiento y sus fines, un mayor número de usuarios podrán negarse a dicho tratamiento, a diferencia de la mera prohibición del acceso intencionado no autorizado.

Fruto del funcionamiento del propio sistema[184], que exige la revisión periódica de la normativa, se aprueban un nuevo conjunto de

[184] El artículo 25 de la Directiva marco 2002/21 establece "1. La Comisión examinará periódicamente el funcionamiento de la presente Directiva y presentará un informe al Parlamento Europeo y al Consejo, por vez primera a más tardar a los tres años de la fecha de aplicación indicada en el párrafo segundo del apartado 1 del

disposiciones[185] para la reforma del paquete anterior. Entre esas disposiciones nos encontramos con la **Directiva 2009/136/CE** del Parlamento europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

Una de las principales novedades introducidas por la Directiva 2009/136 consiste en la modificación de la regulación de las cookies. De este modo, se pasa de un modelo de exclusión voluntaria (*opt-out*) establecido por la Directiva 2002/58 a un modelo de *opt-in*. Así, el artículo 5.3 queda redactado de manera que "únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su *consentimiento después* de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red

---

artículo 28. A tal efecto, la Comisión podrá solicitar información a los Estados miembros y éstos deberán facilitarla sin dilación injustificada".

[185] Se aprueban la Directiva 2009/114/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 por la que se modifica la Directiva 87/372/CEE del Consejo relativa a las bandas de frecuencia a reservar para la introducción coordinada de comunicaciones móviles terrestres digitales celulares públicas paneuropeas en la Comunidad y la Directiva 2009/140/CE del Parlamento Europeo y del Consejo de 25 de Noviembre de 2009 por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónica.

de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario". En relación a las cookies exceptuadas del requisito del consentimiento previo, es de obligada lectura el Dictamen 4/2012[186] del GT29. En él se afirma que para decidir si una cookie está exenta del requisito de obtención del consentimiento informado, es importante comprobar detenidamente si cumple alguno de los dos criterios de exención definidos en el articulo 5, apartado 3, modificados por la Directiva 2009/136/CE. Si tras un examen detallado, persisten serias dudas sobre el cumplimiento o no de los criterios de exención, "los operadores del sitio *web* deberían considerar atentamente si existe la posibilidad práctica de obtener el consentimiento de los usuarios de manera sencilla y discreta, evitando así cualquier forma de inseguridad jurídica". Como ejemplo de cookies exentas, siempre que no se usen para otras finalidades adicionales, se citan en el Dictamen (p 12) las siguientes:

1. Cookies de entrada del usuario (identificador de sesión) para la duración de una sesión o cookies persistentes limitados a unas horas en ciertos casos.
2. Cookies de autenticación utilizados para prestar servicios autenticados para la duración de una sesión.
3. Cookies de seguridad centrados en el usuario que se utilizan para detectar abusos de autenticación para una duración limitada y persistente.
4. Cookies de sesión de reproductor multimedia, tales como los *flash player cookies*, para la duración de una sesión.
5. Cookies de sesión para equilibrar la carga, para la duración de la sesión.
6. Cookies persistentes de personalización de la interfaz de usuario, para la duración de una sesión (o algo más).

---

[186] Dictamen 4/2012 sobre la exención del requisito del consentimiento de cookies, adoptado el 7 de Junio de 2012. Disponible en http://ec.europa.eu/justice/data-protection/article29/documentation/opinionrecommendation/files/2012/wp194_es.pdf

7. Cookies de terceros para compartir contenidos sociales por los miembros conectados a una red social.

En el Dictamen también se pone de manifiesto que si una cookie se utiliza para varios fines, sólo estará exenta del requisito del consentimiento informado si cada uno de dichos fines encaja en alguno de los supuestos exceptuados. También se destaca que, a pesar de que las cookies de origen de sesión en mayor medida resultarán exentas, a diferencia de las cookies de origen persistentes, el criterio básico para determinar la exención no ha de ser el técnico, sino la finalidad de la cookies.

Otra de las modificaciones introducidas por la Directiva 2009/136/CE en la Directiva 2002/58, es la modificación de la definición de "datos de localización". Así, se entiende por dato de localización (artículo 2c) "cualquier dato tratado en una red de comunicaciones electrónicas *o por un servicio de comunicaciones electrónicas* que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el publico" . La única modificación estriba en añadir "o por un servicio de comunicaciones electrónicas" no por ello baladí, pues en nuestra opinión, al hacer hincapié en los sujetos que pueden tratar estos datos y no sólo en el lugar donde se tratan (red de comunicaciones electrónicas), refuerza su protección.

Por otro lado, al catálogo de definiciones establecidas en el artículo 2 de la Directiva 2002/58, se añade el concepto de "violación de los datos personales", entendiendo por tal la "violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad". En este sentido, se incluye en el artículo 4[187] una regulación más extensa de las medidas de seguridad

[187] Artículo 4 Directiva 2002/58 tras la modificación operada por la Directiva 2009/136:

"Sin perjuicio de lo dispuesto en la Directiva 95/46/CE, las medidas a que se refiere el apartado 1, como mínimo:

— garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley,
— protegerán los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos, y
— garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.
Las autoridades nacionales competentes podrán examinar las medidas adoptadas por los proveedores de servicios de comunicaciones electrónicas disponibles al público y podrán formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.
2. En caso de que exista un riesgo particular de violación de la seguridad de la red, el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá informar a los abonados sobre dicho riesgo y, cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el proveedor del servicio, sobre las posibles soluciones, con una indicación de los posibles costes.
3. En caso de violación de los datos personales, el proveedor de los servicios de comunicaciones electrónicas disponibles al público notificará, sin dilaciones indebidas, dicha violación a la autoridad nacional competente.
Cuando la violación de los datos personales pueda afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el proveedor notificará también la violación al abonado o al particular sin dilaciones indebidas.
La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la autoridad competente que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos.
Sin perjuicio de la obligación del proveedor de informar a los abonados o particulares afectados, si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la autoridad nacional competente podrá exigirle que lo haga, una vez evaluados los efectos adversos posibles de la violación.
La notificación al abonado o al particular describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información, y recomendará medidas para atenuar los posibles efectos adversos de dicha violación. La notificación a la autoridad nacional competente describirá, además, las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales.
4. Sin perjuicio de las medidas técnicas de ejecución adoptadas con arreglo al apartado 5, las autoridades nacionales competentes podrán adoptar directrices y, en caso necesario, dar instrucciones sobre las circunstancias en que se requiere que el proveedor notifique la violación de los datos personales, sobre el formato que debe

que ha de adoptar los proveedores de un servicio de comunicaciones electrónicas disponible para el público.

En relación al tratamiento de los datos de tráfico para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido (artículo 6.3 Directiva 2002/58), podrán tratarse en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Se añade que dicho consentimiento ha de ser previo. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

En relación a las comunicaciones no solicitadas, el nuevo artículo 13 añade un nuevo párrafo en el que se establece que los Estados miembros velarán porque que cualquier persona física o jurídica

---

adoptar dicha notificación y sobre la manera de llevarla a cabo. Podrán asimismo controlar si los proveedores han cumplido sus obligaciones de notificación con arreglo al presente apartado e imponer sanciones apropiadas en caso de incumplimiento.

Los proveedores llevarán un inventario de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a las autoridades nacionales verificar el cumplimiento de las disposiciones del apartado 3. El inventario solo incluirá la información necesaria a tal efecto.

5. Para garantizar una aplicación coherente de las medidas mencionadas en los apartados 2, 3 y 4, la Comisión, previa consulta a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido de conformidad con el artículo 29 de la Directiva 95/46/CE y al Supervisor Europeo de Protección de Datos, adoptará las medidas técnicas de ejecución en relación con las circunstancias, la forma de presentación y los procedimientos aplicables a los requisitos de información y notificación a que se refiere el presente artículo. La Comisión velará por que participen todas las partes interesadas pertinentes, especialmente con fines informativos sobre las mejores soluciones técnicas y económicas disponibles para aplicar el presente artículo.

Estas medidas, destinadas a modificar elementos no esenciales de la presente Directiva completándola, se adoptarán con arreglo al procedimiento de reglamentación con control contemplado en el artículo 14 bis, apartado 2".

adversamente afectada por las infracciones de las disposiciones nacionales adoptadas en desarrollo del presente artículo, y por lo tanto con intereses legítimos en la cesación o prohibición de dichas infracciones, incluidos los proveedores de servicios de comunicaciones electrónicas que deseen proteger sus intereses comerciales legítimos o los intereses de sus clientes, pueda emprender acciones legales contra dichas infracciones. Además, se incluye la posibilidad de que los Estados miembros establezcan sanciones a los proveedores de ser vicios de comunicaciones electrónicas que contribuyan por su negligencia a la comisión de infracciones de las disposiciones nacionales adoptadas en desarrollo del presente artículo.

Siguiendo con la normativa comunitaria, debemos mencionar la **Decisión Marco 2008/977/JAI** del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Esta Decisión, anterior a la entrada en vigor del Tratado de Lisboa, es el único instrumento a nivel europeo sobre la materia, ya que el resto de normas existentes se enmarcan dentro del llamado "tercer pilar". Su objetivo (artículo 1) es "garantizar un alto nivel de protección de los derechos y libertades fundamentales de las personas físicas y en particular su derecho a la intimidad en lo que respecta al tratamiento de datos personales en el marco de la cooperación policial y judicial en materia penal, contemplada en el título VI del Tratado de la Unión Europea garantizando al mismo tiempo un alto nivel de seguridad pública". A la vez que se mantienen en vigor las normas específicas sobre la materia dictadas en el marco del tercer pilar, el ámbito objetivo de la Decisión Marco se circunscribe al tratamiento transfronterizo de datos, lo que necesariamente conlleva un nivel de protección limitado y no homogéneo, además de requerir de transposición en cada Estado miembro, ya que el tratamiento de los datos personales dentro de los estados miembros no queda sometido a dicha Decisión Marco.

En este punto debe mencionarse el **Tratado de Lisboa de 2007,** debido a que elimina la estructura institucional basada en los llamados tres pilares, introducida por el Tratado de Maastricht, lo cual tiene

trascendencia en la legislación de protección de datos, ya que según al pilar al que pertenecieran, se seguían procedimientos diferentes. Así, hasta el Tratado de Lisboa, la legislación en materia de protección de datos se repartía entre el primer pilar (protección de datos con fines privados y comerciales) el cual se sometía al sistema comunitario de toma de decisiones y el tercer pilar (cooperación policial y judicial en materia penal), donde la toma de decisiones se realizaba a nivel intergubernamental.
La eliminación del sistema de pilares junto con las nuevas competencias que el Tratado de Lisboa otorga al Parlamento Europeo en materia legislativa, simplifican el sistema de protección de datos hasta la fecha existente. A su vez, el Tratado de Lisboa hizo jurídicamente vinculante la Carta de los Derechos Fundamentales de la Unión Europea para todos los países miembros de la Unión, (excepto Reino Unido y Polonia), y por tanto, al artículo 8 en el que se consagra el derecho a la protección de datos de carácter personal. Esto hace que estemos ante un nuevo escenario jurídico[188] que permitirá elaborar una normativa única y directamente aplicable en todos los estados miembros, en materia de protección de datos, incluído el ámbito de la cooperación judicial y policial en materia penal.

Dictámenes y Recomendaciones del grupo de trabajo del artículo 29 (GT29)

La Directiva 95/46, en su artículo 29, crea un "grupo de protección de las personas en lo que respecta al tratamiento de datos personales" de carácter consultivo e independiente, más comúnmente conocido como el Grupo de trabajo del artículo 29 (GT29). Está compuesto por un representante de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad creada por las instituciones y organismos comunitarios (Supervisor Europeo de protección de datos), y por un representante de la Comisión Europea,

[188] Vid. RALLO LOMBARTE, A., *Revista de Derecho Político de la UNED*, n. 85, Septiembre-diciembre 2012, pp. 26-29.

que realiza las funciones de secretaría del grupo. Las funciones del GT29 son:
a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas en aplicación de la presente Directiva 95/46 con vistas a contribuir a su aplicación homogénea; de hecho, si el GT29 comprobase la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la UE, deberá informar a la Comisión
b) emitir dictámenes destinados a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
c) asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.
En nuestra opinión, la actividad más interesante del GT, por su calidad y repercusión, son los Dictámenes o recomendaciones[189] que, a iniciativa propia emite. El GT elabora un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la UE y en los países terceros, y lo transmite al Parlamento Europeo, al Consejo y a la Comisión.

Paquete de protección de datos 2012: Propuesta de Reglamento Europeo sobre Protección de Datos

Coincidiendo con una nueva legislatura en el Parlamento Europeo (2009-2014), y las nuevas competencias obtenidas por éste tras el

[189] Pueden consultarse en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Tratado de Lisboa[190], la Comisión Europea incluye entre sus objetivos la iniciativa legislativa de un nuevo paquete de protección datos (*Data Protection Package*). Como hemos señalado anteriormente, el Tratado de Lisboa elimina el sistema de pilares, por lo que nos encontramos con el escenario perfecto para desarrollar un nuevo marco legislativo en materia de protección de datos, eliminando los textos vigentes herederos de la antigua estructura basada en pilares[191]. De este modo, tras la realización de una consulta pública[192], el 4 de noviembre de 2010, la Comisión publica la Comunicación COM(2010) 609 final[193], en la que bajo el título "*Un enfoque global de la protección de los datos personales en la Unión Europea*", identifica los problemas actuales, plasmando así las necesidades de la reforma y establece una serie de objetivos.

Como principales **problemas** identifica los siguientes:

---

[190] Artículo 14.1 del Tratado de la Unión Europea de 7 de febrero de 1992 firmado en Maastricht: "El Parlamento Europeo ejercerá conjuntamente con el Consejo la función legislativa y la función presupuestaria (…)". El artículo 16 del TFUE establece por su parte que "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".

[191] Así, la Directiva 95/46, la Directiva 2002/58 y el Reglamento 45/2001 entre otros, pertenecerían al antiguo primer pilar y la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, al tercer pilar.

[192] Pueden consultarse los resultados de la consulta en http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

[193] Disponible en http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:ES:PDF

-Abordar el impacto de las nuevas tecnologías: se debe clarificar y precisar la aplicación de los principios de la protección de datos a las nuevas tecnologías, con el fin de garantizar una protección real y efectiva de los datos personales, con independencia de la tecnología utilizada para tratar estos datos

- Reforzar la dimensión de mercado interior de la protección de datos: resulta necesario armonizar la legislación de los estados miembros, pues a pesar del actual marco jurídico común, el sector privado reclama una mayor seguridad jurídica e igualdad de condiciones en los diferentes mercados.

-Hacer frente a la globalización y mejorar las transferencias internacionales de datos: un mercado global conlleva la subcontratación de empresas fuera de la UE, lo cual supone problemas a la hora de determinar la legislación aplicable y la exigencia de responsabilidades. A su vez debe simplificarse el régimen de las transferencias internacionales de datos.

-Consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre protección de datos: conveniencia de reforzar el papel de las autoridades encargadas de la protección de datos para garantizar la aplicación de las normas.

-Mejorar la coherencia del marco jurídico que regula la protección de datos: se constata el consenso existente entre los participantes en la consulta sobre la necesidad de disponer de un instrumento global, aplicable a todos los tratamientos en todos los sectores y políticas de la Unión, que garantice un enfoque integrado y una protección global, coherente y eficaz.

Ante estos problemas, los **objetivos** marcados por la Comisión para la reforma legislativa en materia de protección de datos son:

-Reforzar los derechos de las personas, mediante las siguientes medidas:

- garantizando una protección adecuada en cualesquiera circunstancias, en el sentido de que se reconoce que algunas situaciones que implican el tratamiento de información especifica requieren la aprobación de medidas suplementarias en el marco del Derecho de la Unión;

- aumentando la transparencia para los interesados, mediante la utilización de un lenguaje claro y sencillo y facilitando el acceso a la información;
- reforzando el control sobre los propios datos, partiendo del fortalecimiento del principio de minimización de datos, mejorar las condiciones para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, clarificar el "derecho al olvido" y garantizar la portabilidad de los datos;
- fortaleciendo la sensibilización de la población respecto de los riesgos vinculados al tratamiento de los datos personales y respecto de sus derechos, planteándose incluso el establecimiento de obligaciones de realizar acciones de sensibilización;
- garantizando un consentimiento informado y libre, mediante el fortalecimiento de las normas en materia de consentimiento;
- protegiendo los datos sensibles, mediante el estudio de la inclusión de nuevas categorías de datos como "sensibles, como por ejemplo, los datos genéticos;
- reforzando la eficacia de las vías de recurso y las sanciones, mediante el estudio de la posibilidad de ampliar el poder de recurrir a los órganos jurisdiccionales nacionales a las autoridades encargadas de la protección de datos y a las asociaciones de la sociedad civil, así como el estudio de la posibilidad de endurecer las disposiciones vigentes en materia de sanciones;

-Profundizar en la dimensión de mercado interior:

- aumentando la seguridad jurídica y garantizando condiciones iguales a los responsables del tratamiento;
- reduciendo la carga administrativa;
- clarificando las normas relativas a la legislación aplicable y al Estado miembro responsable;
- reforzando la responsabilidad de los responsables del tratamiento;

- fomentando las iniciativas en materia de autorregulación y examinar la posibilidad de instaurar regímenes europeos de certificación;

-Revisar las normas de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal**;**
-en relación a la dimensión mundial de la protección de datos, clarificar y simplificar las normas aplicables a las transferencias internacionales de datos y promover principios universales mediante la elaboración de normas jurídicas y técnicas de alto nivel en materia de protección de datos en los terceros países y a nivel internacional y la defensa del principio de reciprocidad de la protección
-Reforzar el marco institucional para una mejor aplicación de las normas de protección de datos, mediante la clarificación y armonización del estatuto y los poderes de las autoridades nacionales de protección de datos y la mejora de su cooperación y coordinación.

El Parlamento Europeo, mediante Resolución de 6 de julio de 2011 aprobó que respaldaba el enfoque adoptado por la Comisión para la reforma del marco legislativo europeo en materia de protección de datos. Así, el 25 de Enero de 2012 la Comisión publicó el mencionado paquete legislativo para la reforma de la normativa de protección de datos de la UE. Dicho paquete incluye una Comunicación[194] sobre los principales objetivos de la reforma; la propuesta de Reglamento Europeo sobre protección de datos; una propuesta de Directiva específica sobre el tratamiento de los datos personales en el marco de la cooperación policial y judicial en materia penal, y un informe sobre la aplicación de la Decisión Marco de 2008, la cual en principio

[194] COMUNICACIÓN COM(2012) 9 final de la Comisión al Parlamento Europeo, al Consejo, al Comité´ Económico y Social Europeo y al Comité de las Regiones "*La protección de la privacidad en un mundo interconectado Un marco europeo de protección de datos para el siglo XX*I", que expone los principales componentes de la reforma del marco jurídico para la protección de datos de la UE, en la línea de los objetivos marcados por la Comunicación COM (2010) 609 final anteriormente mencionados disponible en http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:ES:PDF

quedaría derogada por la Directiva. Dicha Comunicación, "La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI" , afirma que el objetivo de las reformas legislativas propuestas es reforzar los derechos vigentes, otorgar a los ciudadanos medios eficaces y operativos para asegurarse de que están plenamente informados del destino de sus datos personales y posibilitarles un ejercicio más efectivo de sus derechos.
Siguiendo la línea marcada por la Comunicación de 2010, COM(2010) 609 final, fija los siguientes objetivos:

-Aumento del control de los ciudadanos sobre sus datos personales:

- siempre que se requiera el consentimiento, éste deberá ser explícito, es decir, mediante una declaración o actuación clara y afirmativa por parte del interesado;
- establecer un derecho efectivo al olvido, entendido como el derecho a que se supriman sus datos si retiran su consentimiento y no existen motivos legítimos para conservarlos;
- garantizar un acceso fácil a los datos propios y el derecho a la portabilidad de los datos;
- reforzar el derecho de información, especialmente con respecto a los menores;
- mejorar los medios que permiten a los ciudadanos ejercer sus derechos, reforzando la independencia y competencias de las Autoridades nacionales de protección de datos y ensanchando las vías de recursos administrativos y judiciales en caso de violación de los derechos de protección de datos. Legitimar a las asociaciones debidamente habilitadas para ejercitar acciones judiciales en nombre de los particulares;
- reforzar la seguridad de los datos, fomentando el uso de tecnologías que protejan la privacidad, privacidad desde el diseño, regímenes de certificación de la privacidad y

estableciendo la obligación general para los responsables del tratamiento de notificar toda violación de datos, tanto a los afectados como a las autoridades competentes en materia de protección de datos;

- aumentando la responsabilidad de quienes traten datos, mediante el nombramiento en las empresas de un Delegado de Protección de Datos, la imposición de la obligación de realizar evaluaciones de impacto sobre la protección de datos a las organizaciones que realicen tratamientos con cierto riesgo e introduciendo la privacidad desde el diseño.

-Potenciar la dimensión de mercado único de la protección de datos:

- aprobar un Reglamento en materia de protección de datos aplicable directamente en todos los estados miembros, lo cual supondrá un ahorro de cargas administrativas que redundará en un ahorro económico;
- ampliar la independencia y facultades de las autoridades nacionales de protección de datos;
- crear un sistema de "ventanilla única" de modo que los Responsables de tratamiento sólo tendrán como interlocutor a una autoridad nacional de protección de datos (la del estado miembro donde esté sito el establecimiento principal);
- cooperación eficaz entre las autoridades nacionales de protección de datos, estableciendo la obligación de realizar investigaciones e inspecciones en caso de petición de una Autoridad y el reconocimiento mutuo de sus decisiones. En este sentido, crear un mecanismo de coherencia a nivel de la UE asegurando que las decisiones de las Autoridades nacionales con mayor repercusión europea tengan en cuenta los puntos de vista del resto de autoridades;
- elevar el rango del Grupo de trabajo del artículo 29, convirtiéndolo en un Consejo Europeo de Protección de Datos, asumiendo la Secretaría, el Supervisor Europeo de Protección de Datos.

-Aprobar una Directiva en el ámbito de la cooperación policial y judicial en materia penal, para asegurar un alto nivel de protección de los datos personales en dicho ámbito y facilitar los intercambios de datos personales entre la policía y las autoridades nacionales de protección de datos.
Dicha Directiva aplicará los principios generales de protección de datos, pero respetando lo específico de dichos ámbitos y establecerá los criterios mínimos armonizados para toda posible limitación de las reglas generales.

-en relación a la dimensión mundial de la protección de datos se proponen las siguientes medidas para afrontar los retos que plantea la globalización:

- normas claras en la determinación de los supuestos en que el Derecho europeo se aplique a Responsables del tratamiento situados en terceros países, comprendiendo los supuestos en que se ofrezcan bienes y servicios a ciudadanos europeos o se realice un control de su comportamiento
- simplificar y reforzar las normas sobre transferencias internacionales de datos a terceros países.

El Parlamento Europeo, a través de la Comisión de Libertades, Justicia e Interior (conocida como la Comisión LIBE), en palabras de su propio presidente, Juan Fernández López Aguilar[195], "acogió favorablemente desde el primer momento esta iniciativa de la Comisión. La Comisión LIBE la hizo suya y la ha tramitado con plena conciencia al estar dando cauce a uno de los expedientes legislativos

[195] FERNÁNDEZ LÓPEZ AGUILAR, J., "Data Protection Package y Parlamento Europeo", p. 31, en RALLO LOMBARTE, A. y GARCÍA MAHAMUT, R., *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015.

no solamente más complejos sino más importantes no ya de la legislatura sino de toda la historia del Derecho Europeo".

1.4 Evolución del derecho a la protección de datos

La normativa actual en materia de protección de datos ha llegado a un grado de madurez suficiente, por la que deberíamos ser capaces de adelantarnos a los acontecimientos y legislar en pro de los intereses de las personas, de los titulares de los datos. Hemos comentado anteriormente las cualidades positivas de la normativa vigente en materia de protección de datos (principalmente la Directiva 95/46), pero ello no ha sido óbice para detectar determinados problemas, los cuales han motivado el planteamiento de una reforma de la normativa europea en la materia.

Como principales problemas u obstáculos señalaremos los siguientes:

1. falta de concreción o ambigüedad a la hora de determinar los criterios de aplicación de las normativas nacionales cuando se producen tratamientos en diferentes estados miembros ; el concepto de "establecimiento" ha generado multitud de problemas a la hora de determinar la normativa aplicable.
2. la propia evolución tecnológica, que ha puesto de manifiesto de forma más evidente las diferencias normativas existentes en los estados miembros, provocando una "barrera" a las empresas que desarrollan su actividad en toda o parte de la UE, sobretodo en relación a la normativa aplicable y las diferencias existentes en materia sancionadora.
3. nuevos riesgos para la privacidad, como resultado también de la evolución tecnológica. En este punto pensamos precisamente en el tratamiento de datos masivos.

4. la dificultad práctica en la aplicación de la normativa europea a la prestación de servicios a ciudadanos europeos por parte de empresas no pertenecientes a la UE.

Los anteriores problemas, unidos a la imposibilidad de "escapar" de la aplicación de la norma, han hecho necesario un replanteamiento de la normativa europea en materia de protección de datos. Es por ello que todo apuntaría a pensar que el Reglamento (UE) 2016/679 de protección de datos[196], en adelante RGPD, vendría a solventar todas aquellas situaciones que, en este punto actual, no tienen fácil encuadre en la normativa vigente, como podría ser el análisis de datos masivos, materializando, tras un proceso de madurez de la normativa, la evolución del derecho de protección de datos de carácter personal. No obstante lo anterior, existe una "doble cara" de los Principios de protección de datos, consistente precisamente en la conciencia de saber que los acontecimientos han superado la protección que dichos principios pueden y pretenden ofrecer**.** Es decir, podemos anclarnos en una visión territorial en el sentido de ignorar la globalidad en la que nos hayamos inmersos, así como en una visión digamos "tradicional" que ignore la realidad de los tratamientos de datos que a día de hoy se están produciendo sin respetar la normativa de protección de datos. O bien podemos plantearnos una evolución (lógica) de los principios de protección de datos, que den solución, de verdad, a los nuevos problemas surgidos.

Para analizar si existe dicha evolución de los principios de protección de datos, tomaremos el RGPD, comparándolo con la normativa vigente actual, para ver realmente qué novedades aporta y cómo plasma los Principios de protección de datos y así poder valorar si este Reglamento realmente aborda los puntos críticos planteados de una manera eficaz y con vocación de futuro.

---

[196] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Antes de entrar en el análisis del RGPD, destacar que ya fue objeto de análisis por el GT29 cuando era todavía una propuesta de Reglamento[197] en el que se insta a modificar determinados aspectos del citado texto.
En nuestra opinión, llama la atención, que muchos de los puntos destacados por el GT para ser modificados, son fruto de una deficiente técnica legislativa o de expresión, más que de una cuestión de fondo, o incluso ambas cosas a la vez como veremos a continuación. Analizaremos los puntos destacados por el GT en relación a la última versión de la propuesta de Reglamento, siguiendo el orden de su propio articulado y la versión finalmente aprobada del RGPD. Así, dentro del Capítulo I "Disposiciones Generales":

1) *Objeto y Objetivos*: *articulo 1.2bis*
Se establece la posibilidad de que los Estados miembros puedan mantener o introducir disposiciones más especificas para adaptar la aplicación de las normas del Reglamento "con respecto al tratamiento de datos personales para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés publico o en ejercicio del poder oficial conferido al responsable del tratamiento o para otros casos específicos de tratamiento, tal y como prevé el articulo 6, apartado 1, letras c) y e), definiendo con más precisión los requisitos específicos para el tratamiento y otras medidas para garantizar un tratamiento lícito y equitativo, también para otros casos específicos de tratamiento, tal y como prevé el capítulo ".
El GT considera que, de mantenerse esta disposición, debería ser entendida como una posibilidad dada a los Estados Miembros de especificar y adaptar lo establecido por el Reglamento sin rebajar sus niveles de protección. También subraya que la armonización debe ser siempre el objetivo.
Finalmente, el artículo 6.2 del RGPD establece "Los Estados miembros podrán mantener o introducir disposiciones más específicas

[197] Documento de 17/06/2015 disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX". Por tanto, vemos cómo se ha aprobado sin mayores modificaciones.

2) *Ámbito de aplicación material*: *art 2.2e) / artículo 2.2 d) RGPD*
El Reglamento no se aplicará por parte de las autoridades (...) competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, de ejecución de sanciones penales o "de protección y *prevención frente a las amenazas a la seguridad pública"*.
El GT llama la atención sobre la posibilidad de que una diferente implementación resulte en un diferente nivel de protección. Además, destaca que la "*prevención frente a las amenazas a la seguridad pública"* es una expresión bastante vaga (además de no relacionada con el concepto de delitos) y podría llegar incluso a incluir operaciones de tratamiento sólo por el hecho de que el Responsable opere en el ámbito de la aplicación de la ley. El GT es tajante y afirma que no hay ninguna razón para crear tal flexibilidad y excluir la seguridad pública del ámbito de aplicación del Reglamento.
El artículo 2.2 d) del RGPD establece la no aplicación del RGPD por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, *incluida la de protección frente a amenazas a la seguridad pública y su prevención",* por lo que a pesar del ligero cambio de redacción, el contenido permanece igual.
En cuando a la exención doméstica[198] (art 2.2 d), el GT reconoce la intención de ampliar[199] el ámbito de la exención doméstica del

[198] El Considerando 15 del Reglamento establece "El presente Reglamento no debe aplicarse al tratamiento por una persona física de datos de carácter personal en el transcurso de una actividad personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Las actividades personales y domésticas

Consejo, mediante la eliminación de referencias al interés lucrativo o que las actividades sean "exclusivamente" personales o domésticas, pero recuerda que cualquier excepción ha de ser formulada e interpretada restrictivamente y la exención doméstica debe reducirse a actividades "puramente" personales en concordancia con lo establecido por la Directiva 95/46 y la Jurisprudencia del TJUE.
El artículo 2.2 c) del RGPD[200] establece la no aplicación del Reglamento al tratamiento "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas". Por tanto, vemos cómo se ha eliminado la referencia a la necesidad de ausencia de "interés lucrativo", pero no el adverbio "exclusivamente".

3) *Ámbito de aplicación territorial: artículo 3*
El GT pone de relieve que dada la previsión en el propio Reglamento de un régimen de responsabilidad diferente para Responsables y Encargados del tratamiento, sería aconsejable incluir en su ámbito de aplicación territorial a los encargados de tratamiento no establecidos en la UE pero que traten datos por cuenta de un Responsable sujeto al Reglamento. En caso contrario, nos encontraríamos con que los encargados de tratamiento no establecidos en la UE que tratasen datos

---

incluyen la actividad en las redes sociales y la actividad en línea realizada en el contexto de dichas actividades personales y domésticas. No obstante, el presente Reglamento (...) debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas".

[199] El Consejo propone eliminar el texto en cursiva subrayado del art 2.2 d) "por parte de una persona física sin interés lucrativo en el ejercicio de actividades exclusivamente personales o domésticas"

[200] Considerando 18 RGPD: "El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas".

por cuenta de un Responsable establecido en la UE, estarían sujetos únicamente a una responsabilidad contractual, mientras que si estuvieran situados en la UE, entrarían dentro del ámbito de aplicación del Reglamento.
Vemos cómo el artículo 3.2[201] del RGPD finalmente menciona expresamente al encargado no establecido en la UE, pero en el supuesto en que las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. En el supuesto del párrafo tercero, cuando el Reglamento sea aplicable al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público, sólo se menciona al Responsable.

4) *Definiciones*
En relación al concepto de **consentimiento**, el GT llama la atención sobre la necesidad de establecer claramente la distinción entre *opt in* y *opt out*, pues la definición dada por el Reglamento hace referencia exclusivamente a una "declaración de voluntad" o "clara acción afirmativa" lo que podría chocar con lo afirmado en el considerando 25[202] en relación al consentimiento inequívoco.

---

[201] Artículo 3.2 RGPD "el presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable *o encargado no establecido en la Unión*, cuando las actividades de tratamiento estén relacionadas con a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión".

[202] El Considerando 25 del Reglamento establece "Se debe dar el consentimiento de forma **inequívoca** por cualquier medio apropiado que permita la manifestación libre, especifica e informada de la voluntad del interesado, ya sea mediante una **declaración** escrita, también electrónica, oral o, cuando lo exijan las circunstancias, cualquier otra **acción afirmativa clara** del interesado que manifieste su aprobación del tratamiento de datos de carácter personal que le afecten. Entre otros medios podría recurrirse a la selección de una casilla de un sitio web en Internet o cualquier

Finalmente, el Considerando 32 del RGPD zanja estas dudas, ya que comienza afirmando que "El consentimiento debe darse mediante un *acto afirmativo claro* que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, *el silencio, las casillas ya marcadas o la inacción* no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

Sobre la definición de **dato personal**, el GT llama la atención que lo establecido en el Considerando 24[203], "los números de identificación,

---

otra **declaración o conducta** que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio o la inacción no deben constituir consentimiento. Cuando fuere técnicamente posible y eficaz, el consentimiento del interesado al tratamiento podrá darse recurriendo a los oportunos ajustes de un buscador u otra aplicación. En esos casos será suficiente que el interesado reciba la información necesaria para poder dar un consentimiento libre, específico e informado al comenzar a utilizar el servicio. (...). El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento inequívoco a todos los fines del tratamiento. Si el consentimiento del interesado se ha de dar a raíz de una solicitud electrónica, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

[203] Considerando 24: "Cuando utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de los protocolos de internet o los

los datos de localización, los identificadores en línea u otros factores específicos no (...) deben ser considerados datos de carácter personal cuando no sirvan para identificar o hacer identificable a un individuo", si se interpreta *a sensu contrario* quiere decir que puede haber ocasiones en que los datos de localización o números de identificación, pueden no ser datos personales. Esto, además de erróneo, conllevaría una restricción exagerada sobre el concepto de dato personal.

Muy acertadamente, el GT recuerda que las direcciones IP, identificadores en línea y similares, deberán considerarse datos personales como regla general, tal y como se ha mantenido en la Jurisprudencia del TJUE.

El Considerando 30 del RGPD afortunadamente ha eliminado la referencia a que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos no deben considerarse datos personales cuando no sirvan para identificar o hacer identificable a un individuo. Así, establece que "Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas".

La **seudonimización**, definida en el art 3 ter) de la Propuesta y en el artículo 4.5 RGPD como "el tratamiento de datos personales de

---

identificadores de sesión almacenados en cookies. Ello puede dejar huellas que, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas e identificarlas. Los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos **no** (...) **deben ser considerados datos de carácter personal cuando no sirvan para identificar o hacer identificable a un individuo**".

manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable", debe ser tratada en opinión del GT como una herramienta de minimización de datos, y por tanto, de seguridad, y no como una categoría de datos personales diferente.

Dentro del Capítulo II, "Principios":
5) *Principio de Finalidad (Purpose limitation Principle*): *artículo* 6 / *artículo 6 RGPD Licitud del tratamiento*
El GT sugirió directamente la supresión del párrafo cuarto[204], el cual establecía la posibilidad de tratamiento por parte del Responsable para fines *incompatibles* con aquellos que fundamentaron su recogida. Ello es debido, afirman, a que la compatibilidad no debe confundirse con legitimidad. Establecer que un uso posterior es compatible con el inicial no significa que los datos puedan ser tratados sin una base legal o en aquella que fundamentó el tratamiento original. Es por ello que mucho menos procederá el tratamiento para fines incompatibles a los originales, por mucho que se exija un fundamento legal, tal y como se establece en el mencionado párrafo cuarto del artículo 6. Respecto a este artículo 6, el GT[205] propone la supresión de los párrafos segundo y cuarto, ya que "así se asegura de que el requisito de uso compatible en el artículo 5 y la legalidad del tratamiento en virtud del artículo 6 continúan funcionando como **requisitos acumulativos**".

---

[204] Art 6.4 Propuesta de Reglamento del Consejo: "Cuando la finalidad del tratamiento posterior sea incompatible con aquella para la que se recogieron los datos personales por el mismo responsable, el tratamiento posterior deberá´ tener base jurídica al menos en uno de los fundamentos mencionados en el apartado 1, letras a) a e). El tratamiento posterior por el mismo responsable para fines incompatibles por motivos de legítimo interés del responsable o de un tercero será´ lícito cuando estos intereses superen a los del interesado".
[205] Dictamen 03/2013 sobre la limitación del fin, p 44, disponible en inglés en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

El GT subraya que, según el marco jurídico actual, el tratamiento de datos para fines incompatibles con los especificados en el momento de la recogida, es ilegal y por tanto, prohibido. Como no podría ser de otra manera, el GT afirma que el nuevo Reglamento debería como mínimo asegurar el mismo nivel de protección que la Directiva 95/46 actualmente ofrece.

El párrafo cuarto del artículo 6 no ha sido eliminado, aunque sí modificado, en el sentido de que ya no aparece la palabra "incompatible". Así, establece que "Cuando el tratamiento para otro **fin distinto de aquel para el que se recogieron los datos** personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es **compatible** con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".

No se establece ninguna obligación de documentar tal análisis por parte del Responsable ni referencia alguna a las posibles consecuencias cuando dicho "análisis" no se realice correctamente o no sea ajustado a Derecho.

Resulta altamente llamativo, a la par que peligroso, que se introduzca este cambio en el Principio de Calidad, uno de los pilares básicos de la protección de datos y altamente asentado, por ofrecer garantías a los interesados en lo que respecta al tratamiento de sus datos.

Tratamiento necesario para finalidades de archivo, históricas o estadísticas e investigación científica:

El párrafo segundo del artículo 6 establece que "el tratamiento de datos personales que sea necesario con fines de archivo en interés público o con fines históricos, estadísticos o científicos será lícito siempre que se cumplan las condiciones y garantías previstas en el artículo 83".

El GT sugiere que, tal y como está redactado, parece constituir un nuevo e independiente fundamento legal para el tratamiento de datos, que únicamente necesitaría cumplir los requisitos establecidos por el art 83 (*Excepciones aplicables al tratamiento de datos personales con fines de archivo en interés público o con fines científicos, estadísticos e históricos*). Es por ello que el GT destaca que debe quedar claro que se han de cumplir también con los requisitos establecidos en el párrafo primero del artículo 6, como cualquier tratamiento de datos.

El artículo 5.1 b) del RGPD establece que "el tratamiento *ulterior* de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales". Al incluirse la palabra "ulterior", queda claro que el tratamiento en primer lugar debió fundamentarse en fines determinados, explícitos y legítimos, tal y como se establece en el propio artículo 5.1b), quedando así claro que no se trata de un fundamento independiente para el tratamiento de datos.

Por estas razones el GT29 propone[206] incluir como párrafos separados en el mismo artículo 5 ("Principios relativos al tratamiento") y no el artículo 6 ("licitud del tratamiento"), el supuesto de los criterios necesarios para valorar si la finalidad de un tratamiento de datos es incompatible con la finalidad original y el supuesto de tratamientos

[206] Dictamen 03/2013 sobre la limitación del fin, p. 43.

posteriores para finalidades de archivo, históricas o estadísticas e investigación científica.
El artículo 89 del RGPD establece que el tratamiento de datos con estos fines "estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo".
Por otro lado, el artículo 9.2 de la Propuesta establece la posibilidad de que puedan tratarse datos especialmente protegidos cuando sea "necesario con fines de archivo en interés público o a fines (...) históricos, estadísticos o científicos, y sin perjuicio de las condiciones y garantías contempladas en la legislación de la Unión o del Estado miembro, entre otras las contempladas en el artículo 83", sin exigir ningún otro tipo de fundamento legal.
El Artículo 9.2 j) del RGPD recoge el mismo supuesto, añadiendo que deberá respetarse lo establecido en el artículo 89, apartado 1, "sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Interés legítimo y datos seudoanonimizados:
La utilización de datos seudoanonimizados no debe interpretarse como un supuesto que exima al Responsable del tratamiento de realizar el test de ponderación correspondiente. Es únicamente un factor entre todos los que deberán ser tenidos en cuenta en el test de ponderación, entre los que se encuentra la finalidad del tratamiento.

Debe recordarse en este punto que los datos seudoanonimizados son considerados datos personales[207], ya que la disociación no es irreversible y por tanto, no son datos anonimizados.

El Considerando 47 del RGPD recuerda que el interés legítimo de un responsable del tratamiento puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable.

Tratamiento que no requiere identificación (artículo 10/ artículo 11 RGPD)

El artículo 10 establece "Si los fines para los cuales un responsable somete a tratamiento datos personales no requieren o ya no requieren la identificación de un interesado por el responsable del tratamiento, este no estará ni a obtener (...) información adicional ni a iniciar un nuevo tratamiento con vistas a identificar al interesado con la única finalidad de cumplir (...) el presente Reglamento.(...)" .

---

[207] El Considerando 26 recuerda que "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

El párrafo segundo del artículo 11 del RGPD establece que "Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación".
El GT afirma que este artículo puede conllevar que los Responsables de tratamiento o encargados no tengan que cumplir con el Reglamento en el caso de tratar datos seudoanonimizados. No obstante, como se ha mencionado anteriormente, el propio RGPD establece que los datos seudoanonimizados son datos de carácter personal. Realmente, este artículo no se entiende, pues en el caso de que para dicho tratamiento no sea necesario, de manera definitiva, identificar a los interesados, debería exigirse la anonimización. Y para el supuesto de que, para el tratamiento no fuera necesario identificar a las personas, de manera temporal, no entendemos a qué se refiere el artículo 11 cuando dice "no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento". Bastaría decir que en esos casos, se realizarán los tratamientos procediendo a la seudoanonimización.

Dentro del Capítulo III, "Derechos del interesado":
6) *información al interesado* (*artículo 14/ artículo 13 RGPD*)
El artículo 14 establece los puntos que constituyen el contenido del derecho de información. Además, el GT aconseja especificar información sobre posteriores tratamientos, el período de conservación de los datos, las medidas de salvaguarda adoptadas para las transferencias internacionales y sobre las medidas de seguridad adoptadas.
El párrafo tercero del artículo 13 del RGPD recoge expresamente: que cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho

tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
En el párrafo segundo, entre el contenido del derecho de información, el RGPD ha incluido el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 (*transferencia mediante garantías adecuadas*) o 47 (*Normas corporativas vinculantes*) o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.
Sinceramente, quizá el afán de transparencia e información para con el interesado, precisamente logre el efecto contrario, pues en el caso de la información sobre las transferencias internacionales, se están presuponiendo unos conocimientos técnicos que exceden del nivel medio del interesado. Veremos cómo se implementa el cumplimiento de este artículo[208], por otro lado tan importante en materia de protección de datos.

7) *derechos del interesado-enfoque basado en el riesgo*
El GT pone de relieve que los derechos del interesado deben ser respetados con independencia de los riesgos inherentes al tratamiento. Es por ello que expresiones como las utilizadas en el artículo 16[209]

[208] La AEPD ha publicado una "Guía para el cumplimiento del deber de informar", disponible en https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf donde se establece la posibilidad de cumplir con el deber de información mediante el sistema de capas.
[209] Artículo 16 RGPD: derecho de rectificación "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. *Teniendo en cuenta los fines del tratamiento*, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

(derecho de rectificación), "habida cuenta de los fines para los cuales se hayan tratado los datos", crean inseguridad y posibilitan que el nivel de protección otorgado al interesado no quede garantizado.

8) *derecho a la portabilidad de los datos (artículo 18 Propuesta / artículo 20 RGPD)*
El GT está a favor de que el derecho a la portabilidad se mantenga como un nuevo derecho independiente del derecho de acceso. Puntualiza que debería garantizarse con independencia de la base jurídica que legitimó el tratamiento, pues en el párrafo segundo este derecho se limita a cuando el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b);
El RGPD no ha introducido modificaciones en este punto.

9) *derecho de acceso (artículo 15)*
El artículo 15 establece que no se aplicará el derecho a obtener copia de los datos personales *cuando no sea posible facilitar dicha copia sin revelar datos personales de otros interesado*s o datos confidenciales del responsable del tratamiento.
El GT considera que establecer una restricción general sobre el derecho de acceso, es injustificado por motivos de privacidad, y supondría una reducción de los derechos de los interesados.
El artículo 15 del RGPD, en su párrafo cuarto, acertadamente ha introducido el límite genérico de no afectar negativamente a los derechos y libertades de otros, lo cual es muy distinto a limitar el derecho de acceso tal y como se redactó originalmente en la Propuesta, pues podía suponer una limitación injustificada de este derecho, tal y como puso de manifiesto el GT.

10) *derecho de oposición (artículo 19 Propuesta / 21 RGPD)*

El artículo 19 establece que el interesado "tendrá en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en el artículo 6, apartado 1, letras e) o f), en la primera frase del artículo 6, apartado 4 leída conjuntamente con el artículo 6, apartado 1, letra e) o en la segunda frase del artículo 6, apartado 4. El responsable del tratamiento dejará de tratar los datos personales, (...) salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, (...) los derechos y las libertades del interesado para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial".

El artículo 21.1 del RGPD finalmente establece "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite *motivos legítimos imperioso*s para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".

El GT ya mostró su preocupación por la regulación del derecho de oposición en la Propuesta, por el hecho de que se establezcan límites al citado derecho y, añadimos, límites marcados precisamente por conceptos jurídicos indeterminados, como por ejemplo "intereses legítimos imperiosos".

Nuevamente, estamos ante un caso en que el nivel de protección establecido por la actual Directiva podría verse disminuido, por lo que se recomienda garantizar el nivel de protección hasta la fecha existente. En general, las restricciones que la Propuesta establece en los derechos de los interesados, a lo largo de los artículos 12 a 20 y 5 y en general las excepciones incluidas a través de términos jurídicos indeterminados, van más allá de lo permitido por la Directiva actual y, en palabras del GT, constituyen una **violación del acervo comunitario**.

11) *Realización de perfiles (profiling) (artículo 20 / 22 RGPD)*
El artículo 20 de la Propuesta establece que "Todo interesado tendrá no ser objeto de una decisión (...) basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que *produzca efectos jurídicos* que le conciernan o le afecten de modo significativo".
El GT consideró que deberían incluirse disposiciones relativas a los propósitos para los que los perfiles puedan ser creados y utilizados y obligaciones específicas de información del Responsable a los interesados, en particular sobre su derecho de oposición a la creación de dichos perfiles. Tal y como está redactado, el GT considera que no es claro y que no provee de suficientes garantías a los interesados.
El artículo 22.1 del RGPD ha sido aprobado prácticamente igual, "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte *significativamente de modo similar*".

Dentro del Capítulo IV, "Responsable del Tratamiento y Encargado del tratamiento":
12) *Enfoque basado en el riesgo-Principio de Responsabilidad o rendición de cuentas* (*Accountability*).
El GT considera que el Principio de Responsabilidad es muy importante y debería incluirse la aclaración de que se aplica a todos (Responsables y encargados) y a todas las operaciones de tratamiento.
El artículo 5.2 del RGPD establece "El Responsable del Tratamiento será responsable del cumplimiento de lo establecido en el apartado 1 (*principios relativos al tratamiento*) y capaz de demostrarlo ("responsabilidad proactiva").

13) *Exención de designar un representante a los Responsables no establecidos en la UE (artículo 25.2b) / artículo 27.2 RGPD)*
Se establece la excepción de que los Responsables no establecidos en la UE no tendrán que nombrar un Representante cuando "las

operaciones de tratamiento que tengan un carácter ocasional y tengan pocas probabilidades de dar lugar a (...) un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, el contexto, el alcance y la finalidad del tratamiento". El GT considera que es una excepción muy vaga y que puede afectar a la efectividad del Reglamento. Como se ha repetido en apartados anteriores, cualquier excepción debe basarse en criterios objetivos.

El artículo 27.2 del RGPD establece como excepciones al nombramiento de un representante del Responsable no establecido en la UE,

a) al tratamiento que sea ocasional, que no incluyan el manejo a *gran escala de categorías especiales de datos* indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y *que sea improbable que entrañe un riesgo* para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

Vemos por tanto cómo la crítica del GT sigue plenamente vigente.

14) *documentación o Registros de categorías de actividades de tratamiento de datos personales (artículo 28 Propuesta / 30 RGPD)*

El GT considera que, como regla general, tanto los Responsables como encargados, deben documentar sus actividades de tratamiento, para asegurar la rendición de cuentas y la transparencia, no pudiendo ser objeto de ninguna excepción. No obstante, tanto la Propuesta como el RGPD contemplan excepciones.

La Propuesta en el artículo 28.4b) libera de la obligación de llevar los registros mencionados, a las "empresas u organizaciones que empleen a menos de 250 personas, a menos que sea probable que las operaciones de tratamiento que realicen den lugar a un alto (...) riesgo para los derechos y libertades de los interesados, por ejemplo problemas de discriminación, usurpación de identidad o fraude, cambio no autorizado de la seudonimización, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos

sujetos al secreto profesional o cualquier otro perjuicio económico o social (...) para el interesado, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento".
El artículo 30.5 del RGPD establece finalmente como excepciones a la llevanza de este registro a empresas u organizaciones que empleen a menos de 250 personas, "a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10".
Resulta llamativo que se hayan suprimido las referencias a las situaciones que pueden suponer un riesgo para los derechos y libertades de los interesados, como se citaba en la Propuesta, problemas de discriminación, usurpación de identidad o fraude, cambio no autorizado de la seudonimización, pérdidas económicas, menoscabo de la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional o cualquier otro perjuicio económico o social (...) para el interesado, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento.

15) *Notificación de las brechas de datos personales (artículo 31 Propuesta/ 33 RGPD)*
Con respecto a la obligación de notificación de violación de datos personales, tanto a las autoridades de control como al interesado, el GT sostiene que los supuestos deben ser diferentes en ambos casos, además de más amplios en el caso de notificación a la autoridad de control. En relación a la obligación de notificación de violación de datos personales al interesado, el GT sugiere que debería utilizarse la misma terminología que en la Directiva 2002/58. Excepciones como en el caso de que"el responsable del tratamiento ha tomado medidas ulteriores que garantizan que ha desaparecido la probabilidad de que se materialice el alto riesgo de que los derechos y libertades de las personas objeto de los datos … se vean gravemente afectados", son demasiado amplias y un motivo para no informar a los interesados.

Finalmente, el RGPD establece: "En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, *a menos que sea improbable que dicha violación de la seguridad constituya un riesgo* para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación".
Respecto a las excepciones de la obligación de información al interesado, se mantienen las de la Propuesta:
a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.
No obstante la decisión que haya tomado el Responsable, la Autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga.

16) *Consulta previa a la autoridad de control (artículo 34 Propuesta / 36 RGPD)*
El GT considera que el enfoque de la consulta obligatoria a la Autoridad nacional de control, debe ser compatible y coherente con el principio de rendición de cuentas, limitando por tanto esta obligación a situaciones en que es particularmente necesaria para salvaguardar los derechos y libertades de los interesados.

Actualmente, el RGPD establece que el Responsable deberá consultar a la Autoridad de control antes de proceder al tratamiento, "cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo". Es decir, configura la consulta previa a la Autoridad de control como obligatoria siempre que tras la realización de un PIA o Evaluación de Impacto en la Protección de los Datos Personales (EIPD) el tratamiento entrañe un alto riesgo. Parece ser que el objeto de esta consulta previa es que la Autoridad de control analice las medidas propuestas por el Responsable, ya que en el párrafo segundo del artículo 36 se establece[210] que cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar todos sus poderes de investigación o correctivos.

La cuestión radica en qué se entiende por un tratamiento que entrañe un "alto riesgo", pues es lo que determinará la obligación de consulta previa. Podemos plantearnos que cualquier afectación al derecho fundamental de protección de datos supone un "alto riesgo", por lo que entendemos que es del todo necesario que se clarifique este concepto jurídico indeterminado, entre otros.

---

[210] Artículo 36.2 RGPD "Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación". Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta".

17) *Delegado de Protección de Datos (artículo 35 / 37 RGPD)*
El GT considera que el DPD constituye una pieza fundamental con respecto al Principio de *accountability (responsabilidad proactiva)*.
La actual propuesta de Reglamento establece que "El responsable o el encargado del tratamiento podrán o, cuando lo disponga el Derecho de la Unión o el del Estado miembro, deberán designar un delegado de protección de datos (…)" lo cual puede suponer la no armonización entre los Estados miembros en este aspecto y disminuir la efectividad de tal figura.
El GT apoya la obligatoriedad del nombramiento de un DPD en base a unos criterios objetivos como el tipo, volumen de datos o naturaleza de la actividad.
El RGPD establece la obligatoriedad de designar un DPD, por parte del Responsable y encargado, en los siguientes supuestos:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una *observación habitual y sistemática de interesados a gran escala*, o
c) las actividades principales del responsable o del encargado consistan en el *tratamiento a gran escala de categorías especiales de datos* personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Nuevamente, deberá aclararse qué se entiende por "*observación habitual y sistemática de interesados a gran escala*". Por otro lado, llama la atención la mera existencia del supuesto c) ya que debería quedar englobado en el b) pues no deja de ser una tipología de tratamiento a gran escala, pero de "categorías especiales de datos".
El párrafo cuarto del artículo 37 abre la posibilidad a que, fuera de los supuestos en que es obligatoria la designación de un DPD, "el responsable o el encargado del tratamiento (..) podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el

Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados". Por tanto, la no armonización de esta figura puede disminuir su efectividad, tal y como manifestó el GT a la luz de la Propuesta.

Dentro del Capítulo V, "Transferencia de datos personales a terceros países u organizaciones internacionales":
18) *Principio de Adecuación*
El GT apoya la inclusión en el Reglamento del Principio de Adecuación o suficiencia, tal y como lo recoge el actual artículo 25 de la Directiva 95/46, ya que se trata de un principio angular en el marco regulatorio europeo. No obstante, el RGPD[211] establece como Principio general para las transferencias, el cumplimiento por parte del Responsable y encargado del capítulo (V) relativo a las transferencias, cuyas disposiciones se aplicarán con el fin de asegurar que el nivel de protección de las personas físicas garantizado por el Reglamento no se vea menoscabado. Esto no es lo mismo que establecía la Directiva 95/46 cuyo Principio se basaba en que el país tercero al que se realice la transferencia garantizara un nivel de protección adecuado.
El RGPD distingue entre transferencias basadas en una decisión de la Comisión de adecuación (artículo 45) y transferencias mediante garantías adecuadas (artículo 46), es decir, cuando ante la ausencia de una decisión de adecuación, el Responsable o encargado ofrezcan

[211] Artículo 44 RGPD "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".

garantías adecuadas[212] y los interesados cuenten con derechos exigibles y acciones legales efectivas.

19) *Derogación sobre la base del interés legítimo (artículo 44 Propuesta / 49 RGPD)*
El artículo 44 recoge las excepciones en caso de situaciones específicas. Una de estas situaciones es la basada en el interés legítimo del responsable[213].
El GT considera que, en caso de conservar esta excepción, debería configurarse como un supuesto excepcional y para transferencias no masivas, no repetitivas y sujeta a determinadas garantías.

---

[212] Artículo 46.2 RGPD "Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
b) normas corporativas vinculantes de conformidad con el artículo 47;
c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;
d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;
e) un código de conducta aprobado con arreglo al artículo 40, 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 interesados, o
f) un mecanismo de certificación aprobado con arreglo al artículo 42, 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 interesados.

[213] Art. 44 h) de la Propuesta de Reglamento de 11 de junio "la transferencia *que* no sea de gran escala *ni frecuente* , sea necesaria para la **satisfacción de los intereses legítimos del responsable** que no queden anulados por los intereses o derechos y libertades del interesado y el responsable o el encargado (...) haya evaluado todas las circunstancias que rodean la operación o la serie de operaciones de transferencia de datos y (...) hayan ofrecido, sobre la base de dicha evaluación, garantías apropiadas con respecto a la protección de datos personales".

El RGPD tras relacionar todos los supuestos en que excepcionalmente podrán realizarse transferencias internacionales de datos, a pesar de no existir una decisión de la Comisión ni de garantías adecuadas, añade un párrafo final en el que, en caso de no poder fundarse la transferencia en los supuestos excepcionados, ésta podrá realizarse siempre que no sea repetitiva, afecte solo a un número limitado de interesados, sea necesaria a los fines de *intereses legítimos imperiosos* perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento haya evaluado todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofrezca garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.
Por tanto, este párrafo viene a amparar "la excepción de la excepción" es decir, cuando no pueda realizarse la transferencia, por no existir una decisión de la Comisión, ni se ofrezcan garantías adecuadas, y ni siquiera encaje en los supuestos excepcionales, todavía podrá realizarse la transferencia, siempre que se den una serie de requisitos, entre los que se encuentran el "interés legítimo imperioso" del Responsable, y que se ofrezcan garantías adecuadas.

20) *Encargados y sub-encargados*
El GT reconoce que las condiciones propuestas recogen la posición previamente adoptada por el propio GT en su Dictamen 05/2012 sobre la computación en la nube (WP 196) y en el Documento de trabajo 2/2012 sobre los principios y elementos de las normas corporativas vinculantes para encargados de tratamiento (WP 195).

21) *Acceso por autoridades públicas*
El GT considera que la revelación de datos personales a la autoridad de un tercer país (Juzgado, Tribunal o autoridad administrativa) es una

cuestión muy importante y considera muy acertado el Principio de notificación de dicha solicitud a la Autoridad de protección de datos correspondiente. No obstante, en aquellos casos en que exista un Tratado de asistencia mutua legal o acuerdo internacional, la autoridad competente bajo el tratado o acuerdo internacional debería ser la autoridad que conozca de la solicitud en lugar de la Autoridad de protección de datos, que seria la adecuada para aquellos casos en que no existan estos mecanismos de cooperación o cuando sea difícil identificar la "autoridad competente".

En los Capítulos VI "Autoridades de control independientes", VII "Cooperación y coherencia" y VIII "Recursos, responsabilidad y sanciones":

22) *Ventanilla única o mecanismo One stop-shop*

El GT aboga por una solución que asegure la proximidad con los ciudadanos y una respuesta uniforme a las empresas. El proceso de cooperación debe ser simple, claro y eficiente para todos los actores con la finalidad de asegurar una efectiva supervisión en todas las circunstancias. El GT considera que los detalles de la implementación deberían ser desarrollados por el EDPB (*European Data Protection Board*) en lugar de detallarse en el Reglamento.

23) *Poderes de las Autoridades de Protección de Datos*

Para que el Reglamento sea realmente efectivo, debe dotar de herramientas efectivas a las Autoridades de protección de datos para asegurar el cumplimiento del mismo, y es por ello que son cruciales las facultades concedidas de suspender un tratamiento de datos o de imponer multas. Asimismo, el GT recuerda que todas estas facultades de las Autoridades de protección de datos deberían aplicarse tanto a entidades públicas como privadas. El GT considera necesario introducir una multa administrativa en casos en los que un Responsable o Encargado no cumpla con las obligaciones establecidas en el artículo 53.1 (artículo 58.1 del RGPD).

Vemos cómo finalmente el artículo 83.5 e) del RGPD prevé la posibilidad de multa administrativa por no facilitar acceso en incumplimiento del artículo 58, apartado 1.

24) *Representación de los interesados/ derecho a presentar una demanda (artículo 76 Propuesta/ artículo 80 RGPD*[214])

La posibilidad de que cualquier organización o asociación pueda presentar una reclamación ante la Autoridad de protección de datos, con independencia del mandato del interesado, no deberá conducir a una situación de abuso de los derechos del interesado o para presionar a la autoridad competente, por lo que siempre deberá respetar los intereses de los interesados.

A continuación, incluimos una tabla comparativa entre la Directiva y el RGPD finalmente aprobado. El texto subrayado en la columna del RGPD se refiere a las novedades incorporadas.

[214] Artículo 80 RGPD: "1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento".

Directiva 95/46	RGPD
Principio de calidad art 6	Principios relativos al tratamiento art 5
1. Los Estados miembros dispondrán que los datos personales sean:	**1.** Los datos personales serán:
a) tratados de manera **leal y lícita**;	a) tratados de manera **lícita, leal** y **transparente** en relación con el interesado («licitud, lealtad y transparencia»);
b) recogidos con **fines determinados, explícitos y legítimos**, **y no sean tratados posteriormente de manera incompatible con dichos fines**; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;	b) recogidos con **fines determinados, explícitos y legítimos**, **y no serán tratados ulteriormente de manera incompatible con dichos fines**; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
c) **adecuados, pertinentes y no excesivos** con relación a los fines para los que se recaben y para los que se traten posteriormente;	c) **adecuados, pertinentes** y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
d) **exactos** y, cuando sea necesario, **actualizados**; deberán tomarse todas las medidas razonables para que los **datos inexactos o incompletos**, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean **suprimidos o rectificados**;	d) **exactos** y, si fuera necesario, **actualizados**; se adoptarán todas las medidas razonables para que se **supriman o rectifiquen** sin dilación los datos personales que sean **inexactos** con respecto a los fines para los que se tratan («exactitud»);

e) conservados en una forma **que permita la identificación** de los interesados **durante un período no superior al necesario para los fines** para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las **garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos**.	**e)** mantenidos de forma que se **permita la identificación** de los interesados **durante no más tiempo del necesario para los fines** del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); **f)** tratados de tal manera que se garantice una **seguridad adecuada** de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).
2. Corresponderá a los **responsables** del tratamiento **garantizar el cumplimiento** de lo dispuesto en el apartado 1.	**2.** El **responsable** del tratamiento será **responsable del cumplimiento** de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).
Principios relativos a la legitimación del tratamiento art 7	Licitud del tratamiento art 6
Los Estados miembros dispondrán que el	1. El tratamiento solo será **lícito** si se cumple

tratamiento de datos personales sólo pueda efectuarse si:	al menos una de las siguientes condiciones:
a) el interesado ha dado su **consentimiento** de forma **inequívoca**, o	a) el interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios **fines específicos**;
b) es **necesario** para la **ejecución** de un **contrato** en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o	b) el tratamiento es **necesario** para la **ejecución** de un **contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) es necesario para el cumplimiento de una **obligación jurídica** a la que esté sujeto el responsable del tratamiento, o	c) el tratamiento es necesario para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento;
d) es necesario para proteger el **interés vital del interesado**, o	d**)** el tratamiento es necesario para **proteger intereses vitales del interesado** o de otra persona física;
e) es necesario para el **cumplimiento de una misión de interés público o inherente al ejercicio del poder público** conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o	e) el tratamiento es necesario para el **cumplimiento de una misión** realizada en **interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento;
f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo	f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran

1 de la presente Directiva.	la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. 2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX. 3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento deberá quedar determinada en dicha **base jurídica** o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para

	adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido. 4. Cuando el **tratamiento** para otro **fin distinto de aquel para el que se recogieron los datos** personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar **si el tratamiento con otro fin es compatible con** el **fin para el cual se recogieron inicialmente los datos** personales, tendrá en cuenta, entre otras cosas:

	a) cualquier **relación entre los fines** para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el **contexto** en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la **naturaleza de los datos** personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles **consecuencias para los interesados** del tratamiento ulterior previsto; e) la existencia de **garantías adecuadas**, que podrán incluir el cifrado o la seudonimización.
	Condiciones para el consentimiento
	1. Cuando el tratamiento se base en el consentimiento del interesado, el **responsable** deberá ser **capaz de demostrar que aquel consintió** el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una **declaración escrita**

	que también se refiera a otros asuntos, **la solicitud de consentimiento** se presentará de tal forma **que se distinga claramente de los demás asuntos**, de forma inteligible y de fácil acceso y utilizando un **lenguaje claro y sencillo**. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3. El **interesado** tendrá **derecho a retirar su consentimiento** en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello**. Será tan fácil retirar el consentimiento como darlo**. 4. Al evaluar si el consentimiento se ha dado **libremente**, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.
Tratamiento de categorías especiales de datos art 8	Tratamiento de categorías especiales de datos art 9
1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el	1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos

tratamiento de los datos relativos a la salud o a la sexualidad.	genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
2. Lo dispuesto en el apartado 1 no se aplicará cuando:	**2.** El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
a) el interesado haya dado su **consentimiento explícito** a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o	a) el interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento sea **necesario** para respetar las **obligaciones y derechos** específicos del responsable del tratamiento en materia de **Derecho laboral** en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o	b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento sea necesario para salvaguardar el **interés vital del interesado** o de otra persona, en el supuesto de que el	c) el tratamiento es necesario para proteger **intereses vitales del interesado** o de otra persona física, en el supuesto de que el

interesado esté física o jurídicamente incapacitado para dar su consentimiento, o	interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una **fundación**, una **asociación** o cualquier otro **organismo sin fin de lucro**, cuya **finalidad** sea **política, filosófica, religiosa o sindical**, siempre que se refiera exclusivamente a sus **miembros** o a las **personas que mantengan contactos regulares** con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o	d**)** el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una **fundación**, una **asociación** o cualquier otro **organismo sin ánimo de lucro**, cuya **finalidad** sea **política, filosófica, religiosa o sindical**, siempre que el tratamiento se refiera exclusivamente a los **miembros actuales o antiguos** de tales organismos o a **personas que mantengan contactos regulares** con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiera a datos que el **interesado haya hecho manifiestamente públicos** o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.	e) el tratamiento se refiere a datos personales que el **interesado ha hecho manifiestamente públicos**; f) el tratamiento es necesario para la formulación, el **ejercicio o la defensa de reclamaciones** o cuando los tribunales actúen en ejercicio de su función **judicial**; g) el **tratamiento** es **necesario** por razones de un **interés público esencial,** sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos

	fundamentales del interesado; h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, j) el tratamiento es necesario con **fines de archivo** en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que

	debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.
3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte **necesario** para la **prevención o para el diagnóstico médicos**, la prestación de **asistencia sanitaria o tratamientos médicos** o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por **un profesional sanitario sujeto al secreto profesional** sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una **obligación equivalente de secreto.**	**3.** Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un **profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad**, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.
	4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al **tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.**
4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por **motivos de interés público importantes**, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la	

autoridad de control. 6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión. 7. Los Estados miembros determinarán las condiciones en las que un **número nacional de identificación** o cualquier otro medio de identificación de carácter general **podrá ser objeto de tratamiento**.	
Datos relativos a infracciones, condenas penales art 8.5	Tratamiento de datos personales relativos a condenas e infracciones penales art 10
5. El tratamiento de datos relativos a **infracciones, condenas penales** o medidas de seguridad, sólo podrá efectuarse **bajo el control de la autoridad pública** o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un **registro completo de condenas penales** bajo el control de los **poderes públicos**. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.	El tratamiento de datos personales relativos a **condenas e infracciones penales o medidas de seguridad** conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un **registro completo de condenas penales** bajo el **control de las autoridades públicas.**

Información en caso de obtención de datos recabados del propio interesado art 10	Información que deberá facilitarse cuando los datos personales se obtengan del interesado art 13
Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la **identidad** del **responsable** del tratamiento y, en su caso, de su representante; b) los **fines del tratamiento** de que van a ser objeto los datos; c) cualquier otra información tal como: — los **destinatarios** o las categorías de destinatarios de los datos, — el **carácter obligatorio o no de la respuesta y las consecuencias** que tendría para la persona interesada una negativa a responder, — la existencia de **derechos de acceso y rectificación** de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.	1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: a) la **identidad** y los **datos de contacto del responsable** y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los **fines del tratamiento** a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), **los intereses legítimos** del responsable o de un tercero; e) los **destinatarios** o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de **transferir** datos personales **a un tercer país u organización internacional** y la **existencia o ausencia de una decisión de adecuación de la Comisión**, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las **garantías adecuadas** o apropiadas y a los **medios para obtener una copia de estas o al hecho de que se hayan prestado**.

	3. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el **plazo** durante el cual se **conservarán** los datos personales **o, cuando no sea posible**, los **criterios** utilizados **para determinar** este **plazo**; b) la existencia del **derecho** a solicitar al responsable del tratamiento el **acceso** a los datos personales relativos al interesado, y su **rectificación** o **supresión**, o la **limitación** de su tratamiento, o a **oponerse** al tratamiento, así como el **derecho a la portabilidad** de los datos; c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del **derecho a retirar el consentimiento** en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a presentar una reclamación ante una autoridad de control; e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

	f) **la existencia de decisiones automatizadas, incluida la elaboración de perfiles**, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 3. Cuando el responsable del tratamiento proyecte el **tratamiento ulterior** de datos personales para un **fin que no sea aquel para el que se recogieron**, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2. 4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.
Información cuando los datos no han sido recabados del propio interesado art 11	Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado art 14
1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, **desde el momento del registro** de los datos **o,** en caso de que se piense comunicar datos a un tercero, a más tardar, **en el momento de la primera comunicación** de datos, comunicar al	**1.** Cuando los datos personales no se hayan obtenidos del interesado, el **responsable** del tratamiento le **facilitará** la siguiente información: a) la **identidad** y los **datos de contacto** del responsable y, en su caso, de su representante;

interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello: a) la **identidad del responsable** del tratamiento y, en su caso, de su representante; b) los **fines del tratamiento** de que van a ser objeto los datos; c) cualquier otra información tal como: — las **categorías** de los **datos** de que se trate, — los **destinatarios** o las categorías de destinatarios de los datos, — la existencia de **derechos de acceso y rectificación** de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.	b) los datos de contacto del delegado de protección de datos, en su caso; c) los **fines del tratamiento** a que se destinan los datos personales, así como la **base jurídica del tratamiento**; d) las **categorías** de **datos** personales de que se trate; e) los **destinatarios** o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, **la intención del responsable de transferir** datos personales a un destinatario en un tercer país u organización internacional y la **existencia o ausencia de una decisión de adecuación de la Comisión**, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las **garantías adecuadas o apropiadas** y a los **medios para obtener una copia de ellas o al hecho de que se hayan prestado**. **2.** Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: a) el **plazo** durante el cual se conservarán los datos personales o, cuando eso no sea posible, los **criterios** utilizados para determinar este plazo; b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los **intereses**

	legítimos del responsable del tratamiento o de un tercero; c) la existencia del **derecho** a solicitar al responsable del tratamiento el **acceso** a los datos personales relativos al interesado, y su **rectificación** o **supresión**, o **la limitación de su tratamiento**, y a **oponerse** al tratamiento, así como el **derecho a la portabilidad** de los datos; d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del **derecho a retirar el consentimiento** en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada; e) el derecho a presentar una reclamación ante una autoridad de control; f) la **fuente** de la que proceden los datos personales y, en su caso, **si proceden de fuentes de acceso público**; g) la **existencia de decisiones automatizadas, incluida la elaboración de perfiles**, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. **3.** El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2: a) dentro de un **plazo razonable**, una vez obtenidos los datos personales, **y a más tardar** dentro de **un mes**, habida cuenta de

	las circunstancias específicas en las que se traten dichos datos; b) si los datos personales han de utilizarse para comunicación con el interesado, a más **tardar en el momento de la primera comunicación** a dicho interesado, o c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez. 4. Cuando el responsable del tratamiento proyecte el **tratamiento ulterior** de los datos personales para un **fin que no sea aquel para el que se obtuvieron**, **proporcionará** al interesado, **antes** de dicho tratamiento ulterior, **información sobre ese otro fin** y cualquier otra información pertinente indicada en el apartado 2. **5.** Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que: a) el interesado ya disponga de la información;
2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con **fines estadísticos o de investigación histórica o científica**, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.	b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con **fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u

	obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información; c) **la obtención o la comunicación esté expresamente establecida por el Derecho** de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una **obligación de secreto profesional** regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

2. Los datos como un bien económico

2.1 Economía digital. Impacto del *big data* en la economía

Dejando a un lado la perspectiva del *big data* desde la protección de datos de carácter personal, es indiscutible el valor del *big data* como un bien económico, o más precisamente, de los datos como un bien económico.

En este contexto de una economía digital, se habla de un cambio o transición de lo que denominaríamos economía tradicional o industrial a una economía digital. Una postura contraria a la contraposición entre economía tradicional y digital, es la de PORTER[215] que ya en 2001 afirmó que "La nueva economía no parece tanto una nueva economía sino una vieja economía que tiene acceso a una nueva tecnología" (la traducción es nuestra). De hecho, PORTER sostiene[216] que "necesitamos alejarnos de la retórica sobre "las industrias de Internet", "estrategias de comercio electrónico" y una "nueva economía" y ver Internet como lo que es: una tecnología habilitadora, un poderoso conjunto de herramientas que se pueden utilizar, sabiamente o imprudentemente, en casi cualquier industria y como parte de casi cualquier estrategia". Coincidimos plenamente con PORTER en el carácter habilitador de Internet, que se integra en todos los aspectos de nuestra sociedad, incluída la economía. Tal y como se afirma en un estudio llevado a cabo en el año 2000[217], "la convergencia tecnológica, entre la informática, telecomunicaciones y los contenidos, ha supuesto un cambio en la forma de gestionar los negocios, ha modificado los supuestos económicos fundamentales sobre los que se sustentan la mayoría de las empresas y ha

---

[215] PORTER, MICHAEL E., "Strategy and the internet", *Harvard Business Review* 79, no 3, (March 2001), 62-78, p. 78.

[216] *op. cit.*, p. 64.

[217] BANCO SANTANDER CENTRAL HISPANO, 2000, *Esp@ña on-line, ideas para afrontar la e-conomía*, Madrid, BSCH y Andersen Consulting, p. 22.

transformado la economía industrial en lo que hoy denominamos economía digital. Este hecho supone un cambio de paradigma único en la historia económica mundial: hasta ahora, eran las estrategias empresariales las que decidían o influían sobre las tecnologías a emplear; en este nuevo paradigma, las nuevas tecnologías son las que marcan las estrategias a desarrollar". Es decir, no creemos que deba entenderse la economía digital como un modelo económico que puede adoptarse o no, sino como la consecuencia lógica e irremediable producida por los avances tecnológicos. Como se menciona en el citado estudio[218], Craig Barret, por aquel entonces Consejero Delegado de Intel, ya entonces afirmó "En cinco años no habrá compañías de Internet porque todas las compañías serán de Internet... o no existirán".

En el contexto de la llamada economía digital, los datos juegan un papel de capital importancia, hasta el punto de hablar de la economía de los datos o economía basada en los datos. La "economía de los datos", en palabras de la Comisión[219], "se caracteriza por un ecosistema en el que diferentes tipos de agentes del mercado (como fabricantes, investigadores y proveedores de infraestructuras) colaboran para garantizar que los datos sean accesibles y utilizables". Según el Informe *European Data Market Study*[220], "la economía de los datos mide la repercusión global del mercado de los datos, es decir, el mercado en que se intercambian datos digitales como productos o servicios derivados de los datos brutos, en el conjunto de la economía. Implica la generación, recogida, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de los datos que hacen posibles las tecnologías digitales. La economía de datos también incluye los efectos directos, indirectos e inducidos del mercado de datos sobre la economía".

---

[218] *Op. cit.*, p 24.
[219] *Op. cit.*
[220] *European Data Market Study,* SMART 2013/0063, IDC, 2016, p. 133.

En 2014 la Comisión Europea aprobó la Comunicación COM (2014) 442 final[221], *Hacia una economía próspera impulsada por los datos*, en respuesta a la petición de acción de la UE por parte del Consejo Europeo de Octubre de 2013, para proporcionar las condiciones marco adecuadas para un mercado único de datos masivos y computación en la nube. En esta Comunicación la Comisión afirma[222] que la UE, en comparación con EE.UU., ha sido lenta en abrazar la revolución de los datos, además de que también carece de capacidad industrial comparable. Por ello, es necesario crear el contexto propicio para impulsar la economía de los datos, dado que son, afirma la Comisión, el centro de la futura economía y sociedad del conocimiento. La Comisión afirma[223] que "a condición de que se cumplan las normas sobre protección de datos de carácter personal (cuando corresponda), los datos, una vez registrados, se pueden reutilizar muchas veces sin pérdida de fidelidad. Esta generación de valor agregado es fundamental para el concepto de cadena de valor de los datos" . Por tanto, vemos cómo es imprescindible en primer lugar, cumplir con la normativa de protección de datos de carácter personal, y sólo cuando ésta no sea aplicable, bien porque no estamos ante datos personales o bien porque se han hecho anónimos, hemos de contemplar los datos desde la perspectiva económica, como núcleo de la economía. En este sentido la Comisión entiende el RGPD, por entonces todavía no aprobado, como "marco de protección de datos único, moderno, robusto, coherente y exhaustivo para la UE", que mejorará la seguridad jurídica y la confianza de los individuos en el entorno digital.

Siguiendo esta línea, la Comisión Europea está impulsando la denominada *economía de los datos*, en el contexto del Mercado Único Digital, cuya estrategia y hoja de ruta fue presentada en Mayo de

---

[221] Comunicación COM (2014) 442 final, disponible en http://ec.europa.eu/transparency/regdoc/rep/1/2014/ES/1-2014-442-ES-F1-1.Pdf

[222] *Op. cit.*, p. 3.

[223] *Op. cit.*, pp. 5 y 12.

2015, a través de la Comunicación COM(2015) 192 final[224], *Una Estrategia para el Mercado Único Digital de Europa*, de la Comisión al Parlamento Europeo, al Consejo, al Comité Social europeo y al Comité de las regiones. En dicha Comunicación la Comisión afirma[225] que "la economía mundial se está convirtiendo rápidamente en digital" y que "las tecnologías de la información y la comunicación (TIC) ya no son un sector especifico sino el **fundamento** de todos los sistemas económicos innovadores modernos". Es por ello que, como se afirma en la Comunicación, con vistas a aprovechar todas las oportunidades que Internet y las tecnologías digitales ofrecen y dar una respuesta a las cuestiones políticas que se plantean, la Unión Europea se plantea una acción coordinada, a través de la creación del Mercado Único Digital (MUD). La Comisión define el MUD como "aquel en el que la libre circulación de mercancías, personas, servicios y capitales está garantizada y en el que personas y empresas pueden acceder fácilmente a las actividades y ejercerlas en línea en condiciones de competencia, con un alto nivel de protección de los datos personales y de los consumidores, con independencia de su nacionalidad o lugar de residencia".

La estrategia propuesta para el MUD se basará en tres pilares:

1. Mejorar el acceso de los consumidores y las empresas a los bienes y servicios en línea en toda Europa:

Como presupuesto necesario para que el MUD genere nuevas oportunidades de negocio en Europa, deberán eliminarse los obstáculos a la actividad transfronteriza en línea, tales como las diferencias entre Estados Miembros en materia de Derecho contractual y Propiedad Intelectual, así como una reducción de las cargas relacionadas con el IVA. La Comisión también cree necesario unos servicios de paquetería transfronterizos de calidad y a unos precios competitivos, para que los consumidores adquieran confianza en el comercio electrónico transfronterizo. Asímismo, deberá

---

[224] Disponible en http://eur-lex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[225] Comunicación COM(2015) 192 final, p. 3.

eliminarse cualquier discriminación por razón de la nacionalidad o ubicación geográfica.

2. Crear las condiciones adecuadas para que las redes y servicios digitales prosperen:

El MUD necesita de un sector de telecomunicaciones fuerte, de alto rendimiento y a precios asequibles. Para ello, es preciso realizar un proceso de armonización de la normativa, en especial, la de gestión del espacio radioeléctrico. Por otro lado, debe analizarse el papel de las plataformas en línea, de modo que haya un marco legal adecuado a sus actividades. También debe reforzarse la confianza y seguridad en los servicios digitales, ampliando la oferta de soluciones más seguras, y en el tratamiento de datos personales. En este sentido, ya se ha aprobado el RGPD, que según la Comisión "incrementará la confianza en los servicios digitales ya que deberá las personas en relación con el tratamiento de datos personales por parte de todas las empresas que ofrezcan sus servicios en el mercado europeo".

3. Aprovechar al máximo el potencial de crecimiento de la economía digital europea:

La Comisión afirma[226] que "en menos de una década, la mayor parte de la actividad económica dependerá de los ecosistemas digitales que integraran infraestructuras digitales, equipos y programas informáticos, aplicaciones y datos", por lo que, "será necesario digitalizar todos los sectores si la UE quiere mantener una base industrial fuerte y gestionar la transición a una economía industrial y de servicios inteligente". Señala la Comisión que el 41% de las empresas de la UE no utiliza las tecnologías digitales avanzadas en absoluto.

La Comisión es consciente de que los datos masivos (cuyo sector afirma que está creciendo a un ritmo del 40 % anual, siete veces más rápidamente que el del mercado de las tecnologías de la información), los servicios en la nube y la Internet de las cosas, son fundamentales

[226] *Op. cit.*, p. 15.

para la competitividad de la UE y que para impulsar el MUD es necesario eliminar los obstáculos técnicos y legislativos actualmente existentes; como tales señala:

- los relacionadas con la ubicación de los datos;
- la fragmentación de la normativa en materia de propiedad intelectual y de protección de datos;
- la falta de claridad sobre los derechos para la utilización de los datos;
- la falta de sistemas y servicios abiertos e interoperables y de la portabilidad de datos entre servicios;
- la seguridad jurídica respecto a la atribución de responsabilidades en relación al Internet de las cosas.

Estos factores redundan en la falta de confianza de las empresas y consumidores, y por tanto, en la libre circulación de los datos.

En esta línea, en 2017 la Comisión elaboró la Comunicación COM (2017) 9 final[227], *Construyendo una economía europea de datos,* cuyos objetivos resumiremos a continuación:

- La libre circulación de los datos:

La libre circulación de los datos, segura y fiable, en palabras de la Comisión "resulta fundamental para la protección de las cuatro libertades fundamentales del mercado único de la UE consagradas en los Tratados (mercancías, trabajadores, servicios y capitales)". Permitir y proteger el flujo de datos supone un presupuesto necesario para que una economía de los datos dinámica. Los posibles obstáculos a la libre circulación de datos podrían adoptar diferentes formas, tales como requisitos injustificados de localización de los datos exigidos por las normativas nacionales, motivos de privacidad, de seguridad de la información etc apoyados en la idea equivocada de que los servicios localizados son más seguros que los transfronterizos. Además, la Comisión destaca que las autoridades públicas no deben utilizar la privacidad como motivo para restringir injustificadamente la libre

[227] Comunicación COM (2017) 9 final, disponible en http://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:52017DC0009

circulación de datos, tal y como el propio RGPD establece[228]. La Comisión recuerda que el Principio de Libre Circulación de los datos también es de aplicación en aquellos casos en que el RGPD permita a los Estados regular cuestiones específicas.

- Acceso y transferencia de datos:

En relación a los datos generados por máquinas o el Internet de las cosas, con el objetivo de aprovechar al máximo este tipo de datos, la Comisión considera imprescindible facilitar a los agentes del mercado el acceso a estos conjuntos de datos, lo cual es complicado pues los productores de los datos son los únicos con acceso, lo que según la Comisión, puede restringir su utilización en mercados descendentes.

En relación al tipo de datos tratados, como bien apunta la Comisión, los datos generados por máquinas pueden ser personales o no personales. En el primer caso, está claro que se aplicará la normativa de protección de datos, salvo que se anonimicen. Por tanto, los agentes intervinientes en la economía de los datos "tratarán habitualmente ambos tipos de datos". Además de la normativa de protección de datos, podría llegar a ser de aplicación la normativa de propiedad intelectual, el derecho sui generis sobre bases de datos y la normativa sobre protección de secretos comerciales (Directiva 2016/943), pero no sería lo habitual. En este sentido, cabe destacar el Proyecto de Directiva sobre los derechos de autor en el mercado único digital (COM(2016) 593 final), que introduce medidas para adaptar las excepciones y limitaciones al entorno digital y transfronterizo. Tal y como se establece en su Considerando 5, "en los ámbitos de la investigación, la educación y la conservación del patrimonio cultural, las tecnologías digitales permiten nuevos tipos de usos que no están claramente enmarcados por las normas vigentes de la Unión sobre excepciones y limitaciones. Por otra parte, el carácter optativo de las excepciones y limitaciones previstas en las Directivas 2001/29/CE, 96/9/CE y 2009/24/CE en esos ámbitos pueden afectar negativamente al funcionamiento del mercado interior, especialmente en el caso de

[228] Artículo 1.3 del RGPD "La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

los usos transfronterizos, que ocupan un lugar cada vez más importante en el entorno digital. Por consiguiente, procede evaluar de nuevo en función de esos nuevos usos las excepciones y limitaciones vigentes establecidas por el Derecho de la Unión que sean pertinentes para la investigación científica, la enseñanza y la conservación del patrimonio cultural. Es conveniente establecer excepciones o limitaciones obligatorias con respecto a los usos de tecnologías de minería de textos y datos en los campos de la investigación científica, la ilustración con fines educativos en el entorno digital y la conservación del patrimonio cultural". El Proyecto de Directiva define (artículo 2.2) "minería de textos y datos", como "cualquier técnica analítica automatizada para analizar textos y datos en formato digital a fin de generar información sobre pautas, tendencias o correlaciones". Tal y como se afirma en el Considerando 8, "estas tecnologías permiten a los investigadores tratar grandes cantidades de información para obtener nuevos conocimientos y descubrir nuevas tendencias". No obstante, existe cierta inseguridad jurídica a la hora de determinar hasta qué punto pueden llevar a cabo actividades de minería de textos y datos de contenidos. En el mismo Considerando se afirma que "en determinados casos, la minería de textos y datos puede comportar actos protegidos por derechos de autor o por el derecho sui generis sobre las bases de datos, en particular la reproducción de obras u otras prestaciones o la extracción de contenidos de una base de datos. Cuando no existe ninguna excepción o limitación aplicable, debe solicitarse una autorización a los titulares de derechos para llevar a cabo tales actos. La minería de textos y datos también puede tener por objeto meros hechos o datos que no están protegidos por derechos de autor y, en tales casos, no ha de ser necesaria una autorización". Puede ocurrir incluso que aun teniendo un acceso lícito a los datos, se excluya en las condiciones de la licencia, el uso de minería de textos y datos. El aumento del uso de las tecnologías en el ámbito de la investigación, unido a esta inseguridad jurídica, puede que afecte a la posición de Europa en materia de investigación. Para solventar este problema, esta inseguridad jurídica debe subsanarse estableciendo una excepción obligatoria respecto del derecho de reproducción, así como del derecho de prohibir la extracción de una base de datos

(Considerando 10), que se materializa en el artículo 3 del Proyecto de Directiva.

Respecto a la cuestión del acceso a los datos, el hecho de que el fabricante o proveedor del dispositivo tenga el "control de facto" de los datos generados, según la Comisión puede acarrear que el usuario no pueda autorizar el uso de los datos por un tercero. Aquí nos planteamos que, dado que se tratarán también datos personales, el fabricante deberá garantizar el derecho a la portabilidad[229] del interesado, por lo que sí podría facilitarlos a otro proveedor de servicios, o incluso "cuando sea técnicamente posible" que se transmitan directamente a otro Responsable. No obstante, podría argumentarse que el derecho a la portabilidad se aplicaría únicamente sobre datos personales, pero entendemos que todos los datos generados por el usuario, en tanto que se refieren a él como usuario del dispositivo, todos podrán ser objeto del derecho a la portabilidad.
La Comisión es partidaria de crear un marco europeo para regular el acceso a los datos generados por máquinas, para evitar fragmentación normativa dentro de Europa que sería negativa para el desarrollo de la

[229] Artículo 20 del RGPD "1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
b) el tratamiento se efectúe por medios automatizados.
2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros".

Economía de los datos, y plantea cuestiones que deberán debatirse entre las diferentes partes implicadas:

a) Mejorar el acceso a los datos anónimos generados por máquinas:

en nuestra opinión, los datos sólo serán anónimos tras el debido proceso de anonimización, pues en principio irán referidos al titular del dispositivo, y por tanto, estaremos ante datos de carácter personal.
La Comisión afirma que "mediante la puesta en común, reutilización y agregación, los datos generados por máquinas se convierten en una fuente de creación de valor, innovación y diversidad de modelos empresariales", lo cual resulta teóricamente lógico, pero en la práctica es mucho más complicado, pues no debemos olvidar que estamos dentro del sector privado y que además, en nuestra opinión, el usuario, antes de cualquier proceso de anonimización, deberá autorizar previamente la utilización de sus datos.
La Comisión plantea que las autoridades públicas deberían tener acceso a los datos cuando redunde en el "interés general" y permita mejorar el funcionamiento del sector público, bien sea en relación a información estadística o para investigación científica en relación a las ciencias médicas, sociales y medioambientales.
La Comisión habla[230] de los derechos de los "productores de datos" en relación al usuario del dispositivo y de los "titulares de datos" para referirse a los fabricantes, proveedores de servicios u otras partes. Se plantea por un lado que podría otorgarse al "productor de datos" el derecho a utilizar y autorizar la utilización de los datos no personales y por otro lado, "elaborar un marco basado potencialmente en determinados principios fundamentales, tales como las condiciones justas, razonables y no discriminatorias, para que los titulares de datos, tales como fabricantes, proveedores de servicios u otras partes, proporcionasen un acceso remunerado a los datos que poseen después de su anonimización". Consideramos imprescindible esta cuestión por las consecuencias que optar por uno u otro enfoque tendrían para los usuarios y para los tratamientos masivos de datos.

[230] COM (2017) 9 final, pp. 14 y 15.

b) Facilitar e incentivar el intercambio de datos:

En relación a las dificultades comentadas en el punto anterior, los incentivos resultan vitales para esta cuestión, pero deberán garantizarse las condiciones de igualdad para los agentes intervinientes. La Comisión plantea la posibilidad de establecer orientaciones para los contratos sobre los "derechos de control de los datos no personales" para ofrecer una mayor seguridad jurídica a las empresas. También menciona la Comisión la importancia del fomento del desarrollo de soluciones técnicas para la fiabilidad de la identificación y el intercambio de datos ya que "la trazabilidad y la identificación clara de las fuentes de datos constituyen un requisito previo para un verdadero control de los datos en el mercado". Nos planteamos si la identificación persistente de las fuentes de datos podría ser incompatible con el debido proceso de anonimización, irreversible por definición.

c) Proteger las inversiones y los activos:

La Comisión afirma que "cualquier solución futura debe también tener en cuenta los intereses legítimos de los agentes del mercado que invierten en el desarrollo de productos, garantizar un rendimiento razonable de sus inversiones y contribuir, por ende, a la innovación". Vemos por tanto, la dificultad que entraña facilitar un acceso e incentivar el intercambio de los datos, con los intereses legítimos de los intervinientes y una distribución equitativa de los beneficios.

d) Evitar la revelación de datos confidenciales:

Este objetivo en nuestra opinión es más bien es una *conditio sine qua non* de este posible marco europeo para el acceso a los datos. En este punto será muy importante la regulación de la responsabilidad en materia de protección de protección de datos.

e) Minimizar los efectos de cautividad, sobretodo en relación a pymes y particulares.

- Responsabilidad de los agentes involucrados en la economía de datos:

La Comisión es consciente de la importancia de establecer unas normas claras en materia de responsabilidad para la Economía de los

datos, pues sólo así se generará la confianza necesaria para los usuarios y el resto de agentes intervinientes. A su vez, la Comisión también es consciente de que la actual normativa sobre responsabilidad (extracontractual) por productos defectuosos[231] resulta de difícil aplicación al contexto del Internet de las cosas, razón por la cual ha puesto en marcha una amplia evaluación[232] de dicha Directiva. Entre los motivos que dificultan la aplicación de la normativa actual sobre productos defectuosos al ámbito del Internet de las cosas, la Comisión cita la incertidumbre sobre la naturaleza jurídica de los dispositivos IoT, si son productos, servicios o productos asociados a la venta de un servicio. Recordemos que la actual Directiva 85/374 no se aplica a los servicios, pero sí a los productos asociados al suministro de un servicio. Otro motivo sería la complejidad de la cadena de valor del producto o servicio y las interdependencias entre los agentes involucrados; y como tercer motivo la Comisión cita el carácter autónomo de estas tecnologías.
Como posibles soluciones, la Comisión menciona diferentes enfoques como la asignación de responsabilidad en función de la generación del riesgo o de la gestión del mismo; o incluir regímenes de seguro voluntarios u obligatorios.

- Portabilidad e interoperabilidad de datos no personales y otras normas técnicas apropiadas para su implementación:

Respecto a la portabilidad de datos no personales, la Comisión es consciente de que actualmente no existen normas que garanticen ni siquiera un nivel mínimo de portabilidad de los datos, en parte por la

---

[231] Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos, basada en el Principio de responsabilidad objetiva

[232] http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=9048
consulta pública sobre la evaluación de la Directiva 85/374/CEE. Puede consultarse la hoja de ruta de la evaluación y la estrategia de consulta en http://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products/ Páginas consultadas el 01-04-2017

dificultad técnica y económica, afirma la Comisión. Aquí nos planteamos quién sería el sujeto que podría exigir la portabilidad, si el usuario o una empresa. La Comisión propone la posibilidad de desarrollar derechos a la portabilidad de datos no personales, "en particular referidos a los contextos de empresa a empresa". También plantea la posibilidad de elaborar unas "cláusulas contractuales tipo que exigieran al prestador de servicios incluir la portabilidad de los datos de un cliente". Si estamos hablando de datos no personales, llama la atención que se refiera a los "datos de un cliente". Además, si el RGPD no establece la obligación en todo caso[233] de garantizar el derecho a la portabilidad de los datos personales de responsable a responsable, sería una incongruencia que sí se pudiera exigir respecto de los datos no personales.

En relación a la interoperabilidad, ésta está estrechamente relacionada con la portabilidad de los datos, en cuanto permite el intercambio de datos entre múltiples plataformas, facilitando tanto el cambio de proveedor como el uso simultáneo de varias plataformas. Para lograr una "portabilidad auténtica de forma tecnológicamente neutra" deben elaborarse unas normas técnicas apropiadas, y la Comisión se ha comprometido a respaldar dichas normas[234].

Está fuera de toda discusión que la portabilidad e interoperabilidad de los datos son requisitos previos necesarios para garantizar el pleno desarrollo de la Economía de los datos desde una perspectiva económica, pero no debe pasarse por alto el hecho que como la propia

---

[233] recordemos que el artículo 20.2 del RGPD establece que "el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable *cuando sea técnicamente posible"*. En el Considerando 68 se afirma que "(…) El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles (…)".

[234] COM(2016) 176 final, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité´ Económico y Social Europeo y al Comité´ de las regiones, Prioridades de normalización en el sector de las TIC para el mercado único digital, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016DC0176&from=ES

Comisión afirmaba[235] "un aspecto común que vincula la libre circulación de datos con las cuestiones emergentes del acceso y la transmisión de datos es que las empresas y agentes de la economía de los datos tratarán tanto datos personales como no personales, y que los flujos y los conjuntos de datos contendrán habitualmente ambos tipos. Cualquier medida deberá tener en cuenta esta realidad económica, así como el marco jurídico relativo a la protección de los datos personales, respetando al mismo tiempo los derechos fundamentales de las personas". Es decir, no resulta tan fácil realizar la separación de datos personales y no personales, pues no debe pasarse por alto que todos los datos, siempre que vinculados al titular de un dispositivo, deberán ser considerados personales. Por lo que hablar de la portabilidad de datos no personales, parte de la premisa de que siguen vinculados a un dispositivo o servicio, y por tanto, son datos personales. Podría argumentarse que los datos se portarían anonimizados, y aquí habría que responder previamente a cuestiones tales como quién es el titular del derecho a la portabilidad de datos no personales y quién es el sujeto que sería remunerado por proporcionar dichos datos. Si pensamos en que cualquier fabricante o proveedor de un servicio sea quien pueda pedir dicha portabilidad y se establezca una remuneración para el fabricante o proveedor de origen, ¿en qué lugar queda el usuario, que precisamente ha generado esos datos? Y este enfoque supondría que el usuario no tiene un derecho a negarse a que sus datos (aunque anónimos) no sean utilizados por terceros, por ejemplo, para tratamientos masivos de datos.

- Investigación y pruebas:

La Comisión plantea que "antes de llegar a conclusiones sobre la idoneidad de las posibles soluciones en materia de acceso a los datos y responsabilidad, debería organizarse un ensayo específico para analizar estas cuestiones en un entorno realista, en colaboración con las partes implicadas" y propone como posible escenario de prueba la

[235] COM(2017) 9 final p 10.

movilidad cooperativa, conectada y automatizada[236]. En las conclusiones de la Comunicación analizada, la Comisión afirma que "para construir la economía de los datos, la UE necesita un marco *político* que permita la utilización de los datos en toda la cadena de valor para fines científicos, industriales y sociales".

Por su parte, el Parlamento Europeo, a través del Comité sobre Libertades Civiles, Justicia y asuntos de interior (LIBE), solicitó un estudio realizado en 2015, sobre el impacto en la privacidad del *big data* y dispositivos inteligentes, en el que se pone de manifiesto que[237] "un análisis cuidadoso de las Comunicaciones de 2014 y 2015 muestra que la posición de la Comisión Europea está muy impulsada por el comercio y la economía, prestando poca atención a los retos legales y sociales clave. Si bien *Big Data* se presenta como una oportunidad de mercado que no debe perderse, la privacidad y la protección de datos, así como los riesgos mencionados anteriormente sobre Big Data, se abordan sólo marginalmente" (la traducción es nuestra). Siguiendo esta línea, en 2017 el Parlamento Europeo ha aprobado un *Informe (*Propuesta de Resolución*)*[238] *sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley.*

---

[236] COM(2016) 766 final, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *Estrategia europea sobre los sistemas de transporte inteligentes cooperativos, un hito hacia la movilidad cooperativa, conectada y automatizada* disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016DC0766&from=ES

[237] Disponible en http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU%282015%29536455_EN.pdf p 16.

[238] Informe del Parlamento Europeo, Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 20 de Febrero de 2017 disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//ES#title3

La OCDE[239] ya identificó en 2015 las cuestiones que la adopción del *big data* plantea en la Economía; como pone de manifiesto, algunas cuestiones no son nuevas (como por ejemplo, en relación a la privacidad, la minería de datos o el *profiling),* pero lo que sí es novedoso, afirma, es el aumento de la facilidad para inferir información sobre las personas, aunque éstas no hayan compartido la información voluntariamente. Las cuestiones identificadas por la OCDE, en relación al impacto del *big data* en la Economía son:

1. Privacidad y protección del consumidor:

En este punto, la OCDE resalta aspectos mencionados en el presente trabajo tales como la reducción del ámbito de los considerados datos no personales, y por tanto, la dificultad en la aplicación de la normativa de protección de datos actual eficazmente, especialmente del Principio de finalidad y limitación del uso. También destaca que la complejidad en el ecosistema y actores intervinientes en los bienes y servicios basados en datos, hace más difícil proporcionar a los individuos información completa y comprensible sobre la recogida y uso de los datos personales. La OCDE considera que "el acceso de los consumidores a sus datos personales se considera cada vez más importante para potenciar la innovación y aumentar la competencia en el mercado. Este acceso ayudaría a los consumidores a tomar decisiones mejor informadas al poder comparar los precios, obtener una visión general del historial de sus transacciones, examinar el valor de sus propios datos y participar así activamente en la economía basada en datos" (la traducción es nuestra).

Un punto interesante que destaca la OCDE, es que las Directrices sobre privacidad requieren una especificación de la finalidad previa a la recogida y el uso de datos personales, pero no restringen la naturaleza o el tipo de finalidades para las que se pueden utilizar datos personales. Según la OCDE, "este enfoque ha dejado los contornos del uso responsable de datos en gran medida indefinidos. Por ejemplo,

---

[239] OECD (2013), Working Paper "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by 'Big Data'", OECD Digital Economy Papers, n. 222, OECD Publishing, París. DOI: http://dx.doi.org/10.1787/5k47zw3fcp43-en, p. 334.

uno podría preguntarse: "¿Dónde reside el límite entre, por un lado, mejorar las relaciones con los clientes y, por el otro, la manipulación injusta del consumidor? ¿Cuándo se convierte la optimización del riesgo en discriminación injusta? " (la traducción es nuestra).

2. Acceso abierto a los datos:

La OCDE considera que la vinculación y el uso de datos entre sectores puede impulsar la innovación y generar beneficios socioeconómicos. No obstante, considera que el intercambio apropiado de datos en toda la economía requiere marcos más robustos. Menciona que muchas fuentes de datos de terceros aún no consideran compartir sus datos, y que los incentivos económicos pueden no estar alineados para alentarlo.

3. Riesgos de ciberseguridad:

La OCDE afirma que en tanto que el valor y volumen de los datos recogidos aumenta, también lo hace el riesgo de sufrir brechas de seguridad en torno a los mismos.

La OCDE considera que "dado que el uso de datos en la actualidad requiere que los sistemas de información y las redes sean más abiertos, las organizaciones están obligadas a adaptar su política de seguridad al entorno más abierto y dinámico en el que los datos se intercambian y utilizan ampliamente. Este enfoque es particularmente importante para aprovechar los beneficios de una economía basada en datos".

4. Habilidades y empleo:

La OCDE es consciente de que "personal cualificado con conocimientos en gestión y análisis de datos es esencial para el éxito de una economía basada en datos "más inteligente"", pero más allá de este hecho, la OCDE afirma que las implicaciones completas del *big data* en el empleo aún no se conocen bien. La OCDE observa que puede que determinados puestos de trabajo (que impliquen mano de obra directa) desparezcan, y afirma que "este cambio estructural se produce en un momento en que la economía es frágil y puede exacerbar el mercado de trabajo débil y el sesgo hacia mayores habilidades y desigualdad en los ingresos".

5. Infraestructuras:

Como afirma la OCDE, la disponibilidad de acceso de banda ancha de alta velocidad, en particular el acceso de banda ancha móvil, ha facilitado en gran medida la recopilación, el transporte y la utilización de datos en la economía. No obstante, señala, que la irrupción del Internet de las cosas, requerirá adoptar los cambios necesarios para que los millones de dispositivos puedan conectarse (cambios técnicos), pero también otros cambios regulatorios tales como la apertura del acceso a los mercados mayoristas móviles a empresas que no prestan servicios públicos de telecomunicaciones.

6. Medición:

La OCDE destaca que "el valor de las actividades basadas en datos está mal captado en las estadísticas económicas y, a menudo, insuficientemente apreciado por las organizaciones y los individuos". Es por ello que opina que "una mejora en la medición podría facilitar el desarrollo de políticas mejor adaptadas a la escala, los beneficios y los riesgos de los usos expansivos de los datos. Ello supondría una mejor comprensión del valor añadido de las actividades basadas en datos, incluidas las actividades de procesamiento de datos y almacenamiento de datos, la identificación de sectores en los que los datos constituyen un activo intangible clave y un mayor reconocimiento del impacto en el régimen existente para la recopilación, distribución y uso de datos en toda la Economía" (la traducción es nuestra).

Como vemos, de las seis áreas destacadas por la OCDE en relación al impacto del *big data* en la Economía, las tres primeras tienen relación o pueden tenerla con la privacidad y el derecho a la protección de datos, lo cual pone de manifiesto la importancia del impacto de los tratamientos masivos de datos en materia de privacidad, también desde una perspectiva económica.

Aunque en este punto del presente trabajo hemos querido centrarnos en el *big data* desde una perspectiva económica dejando de lado las implicaciones del *big data* en la privacidad, la posición del Parlamento Europeo pone de manifiesto la inextricable relación de ambas cuestiones. A nuestro entender, la clave reside en la supremacía de la privacidad sobre la perspectiva económica, ya que, como ya ha

puesto de manifiesto la Comisión Europea, una de las claves para el desarrollo de la llamada economía digital, es la confianza de los usuarios. Tras el análisis de la Comunicación (2017) 9 final de la Comisión *La construcción de una economía de los datos europea,* coincidimos con la posición del Parlamento Europeo en su opinión de que los riesgos para la privacidad se abordan marginalmente. Pero además, debe dotarse al análisis de la Comisión de una coherencia jurídica que permita el encaje de todas las cuestiones mencionadas, pues en nuestra opinión no deben tratarse como compartimentos estancos la información de carácter personal y la que no lo es, pues al fin y al cabo, se trata de información, y no puede dotarse a la misma de una naturaleza jurídica diferente en uno u otro caso.

2.2 ¿*Big data* como nuevo bien jurídico?

Tal y como afirma la Comisión Europea[240], "los datos se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso social".
Como comentábamos en el apartado anterior, creemos que la llamada economía digital no es sino el producto de la convergencia tecnológica, pero que ha propiciado un cambio en los supuestos económicos fundamentales, pues como afirma un estudio del año 2000[241], supone un cambio de paradigma único en la historia económica mundial al ser las nuevas tecnologías las que marquen las estrategias a desarrollar. En este sentido, los datos son un nuevo *bien* a tener en cuenta en el escenario económico, una nueva fuente de conocimiento y de riqueza, que de hecho ha dado lugar a la llamada economía basada en los datos (*data-driven Economy*).

[240] Comunicación COM (2017) 9 final, p. 2.
[241] *Op. cit.* BSCH y Andersen Consulting, p. 22.

Así, podemos plantearnos si el *big data* debe considerarse un nuevo bien jurídico[242]. Por nuestra parte, entendemos que no debe confundirse una concreta técnica con un bien jurídico digno de protección; es decir, el *big data* como técnica, no supone un bien jurídico en sí mismo considerado, sino que en todo caso, la información, los datos, constituirían ese bien jurídico, sean objeto de técnicas de *big data* o se pongan a disposición como datos abiertos (*open data*) u otros. No obstante, entendemos la información o los datos como un bien económico, no como un bien jurídico *stricto sensu*. Recordemos que en el derecho fundamental a la protección de datos personales, el bien jurídico protegido no son los datos personales en sí mismos considerados, sino el "poder de control sobre dichos datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado" (STC 292/2000 FFJJ 6º y 7º), por lo que la información o los datos no personales en sí mismos considerados, podrán constituir a lo sumo un bien importante en tanto en cuanto su valor económico, y además, no en todos los casos, sino que dependerá del tipo de información en cada caso considerada.

2.3 Derecho de acceso a la información

2.3.1 Sector Privado

Hemos visto cómo la Comisión Europea aboga por la libre circulación de los datos, el acceso a los datos no personales y su transferencia, pasando por el derecho a la portabilidad e interoperabilidad de los mismos, como motores de la denominada "economía de los datos". Desde esta perspectiva, podríamos plantearnos si existe un derecho a acceder a los datos (no personales). La Comisión Europea, una vez

[242] Vid. MIRALLES MIRAVET, S., "Big data, un nou bé jurídic?", *Món jurídic*, *Revista del Colegio de Abogados de Barcelona*, n. 293, 2015, pp. 18-19, disponible en catalán en http://www.icab.cat/files/242-474995-DOCUMENTO/293b.pdf

analizada la legislación comunitaria vigente, concluye[243] que en relación al tratamiento de datos no personales o anónimos:

No existe un marco legislativo exhaustivo sobre qué derechos pueden ejercerse con respecto al acceso a dichos datos, en particular con respecto a los datos creados por procesos informáticos o recopilados por sensores que procesan información de equipos, máquinas o programas informáticos o con respecto a las condiciones bajo las cuales dichos derechos pueden ejercerse;

Más allá de la Directiva sobre la protección de los secretos comerciales, no hay protección legal con respecto a las inversiones realizadas en la generación y/o recolección de datos;

Sólo existen reglas sobre el acceso a datos privados en un número muy limitado de sectores.

Por tanto, queda claro que no hay un fundamento jurídico que justifique un derecho de acceso a dichos datos por parte de cualquier agente interviniente en el mercado, más allá de un acuerdo contractual, basado en la voluntad de las partes. La Comisión realiza una serie de propuestas[244], no excluyentes, para el futuro marco de acceso a los datos no personales, que transcribiremos resumidamente a continuación (la traducción es nuestra):

1.Enfoque no legislativo:

1.1 Orientaciones para incentivar a las empresas a compartir datos;

La Comisión podría emitir orientaciones sobre cómo abordar en los contratos los derechos de control sobre los datos no personales.

1.2 Fomentar el desarrollo de soluciones técnicas para la identificación fiable, el intercambio y el acceso diferenciado a los datos;

---

[243] SWD(2017) 2 final, Commission Staff Working Document *on the free flow of data and emerging issues of the European data economy*, accompanying the document Communication (2017) 9 final Builing a European data economy, p. 22 disponible en http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0002&from=EN

[244] SWD(2017) 2 final, pp. 30-39.

Con independencia de la creación de derechos sobre los datos no personales, los mecanismos para identificar persistentemente al originador de los datos y a la entidad que desea fijar restricciones sobre el uso de dichos datos, pueden aumentar la confianza y así fomentar el intercambio de datos en contextos B2B. Las entidades en el origen de los datos podrían utilizar medios técnicos estandarizados para marcar en el origen (*watermaking*) determinadas propiedades en los datos como un medio técnico para asegurar su posición económica o preferencias de uso. Esto podría aportar confianza y seguridad adicionales a nivel de los datos, y por tanto codificar las reglas de acceso en los propios (meta) datos.

Los interfaces de programación de aplicaciones (API) pueden también fomentar la creación de un ecosistema de aplicaciones y desarrolladores interesados en los datos en posesión de las empresas, ayudando a las empresas y autoridades públicas a identificar y beneficiarse de diferentes tipos de reutilización de los datos que poseen. Ello beneficiaría a las partes más débiles que así podrían acceder de manera justa a explotar los datos.

1.3 Modelos contractuales tipo

Los costes derivados de las transacciones relativas al uso compartido de datos no personales pueden reducirse mediante la creación de modelos contractuales tipo para licencias de uso de datos que cubran las necesidades comerciales más comunes.

2.Enfoque legislativo:

2.1 Reglas contractuales dispositivas;

Podrían incluirse en la legislación reglas contractuales dispositivas que equilibrarían las condiciones contractuales B2B para aquellos casos en que las empresas no hayan previsto todos los supuestos. Al ser normas dispositivas, la libertad contractual quedaría garantizada. Además, podrían servir como referencia para realizar un control estándar sobre las condiciones contractuales. La Comisión señala que algunos Estados miembros han ampliado los supuestos de aplicación de la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre

las cláusulas abusivas en los contratos celebrados con consumidores, y la Comisión en el contexto de actual revisión de las Directivas relativas al consumidor y marketing, también está evaluando la mencionada Directiva. En un contexto de falta de regulación sobre el uso de los datos no personales, donde queda a la negociación de las partes pactar las condiciones de uso de los datos, quien posea la posición de negociación más fuerte será quien determine dichas condiciones, resultando para la parte más débil un contrato de adhesión. Es por ello muy importante prohibir cláusulas (abusivas) que se atribuyan el uso exclusivo de los datos impidiendo a otras partes, como el usuario del dispositivo, la utilización de los datos.

2.2 acceso para fines de interés público;
El sector público, al igual que el sector privado, está adoptando decisiones basadas en datos y trabajando por aumentar sus capacidades de análisis de datos. En diferentes áreas, el sector público podría mejorar significativamente sus procesos de toma de decisiones, utilizando información comercial. La legislación francesa sobre datos abiertos, ha introducido la posibilidad de que el Gobierno pueda solicitar a los agentes comerciales datos, con la finalidad de confeccionar estadísticas públicas. La Comisión propone que el concepto de "datos de interés público" introducido por la legislación francesa podría adoptarse a nivel europeo para una clase definida de datos a los que se podría dar acceso a organismos del sector público e investigadores financiados con fondos públicos.

2.3 derecho del productor de datos no personales o anónimos;
La Comisión plantea la posibilidad de crear un derecho para el "productor" de los datos no personales o anónimos, con el objetivo de potenciar su comercialización como un bien económico. La Comisión contempla la posibilidad de crear un derecho real y asignar el derecho exclusivo de utilizar los datos, incluido el derecho a conceder licencias de uso. Como derecho real, incluiría su eficacia *erga omnes*, con independencia de las relaciones contractuales, e impedir su uso por terceros no autorizados, incluyendo el derecho a reclamar daños y

perjuicios por acceso y uso no autorizados. La Comisión menciona que tal derecho no sería concebible con respecto a los datos personales por ser un derecho fundamental y aplicarse la legislación sobre protección de datos. Consideramos que no tendría coherencia jurídica concebir un derecho de propiedad sobre la información no personal y un régimen jurídico totalmente diferente para la información personal. En nuestra opinión, esta opción no es apropiada en absoluto para un bien inmaterial como es la información o los datos. La Comisión propone también la opción de, en lugar de concebir un derecho real, crear un conjunto de derechos puramente defensivos, asimilándose más a la protección de la posesión en lugar de la propiedad. La Comisión propone que podrían introducirse medidas en el ámbito del Derecho Civil, tales como el derecho a solicitar medidas cautelares para impedir el uso posterior de datos por terceros sin derecho a ello, o la posibilidad de reclamar daños y perjuicios por el uso no autorizado de los datos.

Llama la atención que en ningún momento la Comisión se plantea que la titularidad de este posible derecho sea el propio usuario, verdadero generador de los datos, lo cual además, le excluye de toda intervención y control sobre los datos.

En cuanto al titular del derecho, la Comisión propone un análisis exhaustivo de todos los elementos o circunstancias relevantes, tales como las inversiones realizadas y los recursos invertidos en la creación de los datos. Cuando sean varias personas o entidades quienes realizan inversiones conjuntas, podría haber derechos conjuntos sobre los datos generados.

Como excepciones a este nuevo posible derecho sobre el "productor" de los datos, se mencionan diferentes supuestos en los que pueda existir una obligación de compartir datos, como por ejemplo, cuando tal derecho no pertenece al fabricante del dispositivo, puede que éste además de tener un interés legítimo en utilizar datos para mejorar el diseño del producto, tenga una obligación legal de controlar el comportamiento de sus productos en el mercado; o cuando haya un "interés público" en poner ciertos datos a disposición de entidades privadas; o bien cuando organismos del sector público tengan un

interés legítimo en acceder a determinados datos (ej información estadística, protección del medioambiente; o por razones de interés científico para investigaciones financiadas total o principalmente con fondos públicos.

2.4 acceso bajo remuneración;
Esta opción requiere el análisis de importantes cuestiones tales como qué datos no personales quedarían dentro del "acceso regulado", es decir, qué grado de apertura se impone a los datos comerciales, los tipos de licencia que el productor o titular de los datos deberá conceder y otras cuestiones que la Comisión pone sobre la mesa.

2.3.2 Sector Público

En relación al acceso a los datos, el derecho de acceso a la información pública en algunos países ha sido reconocido como un derecho fundamental autónomo (ej Portugal), o bien se ha configurado jurisprudencialmente como un derecho fundamental[245], incluido dentro del derecho a la libertad de expresión, en su vertiente del derecho a *recibir* información. En España[246], ni la Jurisprudencia ni la Ley 19/2013 de 9 de Diciembre, de Transparencia acceso a la información pública y buen gobierno, reconocen el derecho de acceso como un derecho fundamental.
Dejando a un lado el debate sobre su carácter de derecho fundamental o no, bien es cierto que el derecho de acceso a la información pública

[245] Artículo 19 de la Declaración Universal de Derechos Humanos; artículo 19 del Pacto Internacional sobre Derechos Civiles y Políticos aprobado por la Asamblea General de Naciones Unidas. El Consejo de Europa adoptó el 27 de Noviembre de 2008 el Convenio sobre derecho de acceso a la información, el cual sólo ha sido ratificado por 10 países http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205

[246] Vid ROLLNERT LIERN, G., "El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la ley de transparencia", Revista Teoría y Realidad Constitucional, n. 34, 2014, pp. 349-368.

tiene como fundamento también la transparencia de los Gobiernos y Administraciones Públicas, pero no debemos olvidar que la sociedad, como generadora de información, tiene el deber de utilizarla para extraer conocimiento y revertirlo en esa misma sociedad. De ahí el derecho a acceder a la información que genera la Administración pública (y el deber de ésta de ponerla a disposición), pues dicho acceso es presupuesto necesario para su utilización o tratamiento y posterior extracción de información que aporte valor.

Es por ello que entendemos que la información, en su dimensión social, y con independencia de otros fundamentos jurídicos que puedan justificar su acceso, por su valor económico y de utilidad para el desarrollo de la Sociedad que precisamente la ha generado.

No obstante el valor que se pueda otorgar a la información en manos de las Administraciones Públicas, o el sector privado, no debemos olvidar la preeminencia en cualquier caso del derecho fundamental a la protección de datos de carácter personal, por lo que la no afección de la privacidad de las personas sería preponderante en cualquier caso, lo que nos llevaría a la posibilidad de concebir una suerte de derecho de exclusión de las personas en relación a los tratamientos masivos de datos. En este sentido, R. MIRALLES[247], habla de "la "objeción de conciencia digital, es decir, tener la capacidad de oponernos a que nuestros datos sean utilizados, incluso aunque sea de manera anonimizada, pero eso sí, sin renunciar a los beneficios de las tecnologías". R. MIRALLES, incluso habla del Principio de Objeción, como uno de los Principios en que debería basarse una futura regulación de *big data*.

Podría argumentarse en contra que, de existir este derecho de exclusión, la veracidad o representatividad de los datos se vería afectada, pero en nuestra opinión, la veracidad de los datos nunca ha sido una característica inherente al *big data*. Es más, este argumento

---

[247] MIRALLES LÓPEZ, R., *Aspectos a considerar en relación al Big Data*, Observatorio Iberoamericano de Protección de Datos, 25 de Julio de 2014, disponible en http://oiprodat.com/2014/07/25/aspectos-a-considerar-en-relacion-al-big-data/

precisamente redundaría en favor de la no discriminación en relación a decisiones automatizadas.

CAPÍTULO III : EUROPA VS EE.UU.

Desde el momento en que vivimos en un mundo globalizado, y las distancias físicas ya no existen gracias a la Sociedad de la información y del conocimiento[1] en la que estamos inmersos, resulta inevitable analizar la normativa por la que se rige la protección de datos de carácter personal en EE.UU., así como en el resto del mundo. El legislador debe ser realista a la hora de redactar las normas pero sin que ello suponga una menor protección de los derechos fundamentales de las personas. En este capítulo analizaremos el derecho a la privacidad en EE.UU., ya que muchas de las empresas que tratan datos de europeos son americanas, y viceversa.

Existe la conciencia o idea de que en EE.UU. no existe un derecho a la protección de datos o derecho a la intimidad, por no ser digno de la misma protección que en Europa, pero nada más lejos de la verdad pues, a pesar de que es cierto que su origen y configuración jurisprudencial distan mucho de lo que en Europa conocemos como derecho fundamental a la protección de datos, actualmente podemos decir que goza del estatus de derecho fundamental.

Analizaremos a continuación la evolución y configuración de la protección de este derecho en EE.UU.

---

[1] Sobre el concepto de Sociedad del conocimiento, KRÜGER "El concepto de 'sociedad del conocimiento' hace referencia, por lo tanto, a cambios en las áreas tecnológicas y económicas estrechamente relacionadas con las TIC, en el ámbito de planificación de la educación y formación, en el ámbito de la organización (gestión de conocimiento) y del trabajo (trabajo de conocimiento)". KRÜGER, K. *El concepto de la 'Sociedad del Conocimiento'*. Biblio 3W, Revista Bibliográfica de Geografía y Ciencias Sociales, Universidad de Barcelona, Vol. XI, nº 683, 25 de septiembre de 2006.

1. El derecho a la privacidad en EE.UU.

Consideramos imprescindible tener una visión global de la regulación de la privacidad, teniendo en cuenta la realidad de los tratamientos transfronterizos de datos. Por ello, en el presente capítulo analizaremos el derecho a la privacidad en EEUU y el ámbito de aplicación de la normativa europea.

1.1 Origen

Como se ha mencionado en el Capítulo II del presente trabajo, el origen del derecho a la privacidad en EE.UU. se sitúa con el artículo publicado por SAMUEL D. WARREN y LOUIS D. BRANDEIS en "The Right to Privacy, *Harvard Law Review* que sobre un concepto utilizado por primera vez por el Juez Thomas M. Cooley[2], resulta el primer texto defensor de la privacidad. No obstante, ello no quiere decir que no existiera preocupación o Jurisprudencia previa[3] sobre la materia.

Casi treinta años después del artículo de WARREN y BRANDEIS, en 1928, el por entonces ya Juez del Tribunal Supremo BRANDEIS utilizó dicho concepto *("the right to be let alone"*) en su famoso voto particular en el primer caso de escuchas telefónicas llevado ante el Tribunal Supremo (*Olmstead v. United States, 277 U.S. 438 (1928)*)

[2] Ver nota al pie 124 del Capítulo II.

[3] En *Ex parte Jackson*, 96 U.S. 727 (1878), el Tribunal Supremo estableció que la Cuarta enmienda prohibía al Gobierno abrir cartas sin una orden judicial; y en Boyd v. United States, 116 U.S. 616 (1886) el Tribunal Supremo estableció que la Cuarta enmienda protege a la persona y no permite al Gobierno exigir la aprehensión de documentos privados bajo requerimiento y su utilización como prueba.

para argumentar que la Cuarta y Quinta enmienda de la Constitución[4] amparaban el derecho a la privacidad. Concretamente, en este caso se cuestiona el hecho de que las escuchas telefónicas realizadas a varios sospechosos de importar, almacenar y vender bebidas alcohólicas, fueran legales o no, ya que se realizaron sin orden judicial. El Tribunal no consideró que constituyera una violación de la Cuarta enmienda (practicar registros y requisas arbitrarias), pues entendía que la Cuarta enmienda se refiere exclusivamente a registros materiales, y en este caso no se había allanado la propiedad de ningún sospechoso, llegando a decir que el cableado y los mensajes telefónicos no están protegidos por la Cuarta enmienda por no formar parte de su casa. Asímismo, tampoco consideró que se infringiese la Quinta enmienda (no incriminación contra uno mismo). Por el contrario, BRANDEIS en su voto particular premonitoriamente defiende una interpretación más amplia de la Cuarta enmienda, que se adaptase a los tiempos y por tanto, a las nuevas formas de invasión de la privacidad de las personas, no quedando relegada a las formas de invasión material (*physical trespass*) o a su vertiente puramente patrimonial.

BRANDEIS pone de manifiesto la necesidad de interpretar la Constitución de manera dinámica, pues una interpretación meramente literal, iría claramente en detrimento de los derechos fundamentales de los individuos frente a las injerencias del Gobierno o cualquier poder establecido. De esta manera, afirma que la Cuarta enmienda debe interpretarse como elemento de protección frente a cualquier intromisión injustificada en la vida de las personas, cualesquiera que sean los medios utilizados, y toda prueba obtenida mediante una

[4] Tal y como apunta D. J. SOLOVE en "A Brief History of Information Privacy Law", PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper n. 215, p. 4, tras la guerra de la independencia, la principal preocupación en materia de privacidad era la protección de la libertad frente a la intrusión del Gobierno, y así queda reflejado en la Tercera (prohibición del alojamiento de soldados en casas privadas sin el consentimiento del propietario), Cuarta (prohibición de registros arbitrarios salvo orden judicial motivada y limitada) y Quinta enmienda (derecho a no declarar contra uno mismo, derecho al debido proceso legal).

intrusión así, debe entenderse como una violación de la Quinta enmienda.
Esta visión negativa del derecho a la privacidad, permitió que la Cuarta enmienda sirviese no sólo para la protección frente a injerencias en el hogar de las personas, sino también frente a cualquier norma que atentase contra el comportamiento o aspectos relativos a la vida íntima de las personas.

Tuvieron que pasar varias décadas para que la interpretación de BRANDEIS fuera acogida jurisprudencialmente. No obstante, seis años después del caso *Olmstead,* se aprobó la *Federal Communicatios Act* , la cual establece que nadie, salvo autorización del emisor, podrá interceptar cualquier comunicación, y divulgar o publicar la existencia, contenido, significado de dicha comunicación, a ninguna otra persona. A pesar de tan clara afirmación, como acertadamente señala J. D. SOLOVE[5], la ley no prohíbe a las autoridades realizar escuchas, sino revelar su contenido en juicio, razón por la cual durante el siglo XX las escuchas realizadas por el FBI y las autoridades estatales han aumentado dramáticamente.
A comienzos de la década de los 60, en *Mapp v Ohio* 367 U.S. 643 (1961), el Tribunal Supremo estableció que en cualquier proceso penal, cualquier prueba obtenida en violación de la Cuarta enmienda sería excluida del proceso.
No obstante, no fue hasta 1965, en el caso *Griswold v Connecticut* 381 US 479, cuando el Tribunal Supremo reconoció la existencia de un derecho a la privacidad proporcionado por la interpretación conjunta de la Primera, Cuarta, Quinta y Novena enmienda. Se debatía si una ley que prohibía los anticonceptivos vulneraba un derecho constitucional a la intimidad en el ámbito del matrimonio y así se concluyó, basándose en la "teoría de las zonas de penumbra"[6]. Dicha teoría manifestada por el Juez Douglas, se basa en inferir el derecho a

[5] SOLOVE, D.J., *op. cit*., pp. 19 y 20.
[6] Vid. FAYOS GARDÓ, A., Los derechos a la intimidad y a la privacidad en el siglo XXI, Dykinson, 1ª ed., 2015, pp. 31 y 32.

la privacidad, no de manifestaciones expresas de las diferentes enmiendas, ya que no existe una declaración constitucional del derecho a la intimidad, sino precisamente de la interpretación de las mismas, de las zonas de penumbra creadas por otros derechos expresamente reconocidos. La importancia de esta sentencia radica, no tanto en su fundamentación, sino en que **por primera vez se reconoce un derecho constitucional a la intimidad.**

En 1967, en *Katz v. United States,* se supera finalmente la visión materialista de la Cuarta enmienda, tal y como defendió BRANDEIS en *Olmstead v. United States.* Se acusa a Charles Katz de traficar con información confidencial relativa a apuestas, por lo que se realizan escuchas a través de un micrófono colocado en las cercanías de una cabina telefónica, prueba gracias a la que en un principio es condenado. Hasta entonces, la Cuarta enmienda exigía que la injerencia física se realizase bien sobre la propia persona o bien sobre algún objeto de su propiedad. El hecho de que la cabina telefónica no perteneciera, obviamente, al acusado, impedía la aplicación de la Cuarta enmienda. Tal y como afirma J. L. RODRÍGUEZ LAINZ[7], "frente a tamaña limitación, el Tribunal, constatando la necesidad de otorgar una garantía constitucional a lo que entonces era ya plenamente reconocido como el derecho a la privacidad, da el paso de trasladar el centro de gravedad de la Cuarta Enmienda de los objetos o lugares, a las personas. Para ello introduce un nuevo juicio de valor de la constitucionalidad de la injerencia, denominado *reasonable-expectation-of-privacy test*; también conocido como *Katz test*. El enunciado de esta doctrina podía resumirse en la siguiente máxima: Un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables". Así, el Tribunal Supremo concluye que el espionaje electrónico constituye registro en el sentido de la Cuarta enmienda.

En 1968, un año después del caso Katz, se aprobó la Ley de Control del Crimen y la Ley Omnibus de Calles Seguras de 1968 (*Omnibus*

---

[7] RODRÍGUEZ LAINZ, J. L., "El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre", *Diario La Ley*, n. 8122, p. 2.

Crime Control and Safe Streets Act), la cual extendió el alcance de la normativa sobre escuchas, aplicándose no sólo a funcionarios del estado sino a cualquier persona. A pesar del gran avance que esto supuso, nos encontramos con una de las grandes limitaciones del sistema americano, ya que sólo se aplica a cualquier escucha auditiva, y no a otras formas de vigilancia realizadas por otros medios, como por ejemplo electrónicos o audiovisuales, lo cual es un gran contrasentido.

No obstante la superación de una interpretación limitante de la Cuarta Enmienda a partir de *Katz*, nos encontramos con toda una jurisprudencia posterior vacilante en torno a qué se entiende por "expectativa razonable de privacidad" en cada caso y según el Tribunal correspondiente.

El derecho a la privacidad también ha sido reconocido a partir de la Decimocuarta enmienda, la cual establece que ningún estado privará a nadie de su vida, de su libertad o de su propiedad sin que se haya seguido el debido proceso legal (*due process*). Así, la Jurisprudencia[8] comienza a reconocer un derecho fundamental a la privacidad a partir del concepto de libertad, inherente a la toma de decisiones en el ámbito privado de especial relevancia para el desarrollo de la personalidad, frente a cualquier injerencia estatal, salvo en el caso de que exista un "interés estatal relevante" (*compeling state interest*).

Es por ello que podemos hablar de una privacidad en la toma de decisiones (*Decisional Privacy*), respecto a la autonomía individual en la toma de decisiones que afecten al cuerpo de un individuo o a su familia, como en *Griswold v Connecticut* en el que el Tribunal estableció que el Gobierno no podría prohibir los anticonceptivos; o de privacidad de la información (*Informational Privacy*), como en *Whalen v Roe* 429 U.S. 589 (1977), donde el Tribunal reconoce por primera vez que el derecho constitucional a la privacidad incluye dos

[8] Comenzando con el voto discrepante del juez Harlan en *Poe v Ullman*, en 1961, ver el excelente análisis jurisprudencial realizado por SALDAÑA, Mª N., "El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego", *Teoría y Realidad Constitucional*, n. 28, 2011, pp. 290-299.

aspectos: la privacidad en la autonomía o *Decisional Privacy* y la privacidad de la información o *Information privacy*, interés individual en no revelar información personal. A pesar de que este derecho a la privacidad de la información no ha sido desarrollado por los tribunales, la mayoría de los tribunales de los diferentes estados lo reconocen.

De este modo, la existencia del derecho fundamental a la privacidad en EEUU ha venido infiriéndose a través de diferentes enmiendas de la Constitución. Como afirma SALDAÑA, Mª N, "Por esto no extraña que la centenaria formulación de la privacidad de Warren y Brandeis no sólo haya enraizado en la tradición constitucional norteamericana de la segunda mitad del siglo XX, sino que continúe emergiendo a la hora de delimitar los ámbitos protegidos constitucionalmente frente a la obtención y utilización de información personal en la sociedad tecnológica avanzada de principios del siglo XXI, eso es, la llamada "informational privacy".

1.2. Evolución

Hemos visto cómo en EE.UU. se ha debatido ampliamente sobre la existencia misma del derecho a la privacidad, debido al silencio de su constitución al respecto, hasta llegar a su reconocimiento por derivación de un Principio constitucional.

De esta manera, bajo el paraguas del derecho a la privacidad en EEUU, se engloba la protección que en Europa otorgamos desde el derecho fundamental a la intimidad, el honor, a la propia imagen y el derecho fundamental a la protección de datos de carácter personal. De ahí que el término "privacidad" sea un concepto muy amplio, coincidente en parte con nuestro concepto de intimidad y protección de datos, precisamente por su gran amplitud.

En multitud de ocasiones se ha puesto de manifiesto por parte de la Doctrina Americana[9], la dificultad misma de definir el término

[9] Vid. SOLOVE, DANIEL J., "Conceptualizing Privacy", 90 *Cal. L. Rev.* 1087 (2002), p. 1088 y 1089. Disponible en :

"privacidad". D. J. SOLOVE afirma[10] que la dificultad en la articulación de lo qué es la privacidad y por qué es importante, a menudo ha hecho que las normas sobre privacidad sean ineficaces y ciegas a los propósitos más amplios para los cuales deben servir. Siguiendo a este autor, a pesar de la multitud de diversas concepciones sobre la privacidad desarrolladas tanto por la Doctrina como por la Jurisprudencia, cabe distinguir seis grandes ámbitos dentro del concepto de "privacidad": 1) el derecho a ser dejado solo 2) acceso limitado a uno mismo (*limited access to the self*) 3) la reserva, el secreto 4) control de información personal 5) derechos de la personalidad 6) intimidad. Estos ámbitos no hacen sino referir a los objetos de protección de los diferentes derechos fundamentales que distinguimos en Europa. El problema en el Derecho Americano reside, además de lograr su encaje constitucional, en las vías de amparo para su reclamación por los afectados.

WARREN y BRANDEIS ya apuntaron que los daños causados a una persona por una invasión de su privacidad, no estaban protegidos específicamente en el derecho de daños[11], a pesar de que, en su opinión, el *Common Law* podría fácilmente desarrollar un remedio para la protección de la privacidad[12].

No obstante, como se puso de manifiesto en *Roberson v. Rochester Folding Box Co*., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902), el Tribunal

---

http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2

[10] SOLOVE, DANIEL J., *op. cit*., p. 1087 (La traducción es nuestra).

[11] La acción por difamación protegía la divulgación de información falsa, pero no de información privada y verdadera. El Derecho contractual protegía la privacidad únicamente de las partes de un contrato.

[12] WARREN y BRANDEIS, *op. cit.,* "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others". "(…) the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone";" (…) the existing law affords a principle from which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds".

no reconoció una acción concreta en la que sostener la reclamación de la demandante por la utilización de su imagen sin consentimiento en un anuncio publicitario (negó la existencia de un derecho a la intimidad), afirmando no encontrar precedentes judiciales y que la creación de la acción correspondía al legislador y no a los Tribunales. La sentencia causó un debate público que finalmente dio lugar al año siguiente a una Ley en el estado de Nueva York que reconoce la acción por invasión de la privacidad.

En 1960, WILLIAM PROSSER[13], introdujo cuatro categorías dentro de la responsabilidad civil por violación de la privacidad, actualmente recogidas en el *Restatement (Second) of Torts* (compilación oficial de las leyes de responsabilidad civil en EE.UU.). Así, se reconocen:

1. la acción por intromisión en la reclusión o invasión por intromisión *(intrusion upon seclusion*), que engloba aquellas acciones que descubran o revelen información privada, como por ejemplo interceptación de las comunicaciones o espiar mediante la captación de imágenes;
2. la acción por difusión pública de hechos privados (*public disclosure of private facts*); a diferencia de la acción anterior, en este caso la información no tiene que ser falsa, sino que los hechos privados difundidos, no son de interés público, y su difusión resulta altamente ofensiva para el sujeto. No podrían plantearse demandas en base a esta acción si dicha información hubiese sido ya difundida en el pasado, pues no habría una expectativa razonable de privacidad, o bien si primase la libertad de expresión o información.
3. acción por distorsión de la imagen (*false light*), correspondería en aquellos casos en que, a sabiendas de la falsedad de una información, altamente ofensiva, sea difundida al público;
4. la acción por apropiación del nombre o la figura (*appropriation*)[14], abarcaría todos los usos comerciales no

---

[13] PROSSER, WILLIAM L, "Privacy", 48 *Cal. L. Rev*., 383 (1960). Disponible en: http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1

[14] Cabe destacar, como un subtipo de la acción por apropiación, aunque no reconocido por PROSSER, el derecho al valor publicitario de la imagen o "*right of*

autorizados de la identidad de una persona y los daños causados a su dignidad;

La invasión por intromisión y la difusión pública de hechos privados, protegen directamente la dignidad del individuo, mientras que las otras dos acciones , distorsión de la imagen e invasión de la privacidad por apropiación, entroncan más con el concepto de propiedad. Siguiendo a PROSSER[15], la primera y la segunda requieren la invasión de algo secreto o privado, mientras que la tercera y la cuarta no. La segunda y la tercera requieren de publicidad, a diferencia de la primera y la cuarta, aunque ésta última normalmente la conlleve. La tercera requiere falsedad, mientras que el resto no.

Además de los agravios mencionados por invasión de la privacidad, la acción por violación del deber de confidencialidad, evolucionó para proteger la revelación de información facilitada dentro de una relación de confianza como la de médico-paciente.

Por otro lado, durante la segunda mitad del siglo XX, conforme la tecnología ha ido evolucionando, y por tanto, los medios para recoger información, han provocado el aumento de la preocupación por la privacidad. A la vez, numerosos organismos gubernamentales están siendo creados, lo cual motiva la aprobación en 1966 de la Ley de Libertad de la información (***Freedom of Information Act*, FOIA**). Esta ley permite a cualquier persona, sin necesidad de alegar un motivo, solicitar información a cualquier agencia del gobierno federal. A su vez todos los Estados han aprobado su propia Ley de Libertad de la información. Si se solicitan registros relacionados con otra persona y la divulgación de estos registros puede invadir la privacidad de esa persona, no se le entregarán estos registros, ya que existen determinadas excepciones[16] para respetar la privacidad de las personas.

---

publicity", reconocido por primera vez en Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc, 202 F.2d 866 (2d Cir. 1953), distinto al derecho de imagen como derecho personalísimo.

[15] PROSSER, W., *op. cit.*, p. 407.

[16] Existen nueve excepciones ("exenciones") bajo las que no se permitirá la divulgación de información amparándose en la FOIA. Las relativas a la privacidad

En 1973, el Departamento de Salud, Educación y Bienestar (HEW, acrónimo en inglés) de EEUU publicó el Informe[17] Archivos, ordenadores y los derechos de los ciudadanos (*Records, computers and the rights of citizens*) realizado por un Comité asesor sobre los Sistemas de Automatización de Datos en los ámbitos de salud, educación y bienestar social, mantenidos tanto por organizaciones públicas como privadas. Este comité asesor a través de su informe, estableció un Código de prácticas honestas de información (***Code of Fair Information Practices*, FIP**s) en relación al tratamiento automatizado de datos personales, el cual ha servido de base para la mayoría de las leyes de privacidad aprobadas posteriormente en los EE.UU.

Los cinco Principios en los que se basa el Código son:

1. No debe mantenerse en secreto la existencia de ningún sistema de archivo de datos personales.
2. Toda persona debe ser capaz de averiguar qué tipo de información sobre su persona se mantiene en cualquier archivo y qué uso se hace de ésta.
3. Toda persona debe ser capaz de impedir que la información sobre su persona obtenida con un fin específico sea utilizada o puesta a disposición para otros fines sin su consentimiento expreso.
4. Toda persona debe ser capaz de corregir o enmendar cualquier archivo que contenga información identificativa sobre su persona.

---

son: 6) Información que, si fuera divulgada, podría invadir la privacidad personal de otra persona; 7) Información compilada para fines de las fuerzas del orden público, si uno de los siguientes daños podrían ocurrir: se podría prever razonablemente que constituirá una invasión no justificada de la privacidad personal. Para más información http://www.foia.gov

[17] Departamento de Salud, Educación y Bienestar Social de los EE.UU. Comité Asesor del Secretario sobre los Sistemas, Archivos y Computadoras y los Derechos Ciudadanos viii (1973) disponible en https://www.justice.gov/opcl/docs/rec-com-rights.pdf

5. Toda organización que cree, mantenga, utilice o distribuya archivos que contengan información de datos personales de identificación debe asegurar la fiabilidad de éstos para los fines perseguidos y adoptar medidas para prevenir el uso indebido de dichos datos.

La aprobación de las FIP, supone un cambio de enfoque en lo que la legislación en materia de privacidad se refiere, pues en lugar de enfocarse en la reparación del daño, acoge los derechos de privacidad como medio para prevenir un riesgo futuro[18]. Un año más tarde, en 1974, se aprueba la **Ley de Privacidad (*Privacy Act*[19])**, que dando respuesta a cuestiones surgidas del Informe del Departamento de Salud, Educación y Bienestar (HEW), regula la recolección y uso de archivos por parte de las Agencias federales y otorga a los individuos el derecho a acceder y corregir su información personal.

En dicha Ley[20] se establece que "el derecho de privacidad es un derecho personal y fundamental protegido por la Constitución de los Estados Unidos". El gran inconveniente es que esta ley únicamente se aplica al sector público y a nivel federal, por lo que queda excluido el grueso del sector privado y las agencias estatales y locales.

Otro aspecto muy criticado de esta Ley es la excepción del "uso de trámite" (*routine use*[21]) definido como, en relación a la revelación de un registro, el uso del registro para una finalidad *compatible* con la finalidad para la cual hubiere sido obtenido. Resaltar que no habla de finalidades *idénticas*, sino compatibles, lo cual por tanto incluye

---

[18] OHM, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization (August 13, 2009)". *UCLA Law Review*, vol. 57, p. 1701, 2010; *U of Colorado Law Legal Studies Research Paper* No. 9-12, p 1734.

[19] Privacy Act of 1974, 5 U.S.C. § 552a.

[20] Anexo V, Sección 2, a) 4 de la Ley de Privacidad de 1974.

[21] En la subsección e) 4 D) se establece que deberá publicarse en el Registro Federal, anualmente por lo menos, una nota acerca de la existencia y carácter del sistema de registros que comprenderá, entre otros aspectos, "cada uso de trámite de los registros comprendidos en el sistema, comprendidos los grupos de usuarios y la finalidad de tal uso". En la práctica, en lugar de recoger todos los posibles "usos de trámite", se describen con términos tan amplios que prácticamente admiten cualquier uso posible de los datos.

finalidades diferentes, siempre que sean "compatibles". Tal y como afirma COLES, T.R[22]., "(…) la *Privacy Act* ha favorecido el deseo de información del Gobierno a expensas de la privacidad individual. En ningún sitio es más evidente esta tendencia que en la exención del uso de trámite" la cual ha sido utilizada por las agencias federales para revelar información sin consentimiento del individuo.

La Ley habla de "registros"[23] (*records*) y "sistema de registros" (*systems of records*). Teniendo en cuenta que la Ley se aplica a los registros que están contenidos en sistemas de registros, significa que para que la Ley se aplique, una agencia debe obtener los registros realizando una búsqueda por el nombre u otro identificador y no simplemente tener la capacidad de hacerlo. Tal y como puso de manifiesto[24] la Comisión de Estudio de la protección de la privacidad creada por la propia Ley (*Privacy Protection Study Commission*) sólo tres años después de la aprobación de la misma, la consecuencia de esta distinción es la total exclusión del ámbito de aplicación de la Ley de aquellos registros que no son obtenidos por el nombre u otro identificador personal. La Comisión ya recomendó en 1977 eliminar la definición de "sistema de registros" y modificar la definición de "registro". La *Privacy Act* modifica la *Freedom of Information Act* (FOIA), en el sentido de que el Gobierno federal podrá negar el

---

[22] COLES, TODD R., "Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption", *The American University Law Review*, vol. 40:957, p. 1001.

[23] Sección 552 a) de la *Privacy Act*, puntos 4 y 5. Registro "cualquier elemento, combinación, o agrupación de información acerca de un individuo (…) y contuviere su nombre o símbolo de identificación u otro detalle de información (…) como una huella dactilar, grabación sonora o fotografía. "Sistema de registros" grupo de registros sujetos al control de un órgano, del cual se recuperare información a partir del nombre del individuo o de algún número o símbolo de identificación … atribuido al individuo".

[24] The Privacy Act of 1974: An Assessment. Appendix 4 to the Report of the privacy protection study Commission. Chapter 4, Revision of the Privacy Act, "Records" and "systems of records" 01/07/1977. Disponible en https://aspe.hhs.gov/report/privacy-act-1974-assessment-appendix-4-report-privacy-protection-study-commission

acceso a determinados archivos cuando suponga una invasión injustificada en la información personal de un individuo.

Hemos visto cómo la *Privacy Act* establece el derecho de todo ciudadano americano a solicitar acceso a los datos que el gobierno federal mantenga sobre su persona. En 1974 se aprueba la Ley Federal de Derechos Educativos y Privacidad Familiar (***The Family Educational Rights and Privacy Act*, FERPA**), que protege la privacidad de los expedientes académicos[25] y otorga a los padres determinados derechos (por ejemplo, derecho a acceder al expediente académico, a obtener una copia, y a limitar el acceso al mismo) en relación a los expedientes académicos de sus hijos. Es de aplicación en las escuelas públicas o estatales y locales que reciben fondos federales. Estos derechos se transfieren a los propios estudiantes una vez han cumplido dieciocho años. Las leyes estatales pueden complementar lo establecido en la FERPA, pero las escuelas además deberán cumplir lo establecido en la ley federal. A pesar de que se exige como regla general el consentimiento de los padres para revelar información personal del estudiante, la FERPA permite divulgar aquella información designada como "información de directorio"[26], que incluye nombre, dirección, teléfono, lugar y fecha de nacimiento, área de especialización académica, participación en actividades oficiales y deportivas, peso y altura de los miembros de equipos deportivos, títulos y premios recibidos, fotografías etc. Para ello, la escuela deberá comunicar previa y públicamente los datos que forman parte de la "información de directorio" y el plazo que los padres tienen para oponerse. Cabe resaltar que la FERPA permite utilizar dichos datos para propósitos comerciales. La escuela deberá informar (no individualmente) anualmente a los padres de los derechos que la ley les otorga.

---

[25] Cfr DAGGETT, LYNN M., "FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students", 58 *Cath. U. L. Rev.* 59 (2009). Disponible en: http://scholarship.law.edu/lawreview/vol58/iss1/4

[26] Sección 5 (A) de la FERPA.

Resulta muy criticable el hecho de que en 2002 el Tribunal Supremo estableció[27] que las reclamaciones por violación de la FERPA no podían fundamentar una reclamación basada en la sección 1983 de la Ley de derechos civiles (*Civil Rights Act*), mecanismo precisamente pensado para reparar cualquier presunta privación de los derechos federales constitucionales y estatutarios bajo pretexto de cumplimiento de una ley estatal, ya que la FERPA no crea derechos personales cuyo cumplimiento se pueda exigir. Nos preguntamos entonces para qué sirve.

En 1978 se aprueba la Ley de Vigilancia de Inteligencia extranjera (***Foreign Intelligence Surveillance Act*, FISA**). Se trata de una ley federal que establece los procedimientos para la vigilancia, tanto física como electrónica, y la recopilación de información en relación a la "inteligencia extranjera". Hasta entonces, las labores de vigilancia y escucha se realizaban sin orden judicial, únicamente autorizadas por el Presidente de los EEUU. Se produjeron muchos abusos, pues amparándose en razones de "seguridad nacional", se realizaron escuchas[28] que involucraban a ciudadanos americanos. Para evitar estos abusos y para regular las actividades de vigilancia relacionadas con la seguridad nacional, se aprobó la FISA. Esta ley no se aplica a la vigilancia de ciudadanos americanos, ya que se exige una orden judicial basada en la causa probable de que se está cometiendo o se ha cometido un delito, en aplicación de la *Omnibus Crime Control and Safe Streets Act* de 1968. Título III.

La ley se creó para establecer un control judicial y del Congreso, sobre las actividades de vigilancia llevadas a cabo dentro de los EEUU, sobre entidades o personas extranjeras. La Ley permitía la

---

[27] En Gonzaga Univ. v. Doe 536 U.S. 273 (2002).

[28] El *Church Committee*, en referencia a su presidente el Senador Frank Church, o Comité Selecto del Senado de los Estados Unidos para el Estudio de las Operaciones Gubernamentales Respecto a las Actividades de Inteligencia, creado en 1975, emitió 14 Informes sobre las actividades relacionadas con la Inteligencia, y puso de manifiesto que tanto la CIA como el FBI habían llevado a cabo actividades de espionaje en violación de los derechos constitucionales de los ciudadanos americanos.

vigilancia, sin orden judicial y con independencia de la existencia de causa probable de que se ha cometido un crimen, de hasta un año, salvo que el contenido de la vigilancia interceptase comunicaciones en las que formara parte un estadounidense, en cuyo caso sería necesaria una orden judicial en un plazo no inferior a 72 horas. Se crea un Tribunal de Vigilancia de Inteligencia extranjera (FISC, *Foreign Intelligence Surveillance Court*) el cual supervisa las solicitudes de órdenes de vigilancia de las agencias federales, contra agentes de inteligencia extranjeros, dentro de los EEUU. A pesar de que las operaciones de vigilancia llevadas a cabo según la FISA deben tener un propósito de inteligencia, la información obtenida puede utilizarse en los Tribunales penales. No obstante, se aplicarían los "procedimientos de minimización[29]" para evitar que las

[29] 50 U.S. Code § 1801 –Definitions h) "Minimization procedures", with respect to electronic surveillance, means—.
(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

investigaciones criminales (ordinarias) se beneficien de las facultades que otorga la FISA.

La modificación más relevante desde su aprobación en 1978, fue en 2001 mediante la conocida como Ley patriótica (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act-Patriot Act).

Antes, en 1986 se aprueba la Ley de Privacidad de Comunicaciones Electrónicas (ECPA, ***Electronic Communications Privacy Act***[30]), que extiende su aplicación a las comunicaciones electrónicas (correo electrónico y "otras comunicaciones electrónicas") ya que hasta entonces, la regulación sobre escuchas o vigilancia se aplicaba únicamente a las comunicaciones orales o mediante micrófonos. Antes de la *Patriot Act*, para obtener una orden judicial, la FISA exigía que "el propósito[31] de la vigilancia sea obtener información sobre inteligencia extranjera"; tras la modificación operada por la Patriot Act, sólo se exige un "propósito relevante o principal[32]" (*significant purpose*) en obtener información sobre inteligencia extranjera, lo cual ha sido criticado por un sector de la Doctrina americana por suponer una ampliación de los poderes de investigación. No obstante, el FISCR[33] (*Foreign Intelligence Surveillance Court of Review*) manifestó su legalidad siendo conforme por tanto con la Cuarta enmienda.

Volviendo a los años 70, se aprueba la Ley de Agencias de informes de crédito (***Fair Credit Reporting Act)***. Se aprobó para evitar los errores y abusos que los informes de crédito que manejan las Agencias de informes, podían provocar, otorgando a los ciudadanos derecho a acceder a sus archivos, impugnar inexactitudes en los mismos o demandar por daños sufridos a causa de incumplimientos de la FCRA,

---

[30] 18 US Code, Chapter 119, 121, 206.

[31] A pesar de que en el texto de la FISA no se especifica que el propósito de vigilancia ha de ser principal, la Jurisprudencia americana lo ha interpretado como "*primary purpose*".

[32] 50 U.S.C. § 1804(a)(6)(B) "that a significant purpose of the surveillance is to obtain foreign intelligence information".

[33] Sealed Case No. 02-001, 310 F 3d 717 (2002).

aunque con la importante limitación de que sólo puede demandarse durante los dos años siguientes a la aparición de la responsabilidad.
También en 1970 se aprueba la **Ley de Secreto Bancario (*Bank Secrecy Act o* *Currency and Foreign Transaction Reporting Act*)**, cuyo principal objetivo era reducir el fraude fiscal y otros crímenes de "guante blanco". Se impuso a las entidades bancarias y financieras la obligación de conservar la información sobre determinadas operaciones y reportar a las autoridades. No obstante, el blanqueo de capitales no fue delito federal hasta 1986, con la aprobación de la Ley de Control de Lavado del dinero (*Money Laundering Control Act*). Lo cierto es que esta Ley ha sido muy criticada pues permite al Gobierno y sus agencias, sin orden judicial, acceder a todos los datos bancarios de un individuo.
En 1978 se aprueba la ley Federal ***Right to Financial Privacy Act (RFPA[34]),*** que viene a remediar el hecho de que los clientes de una entidad bancaria no tenían derecho a la privacidad sobre su información financiera, tal y como se puso de manifiesto en la sentencia del Tribunal Supremo *United States v Miller*[35], pues, se afirmaba que, el interesado no tenía una razonable expectativa de privacidad ya que la Cuarta Enmienda no protege la obtención de información revelada a una tercera persona y transmitida por ésta a las Autoridades. Así, con la RFPA se exige que las Agencias Federales notifiquen previamente a los interesados la solicitud de información y así puedan oponerse a que una institución financiera revele su información. Esta Ley únicamente se aplica al Gobierno y Agencias Federales, y por tanto no a los negocios privados, o gobiernos locales y estatales. El concepto de "instituciones financieras" en este ámbito es entendido de manera amplia, llegando a cubrir a aquellas entidades que sin ser propiamente instituciones financieras, expiden tarjetas de crédito. En 2001 la *Patriot Act* modificó la RFPA permitiendo la revelación de información financiera a cualquier Agencia de inteligencia en relación a investigaciones relacionadas con terrorismo

[34] 12 U.S. Code Chapter 35.
[35] *United States v. Miller*, 425 U.S. 435 (1976).

internacional. Existen además otras excepciones[36] en la norma, en las que no será necesaria una orden judicial para acceder a la información.

En 1980 se aprueba la ***Privacy Protection Act (PPA[37]),*** para proteger a los periodistas principalmente, de tener que facilitar sus fuentes e información sobre una noticia (sobretodo las relacionadas con hechos criminales), antes de que sea comunicada al público, pues les protege la Primera Enmienda. Es necesario ponernos en contexto, pues dos años antes, en *Zurcher v. Stanford Daily*[38] el Tribunal Supremo estableció que la Cuarta Enmienda no prohibía la realización de registros si las autoridades tenían causa probable para creer que podrían encontrar pruebas de un crimen. Así, la PPA vino a superar lo dicho por el Tribunal Supremo en *Zurcher v. Stanford Daily,* pues se exige una citación (*subpoena*) para obtener los materiales que supuestamente contengan información de interés policial, impidiendo los registros como regla general.

En 1984 se aprueba la Ley Federal de política de comunicaciones por cable, ***Cable Communications Policy Act (CCPA[39])***, cuyos objetivos eran establecer una política nacional en relación al servicio del cable, así como las directrices para la regulación estatal, federal y local del servicio, entre otras cosas. A este respecto, destacar que incorpora las *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, y de este modo, las compañías de cable deben informar por escrito[40] en el momento de contratación, y una vez al año durante los años sucesivos, sobre la recogida y uso de información personal ("*personal identifiable information*-PII"). Señalar que, en los casos en que fuera de la regla general que requiere el consentimiento previo del usuario para la revelación de la información, y por tanto se permite la comunicación de datos (PPI),

[36] 12 U.S. Code Chapter 35, § 3413.
[37] 42 U.S. Code Chapter 21ª.
[38] 436 U.S. 547 (1978).
[39] 47 U.S. Code Subchapter V–A.
[40] 47 US Code § 551 (a) (1).

tampoco se podrá facilitar información que revele, directa o indirectamente, los usos del servicio realizados por parte del usuario[41].
En 1988 se aprueba la ***Computer Matching and Privacy Protection Act, CMPPA*** [42]. Anteriormente vimos cómo la Ley de Privacidad de 1974 daba carta de naturaleza al "uso de trámite" (*routine use*[43]), legitimando por tanto usos compatibles de los datos, aunque fueran diferentes a las finalidades por las cuales éstos fueron obtenidos. El Gobierno Federal y sus agencias se apoyaron precisamente en esta "excepción" para realizar análisis y comparaciones y así obtener posibles conductas de fraude o abuso entre los funcionarios. Esta postura fue muy criticada por la Doctrina[44], pues viola el Principio del consentimiento o de que el individuo pueda ejercer un control sobre sus datos. Así pues, se aprueba la *Computer Matching and Privacy Protection Act* en 1988, dotando de un procedimiento a esta práctica y otorgándole legitimidad.
Ese mismo año también se aprueba la ***Employee Polygraph Protection Act EPPA[45],*** que prohíbe la utilización de pruebas de polígrafo en el sector privado, aunque admite determinadas excepciones. La Ley no se aplica al sector público.
También en 1988 se aprueba la ***Video Privacy Protection Act[46],*** que prohíbe revelar PII (*personally identifiable information)* en relación al consumidor.
Durante los años 90, en pleno auge de internet, se aprueban numerosas leyes dada las nuevas situaciones creadas para la privacidad. Así en 1991 se aprueba la ***Telephone Consumer Protection Act[47]*** que permite solicitar a las empresas de telemarketing, no recibir llamadas comerciales (*opt-out*). En 1994 se aprueba la ***Driver's Privacy***

---

[41] 47 US Code § 551(c)(2)(C)(ii).
[42] 5 US Code § 552ª.
[43] ver nota al pie 21 del presente Capítulo.
[44] Ver SHATTUCK, JOHN, "Computer matching is a serious threat to individual rights", *Communications of the ACM*, Junio 1984, Volumen 27, Número 6, pp. 538-541.
[45] 29 US Code, Chapter 22, § 2001 to 2009.
[46] 18 US Code, Chapter 121, § 2710-11.
[47] 47 US Code, §227.

Protection Act*[48]*, DPPA, prohíbe el uso y revelación por parte de cualquier Estado de información personal en relación a los vehículos de motor, salvo consentimiento previo expreso del interesado. Durante años, los Estados habían estado vendiendo esta información a empresas de marketing. Se argumentó que la Ley violaba los principios del Federalismo, pero el Tribunal Supremo estableció que la Ley es una manifestación de la autoridad del Congreso en relación a la regulación del comercio entre estados.

En 1996 se aprueba la Ley federal de Portabilidad y Responsabilidad de Seguro de Salud***-Health Insurance Portability and Accountability Act***[49]***, HIPAA***, primera ley federal que protege la privacidad de los datos relacionados con la salud, aunque no entró en vigor hasta 2003. Un aspecto muy criticado, con toda la razón, de esta Ley, es que si la información médica no es obtenida por un "proveedor de servicios de salud" (*health care provider*) tal y como se define en la ley, quedaría fuera del ámbito de protección de la HIPPA, por lo que podemos decir que no existe un estándar de protección para los datos relativos a la salud.

En 1998 se aprueba la ***Children's Online Privacy Protection Act***[50] (COPPA), que como su propio nombre indica, regula el tratamiento de datos en internet de los menores de 13 años, siendo necesario publicar políticas de privacidad y el consentimiento paterno para su recogida y utilización. La Ley se aplica a páginas web comerciales o servicios en línea, dirigidos a menores, sean americanas o no.

En este punto, cabe destacar el papel de la Comisión Federal de Comercio (*Federal Trade Commission*, FTC) ya que la ley que rige su actividad le otorga competencia para demandar civilmente cuando se produzcan actos o prácticas injustas o engañosas que afecten al comercio. La FTC entiende que éstas prácticas se producen cuando se vulnera lo establecido en una política de privacidad.

En 2003 se aprueba la Ley de Transacciones de crédito Justas y Exactas-***Fair and Accurate Credit Transactions Act*** FACTA, que

---

[48] 18 US Code, Chapter 123, §2721-25.
[49] 42 US Code § 1320d–6.
[50] 15 US Code, Chapter , § 6501-06.

reforma la Ley de Información de crédito justa-*Fair Credit Reporting Act* FCRA de 1970, primera ley federal que reguló el uso de información personal en el sector privado.

La FACTA principalmente busca luchar contra el robo de identidad, pero además protege la información financiera de los consumidores, como los informes de crédito o la información relativa a sus cuentas bancarias . Así, las tres principales agencias de crédito deben emitir una vez al año un informe sobre el crédito del usuario de manera gratuita, de modo que el consumidor pueda verificar si hay datos incorrectos u operaciones no autorizadas. Las víctimas de robo de identidad o fraude sólo deberán avisar a una de las agencias de crédito, que deberá informar al resto y así colocar una "alerta de fraude" en sus informes. Por otro lado, se obliga a que los recibos de las transacciones realizadas con tarjeta bancaria, no incluyan el número de cuenta completo. En los informes ni el número de la Seguridad Social.

También en 2003 se aprueba la *Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 o* ***Can Spam Act***[51]. Esta Ley regula el envío de correos electrónicos de carácter comercial, no únicamente los correos no solicitados. En primer lugar, no se prohíbe el spam, o correo comercial no solicitado, sino que se establecen las bases sobre cómo realizarlo legalmente, y debe ofrecerse al usuario la posibilidad de solicitar no recibir este tipo de información (*opt-out*). Abarca no sólo los correos enviados al consumidor persona física sino también a aquellos correos enviados a cuentas corporativas. Para considerar un email como de carácter comercial, y por tanto, bajo la aplicación de la *Can Spam Act,* el principal propósito de éste ha de ser comercial. Existen determinadas excepciones en la Ley, como por ejemplo aquellos correos electrónicos que se dirijan al consumidor para completar o confirmar una transacción comercial, proveer determinada información sobre el servicio contratado etc. Si un email tuviera varias finalidades (comerciales y no comerciales) para saber si estamos ante un email de

[51] 15 US Code § 7701-13.

"carácter comercial" o bien se aplica una de estas excepciones o deberemos atender a la finalidad *principal (primary purpose)*. Los mensajes comerciales deben incluir una clara identificación de su carácter comercial y la dirección postal del remitente.

Respecto al mecanismo para que el destinatario pueda solicitar la exclusión (*opt ut*), la Ley establece que deberá ofrecerse la posibilidad de enviar un email solicitándolo, o bien cualquier otro mecanismo basado en internet. No podrá solicitarse ningún tipo de cantidad económica por ello, obligar a utilizar mecanismos más allá del envío de un email o visitar una página web para solicitar la exclusión, o exigirle determinada información adicional diferente a la dirección de email o preferencias en relación a la exclusión. La exclusión debe tener efecto en un plazo de 10 días hábiles.

Existen restricciones adicionales para los mensajes comerciales de carácter sexual como por ejemplo que debe especificarse en el asunto del mensaje su carácter "sexual" incluyendo las palabras "sexually explicit" en mayúsculas o que el contenido del mensaje no sea visible en un primer momento por el receptor.

La Ley habilita a la *Federal Communications Commission* (FCC) a regular las comunicaciones realizadas a dispositivos inalámbricas; así, la FCC ha establecido la regla de la autorización expresa (*opt in*) para el envío de comunicaciones comerciales a determinadas direcciones de correo electrónico facilitadas por los operadores de servicios inalámbricos. La Federal Trade Commission (FTC) es el órgano principal para hacer cumplir e imponer sanciones bajo la *Can Spam Act*, pero la Ley también otorga dicha capacidad a otras agencias, federales o estatales, o entidades privadas, en función de la concreta actividad o sujeto infractor. Las sanciones pueden ser civiles o penales.

También en 2003 se aprueba la ***Do not call implementation Act*** [52] a través de la cual se habilita a la FTC a crear a nivel nacional una lista robinson ("do-not-call registry" o Registro nacional no llame, https://www.donotcall.gov) en relación a las llamadas telefónicas de

[52] 15 US Code § 6151-55.

carácter comercial, donde las personas pueden inscribirse voluntariamente, y las empresas deben consultar con carácter previo a la realización de las campañas.

En conclusión, vemos cómo se han aprobado multitud de normas a nivel federal tendentes a proteger la información personal en diferentes sectores, pero que suponen una protección sectorial y fragmentaria, poniendo en evidencia la falta de un derecho expresamente reconocido a la privacidad de la información o a la protección de datos de carácter personal.

Por último, y para completar la evolución del derecho a la privacidad en EEUU, no podemos dejar de mencionar el importante papel que juega la FTC. Siguiendo a SCHWARTZ[53], la Jurisprudencia de la FTC se basa en cinco pilares: 1) la protección contra las "promesas sobre privacidad incumplidas", ya que el incumplimiento por una empresa de lo establecido en su política de privacidad supondrá una práctica fraudulenta o acto desleal en el sentido de la Ley de la Comisión de Comercio Justo de 1914; 2) la promoción de la transparencia, pudiendo constituir un acto fraudulento la difusión no adecuada de la política de privacidad; 3) la exigencia de una seguridad adecuada de los datos, en casos de filtración de datos o incluso cuando la empresa no ha formado adecuadamente a sus empleados en materia de privacidad y seguridad; 4) el requerimiento a las empresas que utilicen la información personal que desarrollen un "programa integral sobre privacidad"; y 5) la petición del "consentimiento expreso" a cualquier usuario antes de que la empresa cambie las prácticas declaradas y proceda a efectuar una divulgación nueva o adicional de la información personal del usuario (inclusión limitada).

Siguiendo a SCHWARTZ [54], a pesar del reforzamiento que ha supuesto el papel de la FTC respecto de la privacidad online en EE.UU., adolece de ciertas limitaciones. Respecto a la política de promesas

---

[53] SCHWARTZ P. M., "Privacidad online: planteamientos jurídicos en EE.UU. y Europa", en *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados,* Fundación Telefónica, Cuaderno 36, Ariel, 2012, p. 61, CC BY NC-SA 3.0.

[54] SCHWARTZ P. M., *op. cit.,* p. 64.

rotas, basta que las empresas no prometan demasiado o sus políticas sean demasiado vagas como para dificultar valorar si ha habido un incumplimiento o no. Además, muchas empresas no recaen dentro del ámbito de aplicación de la FTC, como las entidades financieras, líneas aéreas y operadores de telecomunicaciones. Por último, la FTC es la única que puede hacer cumplir la Ley ya que la FTC Act no contempla fundamentos de demandas privadas.

1.3. *Informational privacy*: el derecho a la protección de datos en EE.UU.

Anteriormente hemos visto cómo el "control de la información personal", forma parte del concepto de privacidad americano. Podríamos pensar que incluye lo que en Europa hemos conceptualizado como derecho fundamental a la protección de datos, pero veremos cómo no se tratan de conceptos puramente equivalentes.

La teoría predominante en la doctrina americana[55], sostiene que control de la información personal implica la capacidad de un individuo de controlar la información que se comunica a los demás sobre su persona. WESTIN define la privacidad como el derecho de los individuos, grupos o instituciones para decidir por ellos mismos cuándo, cómo y hasta que punto se comunica a otros información relacionada con ellos; FRIED sostiene que la privacidad no es simplemente la ausencia de información sobre nosotros en la mente de los demás, sino que es el control que tenemos de la información sobre nosotros.

Otros autores[56], consideran que la teoría del "control de la privacidad" no resulta adecuada para conceptualizar la "privacidad" y tienen

---

[55] WESTIN, A., *Privacy and Freedom*, Atheneum, New York, p. 7; FRIED, Ch., Privacy en *Philosophical dimensions of privacy*, Cambridge University Press, 1984, Ferdinand David Schoeman, p. 209.

[56] Vid. MOOR, J. H., "The Ethics of Privacy Protection", *Library Trends*, vol. 39, n. 1 y 2, Verano/Otoño 1990, pp. 74 y 75.

razón, aunque no precisamente por sus argumentos, en el sentido de que si partimos de un amplísimo concepto de privacidad, no cabe identificar la parte (control de la información) con el todo (derecho a la protección de datos, derecho a la intimidad, honor e imagen). En este sentido, SOLOVE[57] sostiene, muy acertadamente, que la teoría del control sobre la información excluye aquellos aspectos no informacionales de la privacidad.

Además, como podemos ver en la definición de WESTIN, no se identifica privacidad con persona física sino que también cabe predicarse de un grupo o institución, a diferencia de la concepción europea de los derechos relativos a la personalidad.

En realidad, todos los intentos realizados por la Doctrina americana de dar con un concepto de "privacidad" son, digamos en términos generales, correctos (a la par que estériles), porque cada definición describe los diferentes derechos que bajo el término privacidad se protegen en EEUU. La teoría del control de la información personal, no es sino el equivalente del derecho a la protección de datos de carácter personal, que en sus orígenes, como vimos en el primer capítulo del presente trabajo, aparecía ligado o incluido en el derecho a la intimidad, hasta que alcanzó sustantividad propia.

1.3.1 Dato personal vs *informational privacy*

En el segundo capítulo del presente trabajo se comentó ampliamente del concepto de dato de carácter personal. Veamos ahora cómo el Derecho americano aborda dicho concepto de "*informational privacy" o privacy of autonomy o Personally Identifiable Information (PII).*

Actualmente no existe una definición de "*personally Identifiable Information*" (PII) o información personal[58], ni las categorías de datos

---

[57] SOLOVE, D. J., *op. cit.*, "Conceptualizing Privacy", p. 1110.

[58] SCHWARTZ, PAUL M. y SOLOVE, D. J., señalan que desde mediados de los años 90, PII es el término legal específico más utilizado, Vid *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q.

que incluye, a pesar del auge de esta categoría dentro del Derecho relativo a la privacidad. Ni siquiera la primera Ley Federal que utiliza dicha acepción, la *Family Educational Rights and Privacy Act* FERPA de 1974, ofrece una definición del concepto[59].

La *Privacy Act* tampoco ofrece una solución razonable, como se puso de manifiesto anteriormente[60], al hablar de "records" and "systems of records" y excluir de su ámbito de aplicación a aquellos registros que no son obtenidos a través del nombre u otro identificador personal.

La *Cable Communications Policy Act (CCPA)* por primera vez, tal y como señalan SCHWARTZ y SOLOVE,[61] utiliza el concepto de PII como elemento que supone la aplicación de la Ley, con independencia de cómo la información sea guardada o archivada por las compañías. Es decir, es el uso de PII lo que determina la aplicación de la norma. Tal y como afirman SCHWARTZ y SOLOVE[62], "dada la importancia de la PII, es sorprendente que el Derecho de la privacidad de la información en los EE.UU. carezca de una definición uniforme del término". La importancia del concepto radica en que aquellos datos que sean considerados PII quedarán protegidos por la normativa, a diferencia de los que no.

A finales del siglo XIX, cuando WARREN y BRANDEIS publicaron su famoso artículo en defensa del reconocimiento a la privacidad, así como la Jurisprudencia subsiguiente, el concepto de PII no existía ni

---

Rev. 1814 (2011), Disponible en: http://scholarship.law.berkeley.edu/facpubs/1638 , p. 1827.

[59] El problema de la FERPA en relación al concepto de PII, tal y como ponen de manifiesto SCHWARTZ, PAUL M. y SOLOVE, D. J, *op. cit*., pp. 1822-3, es que a pesar de utilizar la acepción de PII, el concepto central de la Ley es "*educational records*", definidos como aquella información directamente relacionada con un estudiante que una institución educativa mantiene en sus archivos o ficheros, de modo que, toda aquella información relativa a los estudiantes pero que no se encuentre en los "archivos educativos" caerá fuera del ámbito de aplicación de la FERPA. Esta situación fue solventada parcialmente, permitiendo un *opt-out* a los padres respecto al uso de los datos de sus hijos para propósitos comerciales.

[60] Ver nota al pie 167 del Capítulo II.

[61] SCHWARTZ, P. M. y SOLOVE, D. J., *op. cit.,* p. 1825.

[62] SCHWARTZ, P. M. y SOLOVE, D. J, *op. cit.,* p. 1816.

era tenido en cuenta ya que se partía de la premisa que la información personal siempre era relativa a una persona concreta, identificada.
A pesar de que en su propia acepción se menciona la palabra "identificable", no queda claro si la información ha de ser relativa a una persona identificada o también identificable. Una interpretación literal, sugiere una respuesta afirmativa, de modo que la información que puede llegar a identificar a una persona, quedaría dentro de esta categoría.
En Europa tenemos una definición[63] clara de "dato personal" siendo "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". En este sentido, P. M. SCHWARTZ y D. J. SOLOVE hablan[64] de una visión expansiva del concepto en Europa, y una visión reduccionista del concepto de PII en EE.UU., y proponen una solución intermedia a través de la creación de una nueva categoría que denominan "PII 2.0", basada en dotar de diferente regulación a los diferentes conceptos de datos identificados o datos identificables, dado el diferente riesgo que, en su opinión, entraña cada categoría.

1.3.2 Concepto FTC dato personal

Por su parte, la FTC[65], aunque no da una definición del concepto, se basa en el concepto de "identificabilidad razonable". Así, en un

[63] artículo 4.1 del RGPD.
[64] SCHWARTZ, P. M. y SOLOVE, D. J., *op. cit.*, p. 1817.
[65] La *Federal Trade Commission*, FTC, es una agencia independiente encargada de regular la competencia y realizar la defensa de los consumidores, completando así la protección dada por las leyes federales y estatales en materia de privacidad. Así, tiene autoridad para hacer cumplir diferentes leyes federales (*The Truth in Lending Act, CAN-SPAM Act, Children's Online Privacy Protection Act, Equal Credit*

Informe de Marzo de 2012[66] realizado para servir de base a la futura normativa que se apruebe en materia de privacidad en los EE.UU., la FTC es consciente de la posibilidad de re-identificación, a partir de conjuntos de datos que objetivamente no contienen PII.

En este momento es necesario realizar una puntualización, y como analizaremos más adelante, realmente hay dos debates que de hecho se están solapando. En primer lugar, en EE.UU., ante la ausencia de una definición legal de qué se entiende por dato personal o PII, se debate si los datos relativos a personas identificables han de recaer en esta definición. En Europa este debate está superado, pues la definición legal de dato personal incluye ambos supuestos. En segundo lugar, y éste es el punto en el que ahondaremos más adelante en el presente trabajo, nos planteamos si, datos que en un primer momento no pueden asociarse a una persona y por tanto, no son relativos a una persona "identificable", pueden llegar a caer dentro de la definición de dato personal gracias a los avances técnicos actuales o futuros, especialmente, el *big data*. Este segundo debate, a diferencia

---

Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act) , y ha impulsado prácticas de autorregulación en el sector de la privacidad, las cuales no han resultado ser muy efectivas dado que no se trata de normas de obligado cumplimiento. Realiza una importante labor divulgativa y de formación, y emite Informes y Recomendaciones para las empresas y el poder legislativo. La FTC también tiene la autoridad para desarrollar reglas (*Rules*) que regulen áreas específicas en materia de privacidad y seguridad de los consumidores. Las principales actuaciones de la FTC en privacidad y seguridad de los datos durante el año 2015 pueden consultarse en https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf

[66] FTC Report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Marzo 2012, p 18-22 disponible en https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf y su Resumen ejecutivo en castellano en https://www.ftc.gov/sites/default/files/documents/reports/cómo-proteger-la-privacidad-de-los-consumidores-en-una-era-de-cambio-veloz-recomendaciones-para/120326privacyreport_es.pdf

del primero, también concierne a los ciudadanos europeos y fundamenta el presente trabajo.

La FTC propone el "*reasonable linkability standard*" o estándar de la enlazabilidad razonable, ya que considera que hay pruebas significativas que demuestran que a partir de diferentes conjuntos de datos, puede llegar a identificarse al consumidor o terminal, incluso si los datos aisladamente considerados no constituían PII, y por tanto, el marco propuesto se aplicará a datos que razonablemente (*reasonable effort*) puedan vincularse a un consumidor, ordenador o aparato específico. Es decir, se utiliza el mismo criterio que en Europa. Como se pone de manifiesto en el Informe de la FTC de Marzo de 2012 anteriormente mencionado, se ha criticado la vaguedad del estándar propuesto por la FTC ("*reasonable linkability standard*") y por tanto la dificultad de llevarlo a la práctica.

Para clarificar su aplicación y dotar de una mayor seguridad a las empresas que recogen y tratan datos de consumidores, la FTC propone determinados supuestos en los que no se considerarán "razonablemente enlazables" ("*reasonably linkable*"), y por tanto, no se aplicará la normativa propuesta, cuando una empresa adopte las siguientes tres medidas:

1. adopte medidas razonables para asegurar que los datos sean pseudoanonimizados (*de-identified*).

Según la FTC, significa que la empresa debe alcanzar un nivel razonable de confianza justificada, de que los datos no se podrán utilizar para inferir información o ligarlos a una persona, ordenador o aparato, lo que dependerá de las concretas circunstancias del caso, y el estado de la tecnología.

2. públicamente se comprometa a no tratar de re-identificar los datos.

La empresa se ha comprometido públicamente a mantener y tratar los datos pseudonanonimizados67 y a no tratar de re-identificarlos. En

[67] En el informe de la FTC de Marzo de 2012, se utiliza la expresión *de-identified*, que traduciremos como *pseudonanimizados*, ya que el texto no ha utilizado la palabra *anonymise* y además porque es posible la reidentificación en este caso concreto.

caso contrario, la FTC tendría competencia sancionadora según la Sección 5 de la Ley de la FTC (FTC Act).

3. contractualmente prohíba a los destinatarios intentar la re-identificación de los datos.

En caso de que la empresa permita el acceso de terceras empresas (proveedores o cualquier otra entidad) a la base de datos pseudoanonimizada, deberá prohibir a través de un contrato, cualquier intento de re-identificación por parte de estos terceros. Además, la empresa deberá realizar una supervisión razonable del cumplimiento de lo establecido en el contrato.

Además, debe añadirse un supuesto que también quedará fuera de la aplicación de la normativa propuesta, respecto de aquellas empresas que solamente recojan datos no sensibles de menos de 5.000 consumidores por año y no lo compartan con terceras partes.

Por tanto, a través de la posición adoptada por la FTC en relación al concepto de PII, podemos hacernos una idea del posible posicionamiento que adopten futuras normas americanas en materia de privacidad.

Anteriormente mencionamos que SCHWARTZ y SOLOVE abogaban, en un artículo anterior al Informe comentado de la FTC de Marzo de 2012, por dotar de una diferente protección jurídica a los datos identificados (PII) y a los identificables (non PII), si bien es cierto que en el Informe preliminar de la FTC de Diciembre de 2010[68] se mantenía la misma postura de incluir dentro del marco legislativo propuesto, no sólo a aquellas empresas que recojan PII, sino también a aquellas que recojan datos que puedan ser razonablemente enlazados a un específico consumidor, ordenador o aparato.

Para SCHWARTZ y SOLOVE [69] si el concepto de PII se define muy "estrechamente" no podrá proteger la privacidad en el mundo actual

---

[68] Preliminary FTC Staff Report *Protecting Consumer Privacy in an era of rapid change-A proposed framework for businesses and policy makers*, December 2010 disponible en https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf p 43.

[69] *Op. cit.*, p. 1827.

en el que se utilizan modernas tecnologías como la minería de datos o el marketing basado en el comportamiento y si se define de un modo amplio, el Derecho a la privacidad será muy difícil de aplicar. Estos autores defienden que el Derecho a la privacidad tenga unos límites flexibles y coherentes. A pesar de que reconocen[70] que la visión expansiva del concepto europeo de PII está más en línea con la tecnología que la visión reduccionista del concepto imperante en EE.UU., opinan[71] que tratar de modo equivalente las categorías de personas identificadas o identificables supone incluir dentro del concepto de identificables, información anónima o pseudoanimizada. Alegan que sería contraproducente cumplir con todos los requisitos de las *Fair Information Practices* (FIPs) pues supondría, que ante un dato identificable, tendríamos que identificar a la persona para poder cumplir con el derecho de información. Hablan del "círculo vicioso" que transformaría información identificable en identificada. En nuestra visión este argumento no se sostiene, pues debemos situarnos en un paso previo, es decir, que el Responsable del tratamiento (utilizando terminología europea) debe decidir *a priori* si tratará datos personales o no, es decir, si se decide que no se van a tratar datos identificables, y por tanto no se aplicará la normativa de privacidad, la empresa simplemente tendrá que vigilar y controlar una correcta anonimización de carácter irreversible. Es decir, tratar esos datos *a priori* identificables, como anónimos, para evitar la aplicación de la normativa. Obviamente esto no se podrá cumplir en todos los casos, pues puede que en aquel momento no se considerara identificable un dato, pero haya devenido así por la evolución tecnológica, pero si se decidió no aplicar la normativa de protección de datos, simplemente habrá que eliminar esa identificabilidad sobrevenida realizando los controles oportunos, bien ex ante de modo preventivo, bien ex post.
Argumentan[72] también estos autores que si se tratan como equivalentes las categorías de identificado e identificable, las empresas tendrán menos motivos para mantener los datos de la

[70] *Op. cit.,* p .1875.
[71] *Op. cit.,* p. 1876-7.
[72] *Op. cit.*, p. 1883.

manera menos identificable posible. Lógicamente, no se trata de lo que las empresas estén o no dispuestas a hacer, se trata de cumplir con la normativa cuyo fin último es proteger el derecho a la protección de datos de las personas, o *informational privacy*. No obstante, como comentábamos anteriormente, si la empresa tiene claro que no va a recoger datos identificables porque no los quiere o no los necesita, precisamente la no aplicación de la normativa de protección de datos será el incentivo para que los mantengan anonimizados y éste además será un reclamo o ventaja competitiva de cara al interesado, pues supondrá una mayor confianza en la empresa.

En conclusión, no podemos apoyar la visión de SCHWARTZ y SOLOVE ("PII 2.0") por una sencilla razón: precisamente porque si existe un problema en que, datos que *a priori* no son datos personales sobre personas identificadas ni identificables, pueden devenir en una de estas categorías, con mayor motivo deben incluirse en la definición de "dato personal" los datos que actualmente son "identificables". Es decir, existe lo que denominaremos una "zona de riesgo" que no es ocupada por datos relativos a personas identificadas ni identificables, y por tanto, queda fuera del ámbito de aplicación de la normativa sobre protección de datos personales, pero que podría llegar a ser de aplicación. Si somos conscientes de este riesgo, el propósito de un Derecho defensor de la privacidad no puede ir a favor de ninguna teoría que agrande dicha "zona de riesgo", sino todo lo contrario. El hecho de no incluir dentro de la definición de PII la categoría de los datos relativos a una persona identificable, no hace sino agrandar dicha zona de riesgo, por lo que no podemos alinearnos con la interpretación de estos de autores.

Es cierto como ponen de manifiesto estos autores, que no es clara la línea que permite distinguir qué datos pueden ser identificables y no identificables (non-PII), pero con la tecnología actual y la venidera, nunca será clara esta línea, por lo que se trata de una cuestión que siempre dependerá del contexto y de los medios existentes en cada momento. Y esta es precisamente la razón de la existencia de la categoría de datos relativos a personas identificables.

Debemos pensar que el sector privado utilizará todos sus medios para conseguir información relativa a personas concretas, dado su mayor valor, por lo que es necesario que el Derecho prevea estas situaciones y salvaguarde la privacidad de las personas.
Por tanto, en relación al concepto de "dato personal" o *informational privacy* en EE.UU., observamos importantes deficiencias. En primer lugar, la ausencia de un concepto uniforme que deriva de la falta de una norma uniformadora o de general aplicación, que a su vez nos lleva a otra deficiencia, la de no tratar de la misma manera casos similares, pues dependerá del concreto sector en el que nos encontremos y la normativa que le sea aplicable, además de la ubicación geográfica, pues no debemos olvidar la existencia de leyes estatales y locales. Otra deficiencia relacionada con la falta de un concepto uniforme, tal y como apuntan SCHWARTZ y SOLOVE[73] es que a pesar de la utilización del concepto *Identifiable* en el concepto de PII, la mayoría de las normas solamente se aplican a personas identificadas (*identified*), lo cual supone que la "zona de peligro" existente en Europa en relación a los datos a priori "no personales", sea mucho menor que en EE.UU., pues aquí también se incluirían los datos relativos a personas identificables.

2. Ámbito de aplicación de la normativa europea

2.1 Directiva 1995/46 de protección de datos de carácter personal

Profundizaremos en el ámbito de aplicación de la Directiva, en relación a los tratamientos realizados fuera de la UE y los problemas surgidos en cuanto a su aplicación práctica, por ser de especial interés para este trabajo.

---

[73] *Op. cit.*, p. 1873.

El artículo 4 de la Directiva establece que los Estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado **en el marco de las actividades de un establecimiento del responsable** del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y **recurra, para el tratamiento** de datos personales**, a medios**, automatizados o no, **situados en el territorio de dicho Estado miembro**, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

En este caso, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

Por tanto, los criterios principales para determinar la aplicación de la normativa son la ubicación del establecimiento del responsable del tratamiento y, cuando el responsable no se encuentre en la UE, la ubicación de los medios o equipos.

En cuanto al concepto de medios o equipos, el Grupo de Trabajo del artículo 29 (GT29), realiza una interpretación amplia[74] del término "equipos", dado que la noción inglesa de *equipment* se ha traducido en otras lenguas de la UE como *medios*. Como el propio GT29 reconoce

[74] Dictamen 8/2010 sobre el Derecho aplicable, p. 9, nota 11, consultable en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_es.pdf

en el Dictamen 8/2010 sobre el Derecho aplicable, **"**las disposiciones de la Directiva pueden aplicarse a servicios con una dimensión internacional, como motores de búsqueda, redes sociales y computación en nube" .

El primer caso analizado por el artículo 4 a) de la Directiva, tratamiento realizado en el marco de las actividades de un responsable con establecimiento en uno o varios Estados miembros, deberá cumplirse la legislación nacional de cada estado miembro. La Directiva no ofrece una definición de "establecimiento", pero el Considerando 19 nos aclara que el establecimiento en el territorio de un Estado miembro implica el "ejercicio efectivo y real de una actividad mediante una instalación estable" y "que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto", por lo que no es necesario que el establecimiento esté dotado de personalidad jurídica propia, siempre que se realice un ejercicio efectivo y real de una actividad. Tal y como se menciona en el Dictamen 8/2010[75], el Tribunal Europeo de Justicia ha declarado que un establecimiento estable requiere una integración permanente de medios humanos y técnicos necesarios para prestar un servicio, lo cual dejaría en principio fuera del concepto de establecimiento la instalación de equipos en un determinado estado miembro, sin ningún medio humano, sin perjuicio de su consideración como "medios". Por tanto, en el caso de un responsable con establecimientos en diferentes estados miembros, habrá que analizar que el tratamiento se realice *en el marco de las actividades* de dichos establecimientos. Podríamos pensar que debería aplicarse cada una de las legislaciones nacionales donde se ubican los establecimientos, tal y como se afirma en el apartado a) *in fine* del articulo 4 de la Directiva, pero tal y como afirma el GT29 "es importante tener presente una visión global de las actividades de tratamiento: una serie de operaciones realizadas en distintos Estados miembros, pero todas ellas orientadas hacia un único

[75] Dictamen 8/2010, p 13, nota 11, Sentencia del Tribunal de Justicia de 4 de julio de 1985, Bergholz, (168/84, Rec. 1985 p. 2251, apartado 14) y sentencia de 7 de mayo de 1998, Lease Plan Luxembourg/ Belgische Staat (C-390/96, Rec. 1998, p. I-2553).

propósito, pudieran muy bien dar lugar a la aplicación de un único Derecho nacional". Así, siguiendo al GT 29, deberá analizarse el grado de implicación de cada establecimiento en el tratamiento de datos realizado, para determinar o no la aplicación del derecho nacional correspondiente.

Debe tenerse en cuenta que cuando un Responsable de tratamiento recurre a un encargado ubicado en otro país, éste deberá cumplir las medidas de seguridad[76] de dicho país.

Analizaremos ahora el supuesto en que el responsable del tratamiento está fuera de la UE ("no esté establecido") (art. 4.1 c), asumiendo que carece de establecimientos ubicados en la UE, ya que ello desencadenaría la aplicación de la correspondiente legislación nacional del estado miembro en cuestión, tal y como hemos visto anteriormente. En estos casos, cuando el responsable recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, se aplicará la legislación de dicho Estado (exceptuando el caso de que dichos medios se utilicen solamente con fines de tránsito). No obstante, no es necesario que el responsable carezca de establecimiento situado en la UE, sino que ese establecimiento sea relevante en relación al tratamiento de datos en cuestión, es decir, cuando el responsable disponga de un establecimiento en la UE, pero éste no realice actividades relacionadas con el tratamiento de datos, no se considerará dicho establecimiento como criterio de aplicación de la legislación nacional correspondiente.

Tal y como pone de manifiesto el GT29, ambos criterios no son excluyentes, pues podría darse el caso de que un responsable disponga de un establecimiento en la UE y recurra a medios en otro estado

---

[76] Artículo 17.3 Directiva 95/46: "La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste·.

miembro, pero no en el marco de las mismas actividades, mismo tratamiento, sino de diferentes. En este caso, se aplicaría la legislación del estado nacional del establecimiento para el tratamiento realizado en el marco de sus actividades, y la legislación del estado nacional donde se ubiquen los medios a los que el responsable a acudido, para la realización de otro determinado tratamiento, en el marco de otras actividades. Tal y como se ha puesto de manifiesto anteriormente, siguiendo el Dictamen 8/2010, el término "medios" constituye un concepto muy amplio, pues no se limita a ser un equivalente de "equipos", sino que incluye intermediarios humanos y/o técnicos.

Así, el GT29 en el Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, aprobado el 30 de Mayo de 2002, afirmaba[77] que "las condiciones en que pueden recogerse datos personales del usuario mediante la colocación de cookies en su disco duro son reguladas por el Derecho nacional del Estado miembro donde se sitúa este ordenador personal". Por tanto, la recogida de datos personales a través del ordenador/terminal de un usuario, mediante cookies o Javascript, se considera un recurso a medios, y por tanto, resulta aplicable la legislación del estado miembro donde se encuentre dicho terminal.

Si tenemos en cuenta que en el caso del recurso a medios (art 41.c) el responsable deberá ser[78] establecido en el territorio de dicho Estado miembro, un proveedor de servicios situado fuera de la UE pero que preste servicios a clientes de toda Europa, deberá tener un representante en cada uno de los estados miembros.

El GT realiza las siguientes consideraciones respecto a la aplicación práctica del artículo 4.1c):

---

[77] WP 56, p. 11, disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_es.pdf

[78] El GT29 pone de manifiesto la necesidad de armonizar las legislaciones nacionales en relación a la ejecución contra un representante, pues en unos países puede ser declarado responsable y sancionado y en otros en un simple mandatario, y para "dar una mayor efectividad al papel del representante". Vid. WP 179, p. 27.

- si debe aplicarse el derecho europeo a todas las fases del tratamiento, incluyendo el realizado fuera de la UE; el GT29 entiende que sí, en la medida en que el vínculo con la UE sea efectivo y no indirecto
- defiende la inclusión de un criterio que incluya un "factor de conexión más específico que tuviera en cuenta la oportuna orientación hacia las las personas" . Como veremos, este criterio ha sido adoptado por el RGPD.

En lo que respecta a las medidas de seguridad aplicables, el párrafo tercero del artículo 17 establece que en el contrato o acto jurídico que vincule al Encargado con el Responsable, deberán establecerse las medidas técnicas y de organización "tal como las define la legislación del Estado miembro en el que esté establecido el encargado". Dado que como pone de manifiesto el GT29 las medidas de seguridad "difieren considerablemente" entre los estados miembros, aunque no debería ser un problema para el encargado o responsable aceptar por contrato unas medidas de seguridad más concretas, "solo en casos en que las normas detalladas sean diferentes o incluso entren en conflicto, el artículo 17, apartado 3, decide a favor del Derecho del encargado del tratamiento". No obstante, el GT recomienda una armonización en materia de seguridad en el futuro RGPD.

En relación a la competencia de las autoridades de control, a pesar de que la Directiva[79] contempla su competencia para supervisar la aplicación de la legislación de protección de datos en el territorio del Estado miembro donde estén establecidas, dado que pueden surgir interrogantes sobre las concretas competencias, el GT considera esencial la armonización en este aspecto, "para garantizar de una

[79] Artículo 28.6 de la Directiva 95/46 "Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.
Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil".

manera eficaz y no discriminatoria la protección de datos transfronteriza" .

El GT realizó una actualización[80] de la Opinión 8/2010, el 16 de Diciembre de 2015, a raíz de la Sentencia del TJUE en el caso Google Spain, dado que, según afirma, las implicaciones de la sentencia son mayores que simplemente determinar el Derecho aplicable al caso concreto. Además de confirmar el criterio amplio en torno al concepto de "establecimiento"[81], tal y como venía siendo interpretado (Dictamen 8/2010), la Sentencia estableció[82] que "El artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales *en el marco de las actividades* de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro".

Para el GT la Sentencia introduce un nuevo criterio a la hora de determinar el Derecho aplicable: el "vínculo indisociable" (*inextricable link)*. El TJUE afirma en el punto 56 que "las actividades

---

[80] Actualización de la Opinión 8/2010, 16 diciembre de 2015, a la luz de la Sentencia del TJUE en el caso Google Spain, disponible en inglés en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf

[81] apartado 19 de la Sentencia "Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades".

[82] Conclusión 2ª de la Sentencia de 13 de Mayo de 2014, en el asunto C-131/12, disponible en http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están *indisociablemente ligadas (*"*inextricably linked to"*), dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades".

En cuanto a si los datos personales tratados por el motor de búsqueda (Google Inc) se trataban "en el contexto de las actividades de un establecimiento" en un Estado miembro, en relación a la actividad de Google España SL, el Tribunal recuerda que el artículo 4.1 a), no exige necesariamente que el tratamiento de datos en cuestión sea llevado a cabo "por" el propio establecimiento en sí, sino que basta con que el tratamiento se efectúe "en el contexto de las actividades del establecimiento". En relación a la determinación del vínculo indisociable (*inextricable link*) entre las actividades de un establecimiento situado en la UE y el tratamiento de datos por parte de un Responsable situado fuera de la UE, el GT destaca que la Sentencia confirma dicho vínculo indisociable incluso si dicho establecimiento no asume efectivamente ninguna función en el propio tratamiento de datos.

2.2 Reglamento europeo de protección de datos

La aprobación del Reglamento (UE) 2016/679, en adelante RGPD, ha venido a clarificar y simplificar la cuestión de su aplicación a responsables o encargados no establecidos en la UE, que como hemos visto en el apartado anterior, ofrecía dificultades importantes en su aplicación tanto práctica como en su justificación normativa, a pesar de que así se venía considerando tanto por parte del GT como por el TJUE, tal y como se puso de manifiesto en la Sentencia del TJUE de

13 de Mayo de 2014 en el asunto C-131/12 entre Google Spain SL/ Google Inc y la AEPD / Mario Costeja González[83].
A diferencia de la Directiva 95/46, el RGPD distingue entre el ámbito de aplicación material y territorial. Así, en relación al **ámbito de aplicación territorial**, el RGPD (artículo 3.2) se aplica al tratamiento de datos personales de interesados que residan en la Unión, realizado por un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

El Considerando 23 razona esta "ampliación" del ámbito de aplicación en la necesidad de "garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento". Además, tal y como afirma SEMPERE SAMANIEGO[84], "utilizando el elemento territorial se va a ganar seguridad jurídica, ya que anteriormente se tenía que realizar una interpretación para saber si realmente se estaban utilizando medios en territorio de la Unión", y, añadimos la cuestión de interpretar qué Derecho Nacional se aplicaba a dicho tratamiento, en caso de que tuviera lugar en varios estados miembros, resultando por tanto una labor de interpretación bastante compleja.
El Considerando 23 también aclara que para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Este Considerando

---

[83] Disponible en http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

[84] SEMPERE SAMANIEGO, F. J., *Comentarios prácticos a la propuesta de Reglamento de Protección de Datos de la Unión Europea*, Libro publicado mediante licencia *Creative Commons* Reconocimiento-No Comercial-Compartir igual, CC BY-NC-SA, 7 de Septiembre de 2013, p. 46.

23 puntualiza que la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no bastan para determinar dicha intención, sino que debe atenderse a otros factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros; la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que puedan revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

En relación al segundo tipo de tratamientos realizados por responsables o encargados no establecidos en la UE pero que supondrían la aplicación del RGPD, (la observación del comportamiento de residentes en la UE en la medida en que este comportamiento tenga lugar en la Unión), el Considerando 24 aclara que para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, "debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive 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".

Siguiendo a SEMPERE SAMANIEGO [85], lo que parece la ampliación del ámbito de aplicación de la normativa europea, realmente no lo es, sino que, como afirma el autor, lo que se ha producido es una sustitución del "cuando se utilicen medios o equipos en el territorio de la Unión" de la Directiva 95/46, por el de ofrecer productos y servicios vía internet.

Con respecto al ámbito general de aplicación del RGPD, en el caso de responsables o encargados situados en la UE, el artículo 3 en su párrafo primero establece que se aplicará al "tratamiento de datos

[85] SEMPERE SAMANIEGO, F.J., *op. cit.,* pp. 15 y 16.

personales *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".

En este aspecto, vemos cómo se han recogido la mayoría de opiniones dadas por el GT en la Opinion 8/2010 sobre el Derecho aplicable, tal y como se comentó en el punto anterior del presente trabajo.

En relación al **ámbito de aplicación material**, el artículo 2[86] del RGPD establece que "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero". Vemos cómo, a diferencia del artículo 3.2 en el que se refiere expresamente al tratamiento de datos personales de "interesados que residan en la Unión", en este artículo se habla simplemente de la aplicación del RGPD a los "tratamientos" de datos.

---

[86] Artículo 2 del RGPD "1**.** El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15".

El Considerando 14 puntualiza que el RGPD se aplica "a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales". Esta aparente pequeña diferencia, podría conllevar la no aplicación del RGPD a un "no residente" en la UE, cuando se realicen los tratamientos especificados en el artículo 3.2, lo cual es un contrasentido, pues si a cualquier persona física le sería de aplicación el RGPD con independencia de su nacionalidad o lugar de residencia, en el caso de tratamientos de datos más sensibles, no tiene sentido limitar la protección del RGPD a los "interesados que residan en la Unión".

Por otro lado, en relación a los tratamientos manuales, el Considerando 15 concreta el inciso final del artículo 2, afirmando que "la protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento". Por tanto, el tratamiento manual de datos queda limitado a aquellos casos en que los datos se incorporen o vayan a incorporarse a un fichero.

Destacar que el Reglamento (CE) 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de estos datos, seguirá vigente aunque deberá adaptarse a los principios y normas del RGPD, con el fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, tal y como se indica en el Considerando 17.

En relación a la exención doméstica, es decir, al tratamiento efectuado por una persona física en el ejercicio de actividades *exclusivamente* personales o domésticas, el Considerando 18[87] concreta que no deberá

[87] Considerando 18: El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional

haber conexión alguna con una actividad profesional o comercial. Cita como ejemplos de actividades personales o domésticas la correspondencia, la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades.

También quedan excluidos del ámbito de aplicación del RGPD los tratamientos realizados por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención. En este punto, nos remitimos a los comentarios realizados en el Capítulo II, apartado 1.1.4, del presente trabajo.

Por último, y aunque el artículo 2 no lo mencione expresamente, en relación a las actividades de los tribunales y otras autoridades judiciales, el Considerando 20, tras establecer su sometimiento al RGPD, establece que con el fin de preservar la independencia del poder judicial en el desempeño de sus funciones, las autoridades de control no tendrán competencia sobre los tratamientos de datos personales cuando los tribunales actúen en ejercicio de su función judicial, lo cual no significa la no aplicación del RGPD, sino que su control y atención de reclamaciones deberá poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro.

2.3 El Escudo de privacidad o *Privacy Shield*

---

o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

Desde el año 2000[88], ha permanecido en vigor el Acuerdo de Puerto Seguro (*Safe Harbor*) entre EEUU y Europa, que garantizaba que toda a aquella empresa que se adhiriera al mismo, se presumía cumplía el nivel de protección exigido por la Directiva 95/46 y por tanto, se permitía la libre transferencia internacional de datos entre empresas o entidades de EEUU y Europa.

La Sentencia del Tribunal de Justicia de la Unión Europea C-362/14[89] (caso Maximilian Schrems), que da respuesta a varias cuestiones prejudiciales, concluye que el Acuerdo de Puerto de Seguro es inválido. Se plantea la cuestión prejudicial de si una Decisión, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide a una autoridad de control de un Estado miembro, examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado. El TJUE concluye[90] que "una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las

---

[88] Decisión 2000/520/CE: Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección 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

[89] Sentencia del TJUE de 6 de octubre de 2015 en el asunto C-362/14 http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=105220

[90] apartado 53 de la Sentencia

facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por el artículo 28 de la referida Directiva (…)". Además, "sería contrario al sistema establecido por la Directiva 95/46 y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de dicha Directiva tuviera el efecto de impedir que una autoridad nacional de control examine la solicitud de una persona para la protección de sus derechos y libertades frente al tratamiento de sus datos personales que hayan sido o pudieran ser transferidos desde un Estado miembro a un tercer país al que se refiere esa decisión de la Comisión" (apartado 56 de la Sentencia).

Los principales motivos que llevan al Tribunal a concluir la invalidez del Acuerdo de Puerto Seguro son:

1. las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. (apartado 90 de la Sentencia).
2. las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión. (apartado 90).
3. se autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización (apartado 93). Por ello no se respeta el contenido esencial del derecho fundamental al respeto de la vida privada

garantizado por el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (apartado 94).

4. no se prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión, por lo que no se respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea (apartado 95).

Así las cosas, tras meses de negociaciones[91], se pone fin a la incertidumbre que suponía realizar transferencias internacionales de datos a un país como EEUU considerado por las autoridades europeas que no ofrece un nivel de protección adecuado, habiendo sido declarado el Acuerdo de puerto seguro y que obligaba a fundamentar dichas transferencias en otros supuestos, tales como el consentimiento del interesado. Finalmente el 12 de Julio de 2016 se aprueba la decisión[92] de adecuación del nuevo Acuerdo entre EEUU y Europa en materia de privacidad, Escudo de privacidad (*Privacy Shield*). De este modo, las empresas adheridas[93] a dicho acuerdo en el registro del Departamento de Comercio de EEUU (FTC), se considerará que cumplen con lo establecido en dicho acuerdo (los principios marco y los principios complementarios establecidos por la FTC), por lo que se mantiene el modelo de autocertificación por adhesión. No obstante, el Departamento de Comercio de EEUU se encarga de garantizar que dichas empresas respeten sus compromisos y la adhesión deberá

---

[91] Dictamen 1/2016 del GT29 de 13 de Abril de 2016 sobre sobre el proyecto de decisión relativo a la adecuación del escudo protector de la intimidad entre la UE y los EE. UU disponible en INGLÉS en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf y resumen ejecutivo en ESPAÑOL en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52016XX0715(01)&from=ES

[92] Decisión (UE) 2016/1250 de la Comisión http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=EN

[93] las empresas adheridas pueden consultarse en https://www.privacyshield.gov/list

renovarse anualmente. El Acuerdo se aplica tanto a Responsables como Encargados del tratamiento, los cuales estarán obligados contractualmente a actuar siguiendo las instrucciones del Responsable del tratamiento europeo. Respecto a las entidades que dejen de ser miembros[94], voluntariamente o bien porque expire su certificación, la FTC las "seguirá de cerca" para "para verificar si van a devolver, borrar o conservar los datos personales recibidos anteriormente. Si conservasen los datos, el Acuerdo establece que deberán seguir aplicando los principios. En los casos en que la entidad hubiera sido eliminada por "persistente incumplimiento" de los principios, la FTC se asegurará de que estas entidades devuelvan o supriman los datos con arreglo al marco.

Como novedades respecto al acuerdo de puerto seguro, en relación al acceso de las Administraciones americanas a datos transferidos en virtud del Escudo de Privacidad, se crea la figura del Defensor del Pueblo, como nuevo mecanismo de supervisión de posibles injerencias con fines de seguridad nacional, independiente de los servicios de inteligencia. Asímismo, la Comisión constata que el Derecho Estadounidense establece limitaciones al acceso a los datos transferidos desde la UE y su utilización por parte de los poderes públicos americanos. En segundo lugar, a través del *Principio de recurso, aplicación y responsabilidad*, se obliga[95] a las entidades a establecer mecanismos de recurso mediante los que los particulares afectados por un incumplimiento, puedan presentar reclamaciones, y que éstas se resuelvan efectivamente. Además, los particulares podrán[96] presentar una reclamación a un órgano de resolución de litigios independiente que en su caso haya sido designado por la organización, a las autoridades nacionales de protección de datos o a la FTC. Para el caso en que sus reclamaciones no sean resueltas por alguna de estas vías de recurso, los particulares podrán invocar el

[94] apartado 35 del Escudo de Privacidad.
[95] Apartado 38 del Escudo de Privacidad.
[96] Apartado 41 del Escudo de Privacidad.

arbitraje vinculante[97] en el marco del panel del Escudo de la Privacidad (Anexo 1 del Anexo II de la Decisión). En tercer lugar, se establecen condiciones más estrictas para revisar el cumplimiento del acuerdo por parte de las empresas adheridas para garantizar la aplicación efectiva de los principios.

Para más información sobre el funcionamiento del Acuerdo, la Comisión Europea ha elaborado una *Guía acerca del Escudo de Privacidad UE-EEUU*[98].

[97] Apartado 42 del Escudo de Privacidad.

[98] Disponible en http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

CAPÍTULO IV : PROBLEMÁTICA DEL *BIG DATA*

Una vez analizado el concepto, encuadre y marco jurídico aplicable a los tratamientos masivos de datos, examinaremos los posibles peligros que conllevan desde diferentes perspectivas, así como la concreta problemática que presentan desde la perspectiva de la normativa de protección de datos.

1.Posibles peligros del *big data*

El tratamiento de datos masivos puede aportarnos grandes beneficios a todas las personas, a nivel global, es decir, el *big data* puede ser muy beneficioso para todos, cuando se utiliza para la búsqueda de un bien común, pudiendo hablar de *big data* como "bien público". No obstante lo anterior, como todas las cosas, el *big data* también puede tener un "lado oscuro[1]" y creemos que no sólo debe analizarse el impacto de los tratamientos masivos de datos a un nivel estrictamente jurídico, pues la privacidad de las personas es un elemento muy importante para garantizar el libre desarrollo de la personalidad y, en último término, la libertad y la dignidad de las personas, como se vió en el segundo capítulo del presente trabajo.
Como posibles "peligros" que puede acarrear el *big data*, podemos mencionar:

- **Despersonalización:** si llegase un punto en el que las personas asumiéramos que en pro de un supuesto "bien común" hemos de ceder parte de nuestra privacidad, el hecho de tener el convencimiento de vivir permanentemente vigilados, puede afectar a los comportamientos

[1] Expresión utilizada por MAYER-SCHÖNBERGER, V., y CUKIER, K., *op. cit.*, p. 210.

individuales, básicamente por el miedo a represalias o por considerar que es la conducta que se espera realicemos. Llevado este planteamiento al extremo, nos encontraríamos en la sociedad descrita por Orwell en "1984".

- **Fundamentalismo del dato o dictadura del dato**: algunos autores han denominado así a la asunción de que la correlación siempre indica causalidad, y por tanto, afirmar que "los datos nunca mienten"[2]. Esto es muy importante pues puede conllevar situaciones de verdadera **discriminación**[3].
- ***Inferential Relation Retrieval* o descontextualización** de la información. Cierta información, fuera de su contexto, puede perder veracidad o sentido, es decir, cuando hay una desvinculación entre la información recogida y las circunstancias que motivaron su recogida, puede suponer que información veraz deje de serlo si se completa o conecta con otra información diferente. También se produce esta descontextualización si la información es utilizada para otros fines diferentes a los que motivaron su recogida. Ello implica gravísimas consecuencias, pues no sólo se estarían produciendo tratamientos no consentidos, sino que podrían conllevar conclusiones que no tienen por qué ser ciertas.
- **Problemas éticos:** "que puedas hacerlo, no significa que debas". En el *Technology Foresight Forum* celebrado el 22 de Octubre de 2012[4], los participantes, entre otras cosas,

---

[2] Destacar el curioso proyecto de Tyler Vigen que ha creado una *web* http://www.tylervigen.com/spurious-correlations donde muestra las aparentes correlaciones entre sucesos inconexos, como por ejemplo el número de personas que se ahogaron en una piscina con el número de películas en las que aparece Nicolas Cage.

[3] *How algorithms rule our working lives*, The Guardian, 1 septiembre de 2016, por Cathie O'Neil disponible en https://www.theguardian.com/science/2016/sep/01/how-algorithms-rule-our-working-lives

[4] http://www.oecd.org/sti/ieconomy/iccptechnologyforesightforum-harnessingdataasanewsourceofgrowthbigdataanalyticsandpolicies.htm

> consideraron que "la dimensión ética del uso de *big data analytics* es cada vez más importante". Un ponente comparó el *big data* con la energía nuclear, "está aquí lo queramos o no. Lo que podemos hacer es promover un uso responsable del *big data*" . En este sentido, el Supervisor Europeo de Protección de datos en su Opinion 4/2015 *Towards a new digital ethics-Data, Dignity and Technology*[5] es consciente, y así lo afirma, de que la dignidad de la persona no es sólo un derecho fundamental en sí mismo sino también el presupuesto para otras libertades y derechos, incluyendo el derecho a la privacidad y a la protección de datos. El SEPD afirma que "los tradicionales conceptos de privacidad, protección de datos y los principios, ya contenían matices éticos para la protección de la dignidad, como el empleo y la salud. Pero las tendencias de hoy en día han abierto un capítulo completamente nuevo, y hay una **necesidad de explorar si los principios son lo suficientemente robustos como para la era digital**". De hecho, el Supervisor Europeo de Protección de Datos creó en Enero de 2016 el *Ethics Advisory Group* (EAG) o Grupo Consultivo sobre ética, cuyo objetivo principal es explorar las relaciones entre los derechos humanos, la tecnología, los mercados y modelos de negocio en el siglo XXI desde una perspectiva ética, con especial atención a las implicaciones para los derechos de privacidad y protección de datos en el entorno digital. El Grupo estará operativo de febrero de 2016 a enero de 2018.

El Consejo de Europa, a través del Comité consultivo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), ha publicado en 2017 unas *Directrices sobre la protección de los individuos en relación al*

---

[5] Opinión 4/2015, de 11 de septiembre de 2015 disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf

Tratamiento de datos personales en un mundo de Big Data[6], con el objeto de proporcionar un marco general para que las Partes apliquen las políticas y medidas adecuadas para hacer efectivos los principios y disposiciones del Convenio 108 en el contexto de *Big Data*. Dichas Directrices han sido redactadas sobre la base de los principios del Convenio 108, a la luz de su proceso de modernización actualmente en curso. Las Directrices recomiendan medidas que las partes implicadas deberían adoptar para prevenir los posibles efectos negativos del *big data* sobre la dignidad humana, los derechos humanos y las libertades fundamentales individuales y colectivas, en particular en lo que respecta a la protección de datos personales. Destacar que entre las definiciones que se ofrecen en las Directrices, se define dato personal como cualquier información relativa a un individuo identificado o identificable, puntualizando que "los datos personales son también cualquier información utilizada para "singularizar" (*single out*) a personas de conjuntos de datos, para tomar decisiones que les afectan sobre la base de información de perfiles de grupo"[7].

El primero de los Principios que las Directrices establecen es el "*Uso ético y social de los datos*". Dada su importancia y claridad, lo reproduciremos (la traducción es nuestra):

"De acuerdo con la necesidad de equilibrar todos los intereses implicados en el tratamiento de datos personales y, en particular, cuando la información se utiliza con fines predictivos en los procesos de toma de decisiones, los responsables y encargados deben tener

---

[6] *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, 23 January 2017, disponibles en Inglés en https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a

[7] Reproducción en inglés de la nota 5 de las Directrices "According to this definition, personal data are also any information used to single out people from data sets, to take decisions affecting them on the basis of group profiling information".

debidamente en cuenta el probable impacto del tratamiento de *big data* y sus implicaciones éticas y sociales más amplias para salvaguardar los derechos humanos y las libertades fundamentales y garantizar el respeto del cumplimiento de las obligaciones en materia de protección de datos establecidas en el Convenio 108" .

"El procesamiento de datos personales no debe estar en conflicto con los valores éticos comúnmente aceptados en la comunidad o las comunidades relevantes y no debe utilizarse en detrimento de los intereses, valores y normas de la sociedad, incluida la protección de los derechos humanos. Si bien la preceptiva definición de la orientación ética puede ser problemática, debido a la influencia de factores contextuales, los valores éticos comunes pueden encontrarse en las cartas internacionales de derechos humanos y libertades fundamentales, como la Convención Europea de Derechos Humanos".

"Si la evaluación del impacto probable de un tratamiento de datos previsto descrito en la Sección IV.2 muestra un alto impacto del uso de Big Data en los valores éticos, los responsables podrían establecer un comité de ética *ad hoc* o confiar en los ya existentes para identificar los valores éticos específicos que deben salvaguardarse en el uso de datos. El comité de ética debe ser un órgano independiente compuesto por miembros seleccionados por su competencia, experiencia y cualidades profesionales y desempeñando sus funciones imparcial y objetivamente".

De la simple lectura de este primer Principio, vemos la importancia que para el Consejo de Europa tiene salvaguardar el impacto del *big data* en relación no sólo a la privacidad sino respecto a cuestiones éticas y sociales con la finalidad de salvaguardar los derechos humanos y las libertades fundamentales, hasta el punto de establecer un Comité de Ética para valorar y salvaguardar los riesgos de impacto en dicho ámbito. De hecho, en las Directrices, se habla continuamente de "derechos fundamentales", poniendo de relieve el posible impacto sobre los diferentes derechos fundamentales que el *big data* puede tener.

Otro de los Principios que se establecen en las Directrices, es el de "*Políticas preventivas y de valoración del riesgo*". Dentro de este

Principio se afirma que "Dado que el uso de Big Data puede afectar no sólo a la privacidad individual y la protección de datos, sino también a la dimensión colectiva de estos derechos, las políticas preventivas y la evaluación de riesgos deberán considerar el impacto legal, social y ético del uso de *Big Data*, incluido el derecho a la igualdad de trato y a la no discriminación". Dado que el *big data* puede afectar a derechos fundamentales, se recomienda que se involucren diferentes actores (individuos o grupos potencialmente afectados por el uso de *big data*) en el proceso de evaluación y diseño del tratamiento de datos. En caso de un impacto significativo en los derechos y libertades fundamentales, se establece que los responsables deberán solicitar asesoramiento de las entidades de supervisión para mitigar los riesgos detectados.

Las Directrices contemplan el papel de la *intervención humana en las decisiones apoyadas por Big Data*. En primer lugar se establece que el uso de Big Data debe preservar la autonomía de la intervención humana en el proceso de toma de decisiones. Las decisiones basadas en los resultados proporcionados por la analítica de Big Data deberán tener en cuenta todas las circunstancias relativas a los datos y no basarse en información descontextualizada o en resultados de tratamiento de datos. La persona que intervenga en la toma de decisiones, sobre la base de argumentos razonables, deberá tener la libertad de no confiar en los resultados proporcionados a través de *big data*. Cuando existan indicios de que haya podido haber discriminación directa o indirecta basada en el análisis de Big Data, los responsables y encargados tendrán la carga de la prueba de demostrar la ausencia de discriminación.

2. *Big data* y protección de datos

En este apartado analizaremos los riesgos específicos que el *big data* plantea respecto a la privacidad, aunque como hemos visto en el apartado anterior, los tratamientos de datos masivos pueden afectar a diferentes derechos y libertades fundamentales.

"Big data, llevado a cabo de manera responsable, puede aportar beneficios significativos para la sociedad y los individuos, en la salud, la investigación científica, el medio ambiente y otras áreas específicas. Pero hay serias preocupaciones sobre el impacto actual y pot
encial del tratamiento de grandes cantidades de datos sobre los derechos y libertades de las personas, incluyendo su derecho a la privacidad. Por lo tanto, **los retos y los riesgos del big data, requieren una protección más eficaz de los datos**". Así comienza el SEPD su Opinión 7/2015 *Enfrentar los desafíos del big data, Un llamamiento a la transparencia, el control de los usuarios, la protección de datos por diseño y la rendición de cuentas*[8].

Actualmente ya se están realizando tratamientos de *big data* que afectan a las personas, o que podrían llegar a afectarlas en un futuro. Se dice que los datos son "anónimos" o que se han "disociado", para argumentar la no aplicación de la normativa de protección de datos. Más adelante profundizaremos en la cuestión de la anonimización y los problemas que plantea, pero vaya por delante que si no se toman medidas *ex ante* que salvaguarden la privacidad de las personas, es muy probable que en un futuro, puedan verse afectados sus derechos, por mucho que actualmente no suponga problema alguno.

El GT29 en su Opinión 3/2013[9] sobre la Limitación de la Finalidad, afirma que el *big data*, a pesar de su potencial de innovación, puede presentar riesgos significativos para la protección de los datos personales y el derecho a la privacidad, y enumera los siguientes:

1. La magnitud de la recolección de datos, seguimiento y elaboración de perfiles, también teniendo en cuenta la variedad y el detalle de los datos recogidos y el hecho de que los datos se combinan a menudo de diferentes fuentes;
2. La seguridad de los datos, que se queda atrás frente a la expansión del volumen;

---

[8] Opinión 7/2015 del SEPD, p. 4, disponible en inglés https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[9] Opinion 3/2013 on purpose limitation, 2 abril 2013, p 45, disponible en inglés en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

3. Transparencia: a menos que se les proporcione información suficiente, los individuos serán sujetos a decisiones que no entiendan y sobre las que no tengan ningún control;
4. Inexactitud, discriminación, exclusión y desequilibrio económico;
5. Aumento de las posibilidades de vigilancia de los gobiernos;

Antes de proseguir, y siguiendo al GT 29, debe hacerse la distinción entre dos posibles perspectivas o escenarios, cuando el Responsable que utiliza *big data* 1) está interesado en la *información*, en obtener correlaciones y patrones 2) cuando el interés se focaliza en el *individuo* mismo. Queda claro que el segundo supuesto, afecta plenamente a la privacidad de la persona, pero no debemos obviar que el primer supuesto no está exento del mismo problema. De hecho, el GT29 recomienda para el primer caso, la aplicación del concepto de "separación funcional"[10], es decir, que los datos utilizados para unos determinados fines, no deben servir para apoyar medidas o decisiones relativas a los titulares de los datos (salvo autorización expresa de los interesados). Para el GT29, el concepto de "separación funcional" va a jugar un papel clave en este primer supuesto, y en la medida en que se consiga, podría ser un factor importante para decidir si los usos posteriores de los datos pueden considerarse compatibles. Para cumplir con este requisito, el GT29 considera que los responsables tienen que garantizar la seguridad de los datos, y todas las demás medidas técnicas y organizativas necesarias para garantizar la separación funcional. Ello quiere decir que, a pesar de que estamos en un escenario donde el responsable busca más obtener correlaciones y patrones en la información con independencia de la identidad de los sujetos, se presupone la aplicación de la normativa de protección de datos.

En el segundo supuesto (se aplican técnicas de *big data* en relación a un individuo, para obtener predicciones o patrones que sirvan para tomar decisiones en relación a ese preciso individuo), se requerirá el

[10] Opinion 3/2013 on purpose limitation, p. 30.

consentimiento libre, específico, informado e inequívoco del individuo. El GT29 afirma[11] que para que el consentimiento sea informado y asegurar la transparencia, el interesado debe tener acceso a su "perfil" y a la lógica del criterio de decisión (el algoritmo) que ha conducido al desarrollo de dicho perfil. Que las organizaciones den a conocer sus criterios de decisión, es una "salvaguarda fundamental" y de las más importantes en el ámbito del *big data*, ya que lo importante no es el tipo de información en sí misma recogida, si es sensible o no, sino las inferencias que pueden obtenerse a partir de la misma, que es lo que puede realmente conducirnos a información sensible o bien, inferencias incorrectas. En este sentido, y para evitarlas, el GT29 propone que los interesados tengan la opción de acceder a su perfil y corregirlo o actualizarlo, lo cual también redundaría en el responsable, ya que tendría una información más exacta. También deberían dar a conocer el origen de los datos.

Además de los riesgos enumerados por el GT29, que para la protección de datos personales puede suponer el *big data*, añadiremos los siguientes problemas que a nuestro juicio afectan directamente a nuestra privacidad.

2.1 Falta de transparencia y control

Hoy en día generamos más información que nunca, tanto los usuarios directamente como los aparatos que utilizamos (internet de las cosas), y ello unido a los avances en las tecnologías de procesamiento y almacenamiento de datos, fijan el perfecto caldo de cultivo para la utilización de técnicas de *big data*. Se aduce por parte de los responsables que no se manejan datos personales o bien que éstos son anonimizados, pues el fin último perseguido es mejorar la toma de decisiones y obtener una mayor eficiencia en la gestión de recursos, tanto materiales como personales. Pero queda claro que las técnicas de *big data* pueden perseguir fines diversos, entre los que se incluyen la aplicación directa a un concreto individuo (por ejemplo, en el ámbito

[11] Opinion 3/2013 on purpose limitation, p. 47.

de la salud). Es sobretodo en estos casos en los que sí será necesario el consentimiento del individuo, y también en aquellos en los que los datos no sean irreversiblemente anonimizados sino desidentificados.
Lo que ocurre es que en el momento actual ni los usuarios son realmente conscientes ni siquiera de lo que significa *big data*, y mucho menos de que sus datos vayan a tratarse con ese fin, ni los responsables tienen claro cuándo o en qué supuestos han de solicitar el consentimiento del interesado. Si a ello unimos el hecho de que los datos son recogidos de las más diversas fuentes, por diferentes responsables, en muchos casos el usuario ni siquiera es consciente de que se están realizando tratamientos de sus datos de esta manera, ni por parte de quién/es, por lo que la falta de transparencia nos conduce irremediablemente a una falta de control por parte del usuario.
Algunos autores[12] en relación al *big data* hablan de la "paradoja de la transparencia", ya que mientras todo tipo de información privada está siendo recogida sin nuestro conocimiento, a la vez se aduce que el *big data* hará del mundo un lugar más transparente.

2.2 Anonimización y privacidad. Seudonimización

Como hemos mencionado anteriormente, muchas veces se utiliza el argumento de que no interesan los datos personales, o que se trata de datos anónimos, para justificar la utilización de técnicas de *big data* sin adoptar las medidas que la aplicación de la normativa de protección de datos exigiría.
En relación a la anonimización, el GT29 publicó el *Dictamen 05/2014*[13] *sobre técnicas de anonimización*, el cual analizaremos a continuación, junto a cómo aborda el RGPD tanto la anonimización como la seudonimización. El objetivo del Dictamen es analizar las

[12] RICHARDS, N. M. y KING, J. H., "Three paradoxes of big data" (September 3, 2013), 66 *Stanford Law Review Online* 41 (2013), p. 42.
[13] Dictamen 05/2014 sobre técnicas de anonimización, 10 de abril de 2014, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

técnicas de anonimización existentes, atendiendo al marco legal existente en la UE sobre protección de datos, y formula recomendaciones para la gestión de estas técnicas "teniendo en cuenta el riesgo residual de identificación inherente a cada una de ellas".

2.2.1 Anonimización: ¿Uso posterior compatible?

En relación al concepto de anonimización, el Considerando 26 de la Directiva 95/46 afirma que "(…) los principios de la protección de datos no se aplicarán a aquellos datos hechos anónimos de manera tal *que no sea posible identificar al interesado*". En esta línea, la AEPD afirma[14] que "La anonimización de datos debe considerarse como una forma de *eliminar las posibilidades de identificación* de las personas". Siguiendo esta postura, el RGPD también en su Considerando 26 establece que "(…) los principios de protección de datos no deben aplicarse a la *información anónima*, es decir *información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable*, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". Destacar la diferenciación que introduce el RGPD entre la "información anónima" y los "datos convertidos en anónimos", ya que en el primer caso, la información anónima nunca ha constituido información de carácter personal, y por tanto, nunca se aplicó dicha normativa, a diferencia de los datos convertidos en anónimos, que en un primer momento sí constituyeron información de carácter personal y por tanto, fueron recabados y tratados conforme a la normativa. En el segundo caso, el proceso de anonimización constituirá un supuesto particular de

[14] Agencia Española de Protección de Datos, Orientaciones y garantías en los procedimientos de anonimización de datos personales, 2016, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf , p. 1.

"tratamiento posterior", como afirma el GT29 en el Dictamen[15], que podrá considerarse "compatible"[16] con el fin original siempre y cuando "el proceso de anonimización genere fiablemente información anonimizada". Es decir, la normativa no contempla la anonimización expresamente como uno de los supuestos que constituyen un tratamiento "compatible" con la finalidad inicial de la recogida de datos, por lo que en principio, deberá cumplir con la "prueba de compatibilidad"[17] según lo establecido en el Dictamen 3/2013 del GT29 sobre limitación de la finalidad. No obstante, si se garantizase la anonimización de la información de modo fiable, podrá entenderse como un fin "compatible" sin necesidad de observar más requisitos.
Además, no debe olvidarse lo que el GT29 denomina "anonimización por defecto", cuando se refiere a la obligación inherente al Principio de Calidad de destruir o cancelar los datos una vez se cumplieron los fines que motivaron su recogida[18]. En este caso, como acertadamente

---

[15] Dictamen 05/2014, pp 7 y 8.

[16] En el sentido del artículo 6.1 b) de la Directiva 95/46 "1. Los Estados miembros dispondrán que los datos personales sean: b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas"; La postura del GT29 en el Dictamen 5/2014 es coherente con la afirmada en el Dictamen 3/2013 sobre limitación de la finalidad, ver ejemplo n. 15, p. 66.

[17] La "prueba de compatibilidad" implica que, además de cumplir con los requisitos de calidad enumerados en el artículo 6 de la Directiva, deberán evaluarse las siguientes circunstancias:
a) la relación entre los fines para los que se recogieron los datos personales y los fines de su tratamiento posterior; b) el contexto en el que se recogieron los datos personales y las expectativas razonables de los interesados en cuanto a su uso ulterior;
c) la naturaleza de los datos personales y el impacto del tratamiento ulterior en los interesados;
d) las salvaguardas adoptadas por el responsable del tratamiento para garantizar un tratamiento correcto e impedir cualquier tipo de efecto negativo indebido en los interesados.

[18] Artículo 6.1e) Directiva 95/46 "1.Los Estados miembros dispondrán que los datos personales sean: e) conservados en una forma que permita la identificación de los

afirman[19] K. EL EMAM y C. ÁLVAREZ, la anonimización es algo diferente o algo más que un uso compatible, es un tratamiento obligatorio producto de las obligaciones de retención de datos.

El RGPD[20] ha introducido en su articulado, los criterios aportados por el GT29 para realizar la "prueba de compatibilidad" (no exhaustivos) para determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la **seudonimización**.

De la lectura del artículo, y tras lo anteriormente expuesto, sorprende enormemente que la mera seudonimización pueda constituir una de las medidas que legitimen el uso posterior de los datos para un fin distinto para el que fueron recogidos, con garantías suficientes.

En nuestra opinión, si ya es criticable[21] la mera existencia del mencionado párrafo cuarto del artículo 6 del RGPD, por atentar

---

interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos".

[19] EL EMAM, K., y ÁLVAREZ, C., "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, Oxford University Press (2015) 5 (1), p. 80.

[20] Artículo 6.4 del RGPD.

[21] Nos remitimos a la crítica realizada en el punto cinco del apartado 1.4 del Capítulo II del presente trabajo.

frontalmente contra el Principio de Calidad, mucho más que la mera seudoanimización o cifrado pueda legitimar un tratamiento "incompatible" posterior, teniendo en cuenta que la seudoanimización supone la aplicación de la normativa de protección de datos de carácter personal, tal y como el propio RGPD reconoce. Creemos que debería haberse incluido la anonimización, en lugar de la seudoanimización, tal y como ha mantenido el GT29 en su Dictamen 5/2014.

Por tanto, no sólo se rebajan los estándares de protección existentes con la Directiva 95/46 que no permitía usos incompatibles de los datos, sino que con esta disposición del RGPD aumentan considerablemente los riesgos para la privacidad de las personas, pues legalmente podrían utilizarse sus datos, eso sí, seudoanonimizados, para usos secundarios incompatibles con aquellos que motivaron la recogida, y lo más grave, sin su conocimiento/consentimiento.

2.2.2 Irreversibilidad vs reidentificación

Siguiendo con el análisis del Dictamen, lógicamente, si el objetivo de la legislación es ser tecnológicamente neutra y así garantizar su aplicabilidad en el tiempo, no se ofrecen técnicas concretas sobre cómo realizar un proceso de anonimización, sino que se pone énfasis en el resultado: no deben permitir identificar al interesado, de manera irreversible. En este sentido, el GT29 destaca que en normas internacionales como la ISO 29100[22] lo esencial también es la irreversibilidad del proceso de modificación de los datos personales que permiten identificar directa o indirectamente al interesado. El

[22] La ISO 29100 define anonimización como el proceso por el cual la información de identificación personal se modifica de forma irreversible de tal manera que el responsable del tratamiento no puede identificar, directa o indirectamente, ya sea por sus propios medios o en colaboración con algún tercero, a la persona asociada a dicha información de identificación personal (ISO 29100:2011).

requisito de irreversibilidad queda por tanto muy claro en la normativa europea[23], siguiendo los criterios sentados por la Directiva 95/46.

No obstante lo anterior, y del mismo modo que en el ámbito de las medidas de seguridad se afirma que la seguridad absoluta no existe, el GT29 afirma que "un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados", por lo que "la anonimización no debe contemplarse como un procedimiento esporádico o puntual, y los responsables del tratamiento han de evaluar regularmente los riesgos existentes". Es decir, por un lado la anonimización (irreversible) es la única forma de garantizar la privacidad de las personas, pero a la vez, el GT29 es consciente de que la capacidad de reidentificación es cada vez mayor. En la misma línea, la AEPD afirma[24] que "El avance de la tecnología y la información disponible hacen difícil garantizar el anonimato absoluto, especialmente a lo largo del tiempo, pero, en cualquier caso, la anonimización va a ofrecer mayores garantías de privacidad a las personas". Es por ello que la AEPD describe la finalidad de un proceso de anonimización como "eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados[25]" .

Por tanto, podemos preguntarnos, dado que siempre habrá un riesgo residual de reidentificación, cuándo estaremos ante un conjunto de datos propiamente "anónimos"[26], y por tanto, que podamos hablar de irreversibilidad.

---

[23] El GT29 afirma (p 6) que "el resultado de la anonimización (…) debe ser, de acuerdo con el actual estado de la tecnología, tan permanente como el borrado. En otras palabras: debe garantizarse que es imposible tratar los datos personales". Y recuerda que la Directiva 2002/58, en relación a los datos de localización y los datos de tráfico establece que "deberán eliminarse o hacerse anónimos" tras la prestación del servicio o cuando ya no sean necesarios.

[24] AEPD, op. cit., Orientaciones y garantías en los procedimientos de anonimización, p. 1.

[25] Ibídem

[26] En relación a las técnicas de anonimización, el CT29 considera (p12) que una estrategia que prevenga los tres riesgos claves de la anonimización (singularización, vinculabilidad, inferencia) tendrá la solidez necesaria para impedir la reidentificación de los datos mediante los medios más probables y razonables que puedan emplear el responsable y cualquier tercero.

El GT29 recuerda que la propia Directiva utiliza el criterio de la "razonabilidad de los medios usados" para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, "si la identificación es razonablemente imposible". En el mencionado Considerando 26, la Directiva afirma que "(..) para determinar si una persona es identificable, hay que considerar el *conjunto de los medios que puedan ser razonablemente utilizados* por el responsable del tratamiento o por cualquier otra persona, *para identificar a dicha persona* (…)".

Por su parte, el RGPD, también en el Considerando 26, establece que "(…) Para determinar si una persona física es identificable, *deben tenerse en cuenta todos los medios*, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una *probabilidad razonable* de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los *factores objetivos*, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos (…)". Vemos cómo el RGPD sigue la línea establecida por la Directiva 95/46 adoptando el criterio de la "razonabilidad de los medios usados", pero además, concreta aportando elementos objetivos como los costes, el tiempo, la tecnología.. para determinar si existe una "probabilidad razonable" de que se utilicen dichos medios.

Algunos autores[27] han criticado la falta de claridad en el Dictamen sobre el concepto de "riesgo aceptable de reidentificación" y que alude al "riesgo cero" como riesgo aceptable. Alegan que el "riesgo cero" no es consistente con la Directiva 95/46, así como con las diferentes nociones de identificabilidad en otras jurisdicciones[28].

[27] EL EMAM, K., y ÁLVAREZ, C., *op. cit*., p. 74.

[28] El problema de la diferente transposición de la Directiva 95/46 en lo que respecta a la noción de "identificabilidad" queda solventado tras la aprobación del RGPD, o mejor dicho, tras su plena aplicabilidad a partir de mayo de 2018.

Afirman también que no hay exigencia ni expectativa legal alguna en lograr el riesgo cero en la reidentificacion de datos anonimizados.
En primer lugar, destacar que la expresión "riesgo cero" no se utiliza en ningún momento en el Dictamen. Simplemente, y como no podría ser de otra manera, se plasma lo que la Directiva establece, es decir, que el resultado de la anonimización sea "de manera tal que ya no sea posible identificar al interesado" y el RGPD sigue el mismo enfoque, "los principios de protección de datos no deben aplicarse a la *información anónima*, es decir *información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable*, o deje de serlo". La prueba de que no se exige el resultado de riesgo cero de manera absoluta, pues como bien señalan los autores, la legislación europea no lo exige, es que, como hemos comentado anteriormente, existe el criterio de "razonabilidad de los medios usados", para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, "si la (re)identificación es razonablemente imposible". Por lo que *a sensu contrario*, si la re-identificación era razonablemente posible, los medios de anonimización utilizados no eran los adecuados. Por tanto, el criterio de la razonabilidad de los medios utilizados, junto con el criterio de la probabilidad razonable de que se utilicen medios para identificar a una persona, aportado por el RGPD, actúan como criterios moduladores respecto a la aplicación o no de la normativa de protección de datos y/o sus consecuencias sancionadoras, por lo que queda en nuestra opinión claro que el límite del riesgo aceptable no es el riesgo cero, en cuyo caso no existiría criterio modulador alguno[29]. En definitiva, consideramos que la anonimización no se configura como una obligación de resultado, sino como una obligación de medios consistente en adoptar los medios razonables que impidan al máximo posible la reidentificación, y de ahí la importancia de confeccionar un informe de impacto que plasme el cumplimiento de dicha obligación de medios.

[29] Cfr EL EMAM, K., y ÁLVAREZ, C., *op. cit.,* p. 75.

En opinión de la AEPD[30] "Los riesgos de reidentificación de los sujetos se deben abordar como un riesgo residual que hay que gestionar y no como el incumplimiento de las medidas de seguridad de protección de datos personales". De hecho, tal y como afirma la AEPD[31] "no es posible considerar que los procesos de anonimización garanticen al 100% la no reidentificación de las personas, por lo que será necesario sustentar la fortaleza de la anonimización en medida de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen".
En nuestra opinión[32], cuando se utilizan expresiones tales como "evitar de forma irreversible su identificación", "que el resultado de la anonimización debe ser, de acuerdo con el actual estado de la tecnología, tan permanente como el borrado" etc, son sólo una muestra del objetivo deseable al que debe tender el Responsable y que precisamente lo diferencian del concepto de seudoanonimización.

2.2.3 Principios de la anonimización

La AEPD ha establecido en su Guía *Orientaciones y garantías en los procedimientos de anonimización de datos personales*[33] los Principios que deben tenerse en cuenta en un proceso de anonimización, siempre bajo el prisma de la protección de datos desde el diseño, por lo que deberán ser tenidos en cuenta desde el inicio y durante todo el proceso.
La AEPD enumera los siguientes Principios:
- *Principio Proactivo*: la gestión de la protección de la privacidad no debe ser reactiva, es decir, consecuencia de la detección de una brecha o problema durante el proceso. Para ello, deberán adoptarse medidas

[30] AEPD, *op.cit*., p. 1.
[31] *Ibidem*, p. 24.
[32] Cfr. EL EMAM, K., y ÁLVAREZ, C., *op. cit.,* p. 74 *in fine*.
[33] *Op. cit.,* pp. 3 y 4.

desde un inicio tales como realizar una clasificación inicial de los datos que permita disponer de una escala de sensibilidad de la información.

- *Principio de privacidad por defecto:* la AEPD sostiene que "conviene que desde el inicio se salvaguarde la privacidad teniendo en cuenta la granularidad o grado de detalle final que deben tener los datos anonimizados". Es decir, si se ha realizado previamente una clasificación de la información asignando por ejemplo un valor (cuantitativo o cualitativo) a cada una de las variables de identificación, se podrán eliminar determinadas variables en caso de ser necesario, eliminando por tanto riesgos a priori.
- *Principio de privacidad objetiva*: la AEPD sostiene que la realización de una Evaluación de Impacto pondrá de manifiesto el umbral de riesgo o riesgo residual de reidentificación, el cual deberá ser asumido por el Responsable del fichero y tenido en cuenta en el diseño del proceso de anonimización. Además, la AEPD afirma que este riesgo residual de reidentificación deberá ser conocido por el destinatario de la información anonimizada y, en caso de que los datos sean para uso público, a todas aquellas personas que puedan utilizarla.
- *Principio de plena funcionalidad:* este Principio trata de garantizar la utilidad de los datos anonimizados, mediante la no distorsión con respecto a los datos no anonimizados. No obstante, debe tenerse en cuenta que siempre habrá cierto grado de distorsión ("diferencial de privacidad") que deberá poder ser cuantificable de cara a determinar el grado de confianza que pueda depositarse en los resultados del análisis de la información.
- *Principio de privacidad en el ciclo de vida de la información*: las medidas adoptadas para proteger la privacidad deben tomarse durante todo el ciclo de vida de la información, es decir, antes y durante el proceso de anonimización, y no sólo al principio.
- *Principio de información y formación*: todo el personal involucrado tanto en el proceso de anonimización como en la explotación de la información anonimizada, debe ser formado e informado sobre sus obligaciones.

2.2.4 Técnicas de anonimización

Teniendo en cuenta los múltiples elementos que han de valorarse a la hora de adoptar una técnica de anonimización (o varias), y de cara a poder probar que se han valorado todos y cada uno de dichos elementos, lo ideal sería que el responsable lo plasmase en un *informe de impacto*, así como las subsiguientes revisiones de riesgos realizadas, porque como afirma el GT29, la anonimización no debe contemplarse como un procedimiento esporádico, sino que los responsables han de evaluar regularmente los riesgos existentes, ya que el riesgo de re-identificación no puede sino aumentar con el tiempo.

Resulta recomendable, antes de aplicar una técnica de anonimización, realizar una fase de pre-anonimización, que consistiría en localizar las variables de información para eliminar las que sean identificadores directos y eliminar o diluir aquellas otras que puedan suponer un riesgo de trazabilidad y por tanto, de reidentificación.

En relación a las concretas técnicas de anonimización expuestas en el Dictamen, el GT29 las analiza teniendo en cuenta el estado actual de la técnica y los tres riesgos clave de la anonimización:

-*Singularización*: posibilidad de extraer de un conjunto de datos algunos (o todos) los registros que identifican a una persona.

-*Vinculabilidad*: capacidad de vincular como mínimo dos registros de un único interesado (o grupo de interesados), ya sea en la misma base de datos o en dos bases de datos distintas (correlación)

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

Partiendo de la base que no hay ninguna técnica infalible, como se afirma en el propio Dictamen, la técnica de anonimización que prevenga estos tres riesgos tendrá la solidez necesaria para impedir la reidentificación.

En el Dictamen se analizan dos principales familias de técnicas de anonimización, la **aleatorización**, y la **generalización**. Pueden combinarse técnicas de ambos grupos, para aumentar las garantías de privacidad. Las técnicas de aleatorización consisten en modificar la

veracidad de los datos, con el objeto de eliminar el vínculo existente entre los datos y la persona. Como técnicas de aleatorización se mencionan la *Adición de ruido*[34], *Permutación*[35] y la *Privacidad diferencial*[36]. Por otro lado, las técnicas de generalización consisten en generalizar o diluir los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud. Como técnicas de generalización el Dictamen analiza la *Agregación y anonimato K*, y la *Diversidad l, proximidad T.*

A continuación, reproducimos una tabla[37] con las diferentes técnicas de anonimización analizadas en el Dictamen y su eficacia en relación a los tres riesgos clave de la anonimización:

	¿Existe riesgo de singularización?	**¿Existe riesgo de vinculabilidad?**	**¿Existe riesgo de inferencia?**
Seudonimización	Sí	Sí	Sí
Adición de ruido	Sí	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash/Tokens	Sí	Sí	Puede que no

Tabla 6: Fortalezas y debilidades de las técnicas analizadas.

[34] Adición de ruido: consiste en modificar los atributos del conjunto de datos para que sean menos exactos, conservando no obstante su distribución general, es decir, añadir o sustraer aleatoriamente una determinada cantidad al valor original. Por ejemplo, en una base de datos relativa al peso de las personas, el sujeto pesa 47 kg, pero lo incluiremos dentro de la horquilla "peso entre 40 y 50 kg" sin hacer referencia a su peso concreto.

[35] Permutación: consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados.

[36] Privacidad diferencial: esta técnica no modifica los datos originales, y se aplica no antes de difundir la base de datos, sino cada vez que se realiza una consulta o cuando se genera una vista anonimizada de la base de datos. La privacidad diferencial indica al responsable del tratamiento cuánto ruido debe añadir, y en qué forma, para obtener las garantías de privacidad necesarias. Por tanto, esta técnica exige una supervisión continua (como mínimo de cada nueva consulta) para evaluar cualquier posibilidad de identificación de una persona en el conjunto de resultados de las consultas.

[37] Tabla del Dictamen 5/2016, p. 26.

El GT29, partiendo de la base de que las técnicas de anonimización anteriormente expuestas no cumplen al cien por cien los criterios de una anonimización efectiva, recomienda ponderar las limitaciones inherentes a cada una de las técnicas, en función de las circunstancias aplicables a cada caso, en orden a escoger una u otra técnica o bien, la combinación de varias de ellas. Cuando la técnica/s elegida/s no cumpla con alguno de los criterios, deberá realizarse una evaluación de los riesgos de identificación, en base a los criterios mencionados anteriormente (singularización, vinculabilidad, inferencia).

El GT29 señala tres riesgos que el responsable debe tener en cuenta a la hora de adoptar técnicas de anonimización:

1. los datos seudonimizados no son datos anonimizados, por lo que si se elige una técnica de seudoanonimización se aplicará la normativa de protección de datos.
2. Una vez que los datos han sido correctamente anonimizados, y por tanto, no es de aplicación la normativa de protección de datos, ello no significa que los interesados queden desprovistos de cualquier protección, pues la Directiva 2002/58 exige el consentimiento del interesado para el almacenamiento o acceso a los terminales del usuario/abonado.
3. No deben olvidarse los efectos que en las personas pueden causar los datos adecuadamente anonimizados, en el caso de la elaboración de perfiles, especialmente cuando la información anonimizada se utiliza para tomar decisiones que causan efectos en las personas.

Otras técnicas de anonimización citadas por la AEPD[38] en su Guía sobre *Orientaciones y garantías en los procedimientos de anonimización de datos personales* son Algoritmos de Hash y Algoritmos de cifrado, que veremos a continuación en el apartado de técnicas de seudonimización o desidentificación, pues consideramos que no son medidas de anonimización propiamente dicha, salvo como

[38] AEPD *op. cit.*, pp. 14 a 16.

dice la propia AEPD se garantice la destrucción segura de las claves y así pueda acreditarse, para garantizar la irreversibilidad del proceso de anonimización.
-*Capas de anonimización*: consiste en aplicar sucesivas técnicas de anonimización, sobre datos ya anonimizados, con la finalidad de garantizar que, en caso de producirse una brecha en uno de ellos, la privacidad de las personas quede garantizada.
-*Perturbación de datos*: consiste en la variación y/o supresión de datos, para evitar que la información resultante revele información personal. Como subtipos de esta técnica de perturbación la AEPD cita la microagregación, el intercambio aleatorio de datos, datos sintéticos, permutación de registros, permutación temporal, redondeo, reajuste de pesos, y la técnica del ruido aleatorio.
-*Reducción de datos*: consiste en reducir el número de datos originales sin alterarlos, reduciendo el nivel de detalle, eliminando por tanto la posibilidad de que datos únicos o atípicos faciliten las posibilidades de reidentificación. Como subtecnicas de reducción de datos, la AEPD cita la eliminación de variables, reducción de registros, recodificación global, codificación superior o inferior y la supresión de registros.

2.2.5 **Fases** del proceso de anonimización

Como bien afirma la AEPD, en todo proceso de anonimización es aconsejable seguir un protocolo[39] de actuación.
Seguiremos en este punto la propuesta realizada por la AEPD en su Guía, teniendo en cuenta que no se trata de un esquema cerrado, como afirma la propia AEPD, sino de una propuesta de estructura.

1) Definición del equipo de trabajo
2) Independencia de funciones
3) Evaluación de riesgos de reidentificación
4) Definición de objetivos y finalidad de la información anonimizada

[39] Ibíd., pp. 5 a 19.

5) Viabilidad del proceso
6) Preanonimización: definición de variables de identificación
7) Eliminación/reducción de variables
8) Selección de técnica/s de anonimización
9) Segregación de la información
10) Proyecto piloto
11) Anonimización

1) Definición del equipo de trabajo:

Las diferentes funciones existentes dentro de un proceso de anonimización pueden ser desempeñadas por los siguientes roles: el Responsable del fichero, el DPD (Delegado de Protección de Datos) o Responsable de protección de datos, el responsable del tratamiento de la información anonimizada (destinatario), un equipo de evaluación de riesgos, un equipo de preanonimización y anonimización, Responsable de seguridad etc

Según la AEPD, es fundamental que se documente la definición y funciones de cada uno de los intervinientes, con el objetivo de garantizar que cada tarea tenga un responsable.

2) Independencia de funciones:

La AEPD afirma que es recomendable que se garantice, dentro de lo posible, que cada uno de los actores, dentro de su ámbito competencial, obre con independencia del resto (Principio de independencia profesional) y sea responsable de las funciones que le hayan sido asignadas. De ahí la importancia del documento de definición del equipo de trabajo.

3) Evaluación de riesgos de reidentificación:

Resulta muy conveniente y necesario realizar una Evaluación de Impacto con el objeto de analizar los posibles riesgos del proceso de anonimización para poder gestionarlos de manera efectiva. Según establece la AEPD[40] "Cabría recordar que ninguna técnica de

[40] *Ibíd*., p. 8.

anonimización podrá garantizar en términos absolutos la imposibilidad de la reidentificación, ya que existirá siempre un índice de probabilidad de reidentificación que debemos intentar atenuar mediante la correspondiente gestión de riesgos". Por tanto, debemos determinar cuál será el umbral de riesgo aceptable y gestionar esos riesgos que hemos determinado como asumibles.

Como muy bien afirma la AEPD, el riesgo de reidentificación está implícito, y se incrementa a medida que transcurre el tiempo desde la anonimización realizada, no por errores en el proceso de anonimización sino "consecuencia de la evolución e incremento de los identificadores indirectos a lo largo del tiempo". La AEPD habla de "variación evolutiva de los riesgos a lo largo del tiempo" por lo que deben realizarse análisis periódicos de los riesgos residuales, con el fin de garantizar la efectiva anonimización a lo largo del tiempo.

5) Definición de objetivos y finalidad de la información anonimizada:

El objetivo no debe ser únicamente la anonimización en sí misma considerada, sino que, siguiendo a la AEPD, el concreto proceso de anonimización estará condicionado por el objetivo final de la información anonimizada, que puede ser formar parte de un conjunto de datos abiertos o bien destinarse a un uso restingido.

En el caso de información anonimizada para un uso restringido, la privacidad de los interesados se podrá reforzar mediante la adopción de contratos de confidencialidad, códigos de conducta, certificaciones y otras garantías jurídicas dentro del proceso de anonimización.

6) Viabilidad del proceso:

En el caso de que el objetivo de la anonimización sean datos especialmente protegidos, la AEPD mantiene que se podría tener en cuenta la existencia de un equipo para el estudio de la viabilidad del proceso de anonimización, que en un informe de viabilidad, refleje los motivos y condiciones específicas para la anonimización de esos datos especialmente protegidos.

7) Preanonimización: definición de variables de identificación:

Todo proceso de anonimización debe comenzar con la preanonimización, en el que se determinan las posibles variables de identificación (directas e indirectas) que deben tenerse en cuenta en el diseño del proceso de anonimización para poder establecer los diferentes criterios de protección.

En función de los objetivos de la información anonimizada, se establecerán las variables de identificación realmente necesarias, eliminando las variables no necesarias. La AEPD pone de relieve la dificultad del proceso de identificación de variables debido a que las variables de identificación indirecta no son siempre "tangibles".

8) Eliminación/reducción de variables:

En esta fase se reduce al mínimo necesario la cantidad de variables de identificación.

Se trata de una medida de carácter preventivo, dado que a menor información personal tratada, menor será el riesgo de reidentificación.

9) Selección de técnica/s de anonimización

10) Segregación de la información:

Se recomienda que el proceso de anonimización se realice en un entorno diferente tanto al entorno en que se explote la información anonimizada como al entorno en el que se traten los datos peronales.

La AEPD también habla de segregación en relación al personal involucrado en los diferentes entornos, como una garantía adicional en aras a evitar la reidentificación.

11) Proyecto piloto:

Se recomienda la realización de una prueba piloto, con datos no reales, con el objeto de comprobar la fortaleza de los procedimientos propuestos, detectar posibles riesgos etc y si el diferencial de privacidad resulta aceptable o no en función de la finalidad proyectada.

12) Anonimización:

Fase en la que se realiza efectivamente la anonimización.

La AEPD no recomienda la utilización de un proceso de anonimización de uso general con independencia del destinatario de la información, del tipo de información a anonimizar y la finalidad a la que se vayan a destinar los datos anonimizados.

Con independencia de la técnica o técnicas de anomización adoptadas, la AEPD[41] es partidaria de adoptar una serie de **garantías** en todo proceso de anonimización ya que "el proceso de anonimización no puede asegurar la imposibilidad de reidentificación de las personas en términos absolutos" . Algunas de las garantías que cita la AEPD son la firma de acuerdos de confidencialidad entre el Responsable del fichero, responsable del proceso de anonimización, responsable del tratamiento de datos anonimizados, y el personal con acceso a la información anonimizada; compromiso por escrito del destinatario de la información anonimizada de informar de cualquier riesgo o eventual identificación; la posibilidad de realización de auditorías al responsable del tratamiento de la información anonimizada por parte del Responsable del fichero sobre el uso de la información anonimizada.

Todas estas garantías deben incluirse en el Informe de impacto de privacidad que se realice, dentro de las salvaguardas encaminadas a la minimización de riesgos.

2.3 Seudoanonimización

En relación a la **Seudoanonimización,** consiste en la sustitución de un atributo por otro en un registro.

El RGPD[42] la define como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas

[41] AEPD *op. cit*., pp. 21 y 22.

[42] Artículo 4.5 RGPD.

destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable". Puntualizar que quizá hubiera sido más preciso que el RGPD utilizase la expresión "desidentificación", ya que la seudoanimización es una técnica de desidentificación, entre otras.

No se trata de una técnica de anonimización, sino de una medida de seguridad[43] útil, ya que reduce la vinculabilidad de los datos con la identidad del/los interesado/s. Por tanto, la normativa de protección de datos es plenamente aplicable a los datos seudonimizados.

Esta es la visión del RGPD, que en su Considerando 28 afirma que "La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos".

Las principales técnicas de seudonimización son:

-*Cifrado con clave secreta*: como su propio nombre indica, se produce un cifrado de los datos que sólo el poseedor de la clave (supuestamente) podrá descrifrar.

-*Función Hash*: se trata de una función que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño. Esta función no es reversible, pero si se conoce el rango de los valores de entrada de la función hash, aplicando la función a estos valores se podría obtener el valor real de un registro determinado.

-*Función con clave almacenada*: se trata de un tipo de función hash que utiliza una clave secreta a modo de valor de entrada suplementario

[43] El artículo 32.1 a) del RGPD la incluye como una medida de seguridad: "1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales (…)".

-*Cifrado determinista o función hash con clave con borrado de clave*: se genera un número aleatorio para cada atributo de la base de datos, a modo de seudónimo, y posteriormente se borra la tabla de correspondencia.
-*descomposición en tokens*: esta técnica suele basarse en mecanismos de cifrado unidireccionales, o bien en la asignación de un número de secuencia o generado aleatoriamente que no derive matemáticamente de los datos originales.
El RGPD[44] es consciente de que para incentivar la adopción de medidas de seudonimización, éstas no deben impedir que el Responsable pueda realizar un análisis general de los datos. Asímismo, indica también que además de haber tomado las medidas técnicas y organizativas necesarias en aplicación del RGPD, se mantendrá por separado la información adicional para la atribución de los datos personales a una persona concreta, indicando el responsable cuáles son sus personas autorizadas.
La reversión no autorizada de la seudonimización es contemplada expresamente por el RGPD[45] como uno de los tratamientos de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, y por tanto, como uno de los riesgos para los derechos y libertades de las personas físicas. Dado que los riesgos son de gravedad y probabilidad variables, éstas "deben determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una

[44] Considerando 29 del RGPD: "Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas".
[45] Considerando 75 RGPD.

evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto"[46].

La seudonimización es una de las medidas acordes con el Principio de privacidad desde el diseño y por defecto. Así se afirma en el RGPD[47], "(…) A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, *seudonimizar lo antes posible* los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad".

El RGPD establece en su artículo 25.1 que "Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la *seudonimización*, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".

La seudonimización, como medida de seguridad que es, en caso de quebrarse y producirse una reversión no autorizada, será una de las causas por las que el responsable deberá, "sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la

[46] Considerando 76 RGPD.

[47] Considerando 78 y artículo 25.1 RGPD.

seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas (…)"[48]. Además, el responsable del tratamiento también deberá comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación[49].

"Anonimización" y privacidad en EEUU

La *Health Insurance Portability and Accountability Act* (HIPAA) aprobada en 1996, establece que se han de cumplir con las normas de privacidad en materia de salud (*Hipaa regulations o Hipaa Privacy Rule*) que el Departamento de Salud y Servicios Sociales (HHS) promulgue. La HIPAA demostró ya en aquellos años su conciencia sobre el peligro de la reidentificación estableciendo una norma para la de-identificación de los datos de salud (PHI, *protected health information*), *de-identification health information* (DHI).

En virtud de esta norma, la información de salud no será personal cuando no identifique a un individuo y si el responsable no tiene una *base razonable para creer que se pueda utilizar para identificar a un individuo*.

Vemos por tanto, cómo también se utiliza un estándar de razonabilidad, pero a diferencia de la normativa europea, no exige el resultado de que no pueda relacionarse con un individuo, pues

---

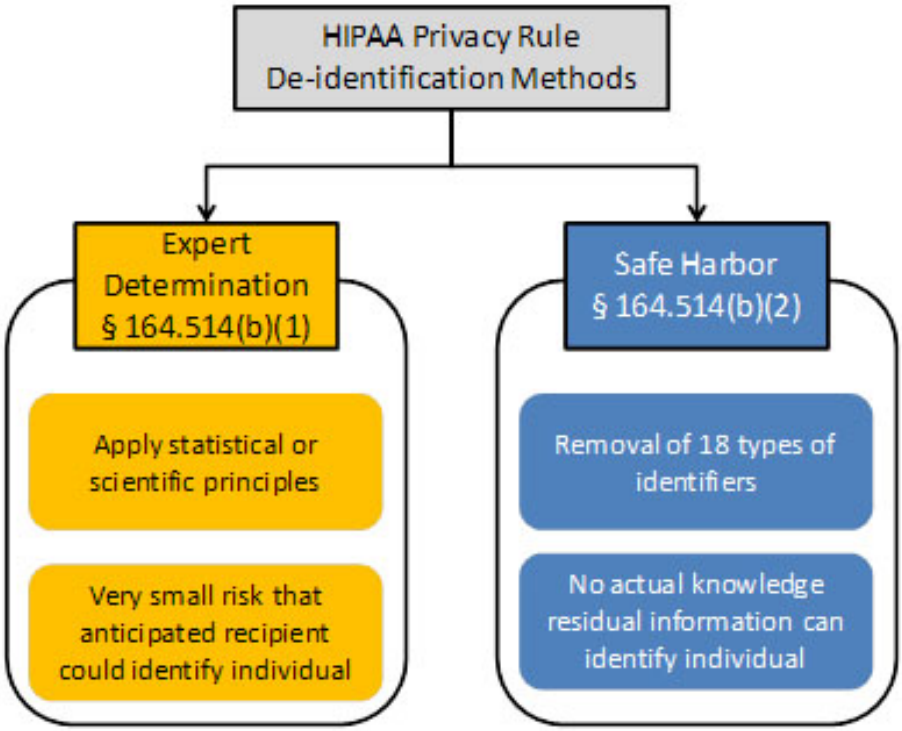
[48] Considerando 85 RGPD.

[49] Considerando 86 RGPD "(…) Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares".

realmente no estamos ante un proceso de anonimización sino de desidentificación, ya que la base de datos original con información personal, sigue existiendo.

Se establecen dos métodos para cumplir con el estándar de desidentificación:

1. el método de la decisión de los expertos (*expert determination method*): cuando una persona con los conocimientos adecuados y experiencia, aplique los principios estadísticos y científicos generalmente aceptados, y determine que el riesgo de que la información podría ser utilizada, solo o en combinación con otra información razonablemente disponible, es muy pequeño y documente los métodos y resultados del análisis que justifica tal decisión;
2. método del puerto seguro (*safe harbor method*): consistente en eliminar los identificadores (18) expresamente relacionados en la Ley.



Fuente: http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/

Como acertadamente afirma OHM[50], asumir que cualquier otra información diferente a los 18 identificadores enumerados por la norma no puede servir para reidentificar al interesado, es un error, por lo que este autor sugiere la revisión de la normativa[51].

[50] OHM, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (August 13, 2009). *UCLA Law Review*, vol. 57, p. 1701, 2010; *U of Colorado Law Legal Studies Research Paper* ns. 9-12, p. 1738, aunque hemos de puntualizar que OHM confunde en este caso concreto la seudoanonimización que realiza la HIPAA con un verdadero proceso de anonimización.

[51] Cfr CAVOUKIAN, A., y CASTRO, D., "Big data and innovation, setting the record straight: de-identification does work", Office of the Information and Privacy

En nuestra opinión, la HIPAA confunde anonimización y desidentificación, queriendo ofrecer los datos seudoanonimizados como si de datos anonimizados se tratase.
El problema de fondo existente en EE.UU., en este ámbito concreto, es la falta de una norma general que obligue a la anonimización o desidentificación de los datos (de cualquier tipo de dato personal y en cualquier contexto, no sólo respecto de determinados en función del sector) para usos posteriores, y la aparente confusión que mantienen, tanto Doctrina como la normativa, respecto a los conceptos de anonimización y desidentificación.
En lo que sí coincide la Doctrina, es que la anonimización no es la solución, pues como afirman I. RUBINSTEIN y H. WOODROW [52], "la anonimización perfecta es un mito".

2.4 ¿Datos ya recogidos? metadatos y reidentificación

Dejando a un lado la teoría, no debemos olvidar que el *big data* no tiene una fecha de salida, sino que es presente, se está produciendo actualmente. Si a esto le unimos el desconocimiento de gran parte de la población de qué es *big data*, y por tanto, la falta de consciencia de que toda su huella digital puede ser utilizada (o está siendo utilizada) por quién sabe, para quién sabe qué, debemos comenzar a pensar en remedios para garantizar los derechos de las personas, no sólo a partir de la aprobación del RGPD, que como hemos visto, no introduce novedades ni garantías especiales con respecto al uso de técnicas de *big data*, sino a partir del momento presente.

Commissioner, Ontario, Junio 2014, p 5, "De acuerdo con las estimaciones de un experto de identificación, sólo el 0,04 por ciento (4 de cada 10.000) de los individuos dentro de los conjuntos de datos desidentificados utilizando el Safe Harbor estándar son singularmente identificables".

[52] RUBINSTEIN, I., y HARTZOG, W., "Anonymization and Risk", August 17, 2015, *Washington Law Review*, vol. 91, n. 2, 2016; NYU School of Law, *Public Law Research Paper*, ns.. 15-36, p. 729. En el mismo sentido, OHM, P.

Cuando las técnicas de *big data* involucren el tratamiento de datos personales, el primer requisito que se ha de materializar es la **legitimidad** en el tratamiento. La legitimidad interviene tanto en la forma en la que los datos son obtenidos como en las repercusiones de dicho tratamiento de datos en el individuo, es decir, si éste las incluía dentro de sus expectativas razonables[53]. Todo ello puede verse cumplido en el caso en que hayamos obtenido el consentimiento del titular de los datos, pero ¿qué ocurre cuando ya disponemos de los datos pero lógicamente no obtuvimos el consentimiento del titular para aplicar técnicas de *big data* ni para qué finalidades?

Respecto a la cuestión de qué ocurre con los datos ya recogidos, la primera respuesta, con la normativa de protección de datos en la mano, sería que se necesita del consentimiento del usuario para que el Responsable pueda utilizar sus datos para *finalidades* de *big data*, comporte la recogida de datos nuevos o no, pues quizá sin necesidad de aportar nuevos datos personales podemos "enriquecer" una base de datos existente, y así obtener nueva información. Fuera del "mundo ideal" donde la normativa de protección de datos se cumple, el único instrumento específico que los ciudadanos tenemos para evitar la toma automatizada de decisiones, basadas en la evaluación de nuestro comportamiento o elaboración de perfiles, será analizado en profundidad en el apartado siguiente, pero simplemente, poner de manifiesto que es el único instrumento de defensa que el interesado puede utilizar.

Los datos ya recogidos o actualmente disponibles, producto de toda la vida digital de una persona, pueden servir para que, datos aparentemente anonimizados de manera efectiva, sean re-identificados.

Así, siguiendo a OHM, P.[54], existen determinados elementos en los datos, lo que el autor denomina "huella dactilar de los datos" (*data fingerprint*) y que nosotros denominaremos metadatos, que identifican unívoca e inequívocamente a las personas titulares de los mismos, a pesar de no constituir *a priori* datos de carácter personal o *personal*

[53] Informe del ICO "Big data and protection", p. 14.
[54] OHM, P., *op. cit.,* p. 1723.

identifiable information (PII). El autor lo compara con las huellas que pueden encontrarse en la escena de un crimen, del mismo modo, los titulares de los datos también generamos "huellas dactilares de datos", metadatos, no compartidas con nadie más.

Los científicos en el área de computación, configuran el modelo de anonimización y re-identificación como un juego de confrontación, de modo que el "adversario" es aquel que intenta re-identificar la información, con independencia de las intenciones buenas o malas de éste. Una vez que el adversario encuentra la "huella dactilar de datos", puede enlazarla o combinarla con información externa o "información auxiliar". Como afirma OHM[55], muchas técnicas de anonimización serían perfectas si el adversario no supiera nada más de las personas, es decir, si no tuviera acceso a esa información externa o auxiliar. Los expertos en informática, conscientes de la cantidad de datos que generamos y publicamos en internet, asumen que el adversario encontrará esa determinada información (metadatos) que permitiría la reidentificación, con el objetivo de diseñar respuestas eficaces ante la peor situación. De hecho, como señalan otros autores[56], hay cinco veces más metadatos que la información que somos conscientes de estar creando, y estos metadatos, pueden ser extraordinariamente reveladores. Como señalan I. RUBINSTEIN y W. HARTZOG[57], esta potencialmente devastadora objeción a la desidentificación se conoce como el "problema de la información auxiliar".

El problema es que no sólo podemos reidentificar, sino que tras la reidentificación, obtenemos mayor información que la que teníamos por separado[58]. Reproduciremos a continuación el ejemplo expuesto

---

[55] OHM, P., *op. cit.*, p. 1724.

[56] KUNER, Ch., CATE, F. H., MILLARD, Ch. y SVANTESSON, D., JERKER B., "The challenge of 'big data' for data protection", *International Data Privacy Law*, 2012, vol. 2, n. 2

[57] RUBINSTEIN, I., y HARTZOG, W., *op. cit.,* p. 713.

[58] Vid. RUBINSTEIN, I., "Big Data: The End of Privacy or a New Beginning?" (October 5, 2012), *International Data Privacy Law* (2013 Forthcoming); NYU School of Law, *Public Law Research Paper*, ns. 12-56, p. 5, donde la autora se plantea si la normativa de protección de datos debe aplicarse a la información "derivada", es decir, a la obtenida a partir de datos anonimizados o generalizados en

por OHM, basado en una base de datos de un hospital que recoge los motivos de visita de pacientes, para explicar la técnica de reidentificación conocida como "*inner join*" (combinación interna). Se trata de combinar dos o más bases de datos (tablas participantes) conectando las filas y la información común a ambas. Cuando las filas de las tablas representan personas, aplicando la técnica de la combinación interna, se asume que las filas en las que coinciden los campos críticos se refieren a la misma persona y se pueden combinar en una única fila en la tabla resultante.

TABLA 1: BASE DE DATOS ANONIMIZADA

Raza	Fecha de nacimiento	sexo	CP	Problema de salud
Negro	25/12/1976	Hombre	31011	Dolor de pecho
Negro	5/05/1950	mujer	31011	Dificultad para respirar
Blanco	29/05/1946	Hombre	31011	Vómitos
Blanco	26/06/1980	mujer	31011	mareos

En esta tabla se desconoce la identidad de las personas y su carácter de fumador o no fumador.

grupos de perfiles. Se cuestiona si la normativa debería aplicarse no sólo a los datos personales sino también a aquellos datos no personales que forman parte del conjunto de datos de donde se obtiene la nueva información. Afirma que de ser así, no habría límites para el ámbito de aplicación de la Directiva y en caso contrario, las técnicas de minería de datos escaparían de la aplicación de la normativa, a pesar de permitir inferencias de información anteriormente privada y/o el uso de grupos de perfiles que podrían acusar mucho más daño que la recogida y uso de información conforme a la normativa.

TABLA 2: BASE DE DATOS NO ANONIMIZADA

Nombre	Fecha de nacimiento	sexo	CP	Fumador
Mario	25/12/1976	Hombre	31011	Sí
María Cruz	5/05/1950	mujer	31011	no
Rafael	29/05/1946	Hombre	31011	no
Estela	26/06/1980	mujer	31011	No

Esta base de datos no indica que estas personas hayan ido al hospital ni el problema de salud concreto.

TABLA 3: BASE DE DATOS RESULTANTE

Nombre	Raza	Fecha nacimiento	sexo	CP	Queja	Fumador
Mario	Negro	25/12/1976	Hombre	31011	Dolor pecho	Sí
María Cruz	Negro	5/05/1950	mujer	31011	Dificultad para respirar	no
Rafael	Blanco	29/05/1946	Hombre	31011	Vómitos	no
Estela	Blanco	26/06/1980	mujer	31011	mareos	no

Ahora, además de su identidad, sabemos que fueron al hospital, por qué motivo y si fuman o no.
Se trata de un ejemplo muy sencillo pero ilustrativo de la facilidad en la reidentificación.
El problema con la reidentificación, como señala OHM[59], es que aun suponiendo que las técnicas de anonimización mejorasen exponencialmente, existen ya múltiples bases de datos expuestas o publicadas sobre las que ya no tenemos control y que conforman esa

[59] OHM, P., *op. cit.*, p. 1729.

"información externa o auxiliar" que puede servir para la reidentificación.

El propio autor objeta[60] el argumento de que el hecho de que la reidentificación pueda ocurrir, no significa necesariamente que vaya a ocurrir, y además sería necesario que el "adversario" tuviese el conocimiento y habilidades necesarias para hacerlo. OHM argumenta que hay poderosas razones económicas para motivar la reidentificación y lo que denomina el "mito del superusuario", es decir, que no es necesario disponer de complicados conocimientos ni ser expertos en computación para lograr la reidentificación.

El propio Gobierno estadounidense[61] reconoce el problema presente de la reidentificación; así afirma tajantemente que "otra realidad del *big data* es que una vez los datos han sido recogidos, es muy difícil mantenerlos anónimos. Si bien actualmente hay esfuerzos de investigación prometedores para ocultar la información personal (PII) dentro de los grandes conjuntos de datos, ahora los esfuerzos más avanzados se focalizan en la reidentificación de datos aparentemente anónimos. La inversión colectiva en la capacidad para fusionar los datos es muchas veces mayor que la inversión en tecnologías que mejoren la privacidad".

Una posible solución podría ser prohibir la reidentificación (la cual por definición actualmente ya estaría prohibida, al menos en Europa, pues estaríamos realizando un tratamiento de datos no autorizado y sin fundamento jurídico que legitimase dicho tratamiento), pero resulta imposible de implementar, pues, coincidimos con OHM en que sería muy difícil de detectar, probar y encontrar al Responsable.

Hasta ahora, la anonimización ha permitido un balance entre los beneficios del flujo de información y la protección de la privacidad. OHM considera que la anonimización ya no es la solución a los

---

[60] OHM, P., *op. cit.*, p. 1730.

[61] *Big Data: Seizing opportunities, preserving values*, Executive Office of the President, mayo 2014, disponible en https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf p 54 (la traducción es nuestra).

problemas de privacidad, y augura unos años de transición hasta que los expertos en privacidad acaben por reconocer lo que él denomina "el fracaso de la anonimización".

A priori la postura de OHM puede parecer demasiado extrema, pues si bien es cierto que cada día hay más datos disponibles a la vez que las técnicas informáticas mejoran, lo cual no hace sino aumentar los riesgos de reidentificación, si la "anonimización" no es una solución, sinceramente no vemos otra alternativa eficaz y respetuosa con la privacidad del individuo, dejando a un lado la solicitud del consentimiento. Lo que ocurre es que creemos que OHM cuando utiliza el término "anonimización" se está refiriendo también a datos desidentificados lo cual no es precisamente lo mismo, por lo que en este sentido tendría razón, pues los datos desidentificados, como hemos visto anteriormente, son datos de carácter personal en Europa, y por tanto, la desidentificación no sería una solución con respecto a la privacidad de las personas, sino una medida de seguridad más.

De hecho, y siguiendo con el punto de vista de la Doctrina americana, RUBINSTEIN y HARTZOG[62], ponen de manifiesto que hay autores que utilizan los términos anonimizacion y desidentificación como sinónimos. RUBINSTEIN y HARTZOG opinan que tienen significados distintos; denominan "desidentificación", siguiendo los estándares fijados por *el National Institute of Standards and Technology* (NIST), al proceso por el cual el custodio de los datos elimina la asociación entre los datos identificativos y el sujeto y "seudoanonimización[63]" lo entienden como una forma de desidentificación que sustituye la identidad del sujeto por un valor (como un seudónimo o un número). Coincidimos plenamente con estas definiciones, y por tanto en el presente trabajo los conceptos "anonimización" y "desidentificación" no se utilizan como sinónimos.

---

[62] RUBINSTEIN, I., y HARTZOG, W., *op. cit.,* p. 710.

[63] Destacar que el RGPD no utiliza en ningún momento el término desidentificación, sino el de seudoanonimización, mientras que el GT29 en su Dictamen 5/2014 sobre técnicas de anonimización, sí utiliza ambos términos, aunque no establece diferencias entre los mismos.

En la Doctrina americana, siguiendo la exposición realizada por RUBINSTEIN y HARTZOG[64], encontramos un debate en torno a la desidentificación; OHM como hemos visto sería uno de los detractores, y en el otro extremo (YAKOWITZ y otros) estarían los que, a pesar de que reconocen que hay cosas por mejorar, piensan que la desidentificación es una herramienta útil y que los riesgos de reidentificación han sido altamente exagerados, ayudados por los casos expuestos en la prensa.

RUBINSTEIN y HARTZOG proponen una solución conciliadora que acabe con el estancamiento del debate sobre la desidentificación; reconocen que las técnicas de desidentificación tienen limitaciones significativas, pero los casos notorios en que se ha roto la desidentificación deben servir para mejorar y obtener nuevos y mejores resultados.

En la misma línea encontramos a autores como CAVOUKIAN y CASTRO[65], que consideran que "la continua falta de confianza en la desidentificación y centrarse en los riesgos de la re-identificación puede hacer que los custodios de datos sean menos proclives a proporcionar a los investigadores acceso a información muy necesaria, incluso si los datos han sido fuertemente desidentificados; o peor aún, a creer que no deben perder su tiempo incluso en el intento de desidentificar la información personal antes de su puesta a disposición con fines de investigación secundarias". Estos autores consideran que "la desidentificación sigue siendo una herramienta fuerte para la protección de la privacidad, siempre y cuando se emplee con eficacia, con herramientas y técnicas actualizadas", ya que la desidentificación, para estos autores, sí funciona, la cuestión es que se utilice de manera efectiva[66]. Además, consideran que las técnicas de desidentificación mejoran progresivamente fruto de investigaciones, lo cual debe ser

[64] RUBINSTEIN, I., y HARTZOG, W., *op. cit.*, pp. 723 y 724.

[65] CAVOUKIAN, A., y CASTRO, D., "Big data and innovation, setting the record straight: de-identification does work", Office of the Information and Privacy Commissioner, Ontario, Junio 2014.

[66] CAVOUKIAN, A., y CASTRO, D., *op. cit.*, pp. 7 y 8.

visto como una oportunidad de mejora de la desidentificación y no como una crítica sobre su utilidad[67].

Compartimos plenamente la visión de RUBINSTEIN y HARTZOG y CAVOUKIAN y CASTRO, pero el problema de fondo existente en en EEUU radica en que no podemos otorgar a los datos desidentificados el tratamiento que daríamos a los datos efectivamente anonimizados.

Tanto EE.UU. como Europa, como no puede ser de otra manera, compartimos los riesgos de la reidentificación, con la diferencia de que en Europa los datos desidentificados siguen siendo datos de carácter personal y por tanto, merecedores de la protección que brinda la normativa de protección de datos, quedando la reidentificación no autorizada, sujeta a las consecuencias sancionadoras de la misma.

No obstante lo anterior, no caeremos en la visión reduccionista de pensar que la anonimización es la solución de cualquier problema, y que por tanto la problemática es diferente en EE.UU. y Europa.

Y esto es así porque en la sociedad de la información en la que vivimos actualmente inmersos, lo que antes podía ser mera información estadística, ahora es muy fácil asociarla a los individuos de los que proviene, por lo que el planteamiento que debemos hacernos a ambos lados del Atlántico, es si la anonimización (irreversible) es realmente posible en el contexto actual[68].

En respuesta a esta pregunta, USTARAN sostiene[69] que, dado que la normativa europea se aplicará cuando un individuo pueda ser identificado teniendo en cuenta el conjunto de los medios que puedan ser *razonablemente utilizados* para su identificación, quiere decir que no basta para la aplicación de la normativa *la mera posibilidad*. USTARAN pone sobre la mesa una idea muy interesante, diferente a la mantenida por la mayoría de la Doctrina que opina que, conforme la tecnología evoluciona, de manera directamente proporcional, la anonimización deja de ser una solución; afirma que una de las ventajas de la anonimización es que la misma tecnología puede

---

[67] *Ibid*., p. 12, aunque debe mencionarse que utiliza la palabra anonimización en el contexto de la desidentificación.

[68] en este sentido, USTARÁN, E., *The future of privacy*, Data Guidance, 2013, p. 96.

[69] USTARÁN, E., *op. cit*., p. 97.

hacerla incluso más efectiva, pues es probable que evolucione a la misma velocidad que las oportunidades de identificación. "Esto es así porque la evolución tecnológica es, en sí misma, neutral y las técnicas de anonimización pueden y deben evolucionar conforme los usos de los datos devienen más sofisticados[70]".

No obstante, tal y como hemos comentado anteriormente, no debemos pasar alto el hecho incontestable de que la anonimización siempre implicará un riesgo de reidentificación (recordemos que el GT29 hablaba de "riesgo residual"), y siguiendo a USTARAN, a la pregunta de cuán remoto ha de ser dicho riesgo para considerar la anonimización una solución funcional, si tenemos en cuenta que el concepto de identificación abarca mucho más que el hecho de identificar a través del nombre y apellido, "la respuesta es realmente un reto[71]".

2.5 Toma automatizada de decisiones

Esto es, decisiones o efectos jurídicos tomadas en base a procesos informáticos y correlaciones (*big data*), sin intervención humana y lo más importante, sin conocimiento de la persona ya que los datos se estarían utilizando para finalidades no especificadas, o incompatibles incluso, con las mencionadas en el momento de la recogida de datos.

En este punto, es interesante mencionar el concepto de la "paradoja de la identidad" de RICHARDS y KING[72], según la cual el *big data* busca identificar pero a la vez amenaza nuestra identidad, en el sentido de nuestro derecho a decidir quiénes somos y no vernos compelidos a seguir un camino no elegido por nosotros.

El sector financiero ha sido el primero en incorporar este tipo de toma de decisiones. Marco Bressan, *Chief Data Scientist* de BBVA,

---

[70] *Ibid*. (la traducción es nuestra)

[71] *Ibid*., p. 98.

[72] RICHARDS, NEIL M. y KING, JONATHAN H., "Three paradoxes of big data", (September 3, 2013), 66 *Stanford Law Review Online* 41 (2013), pp. 43 y 44.

afirmaba[73] en el Mobile World Congress de Barcelona "El siguiente paso es automatizar la toma de decisiones", "El primer objetivo de Big Data fue ayudar a capturar los datos de valor de las organizaciones, ahora estamos tratando de ayudar en la toma decisiones basadas en evidencias. Y lo próximo es simplemente eliminar ciertas decisiones, que se resolverán automáticamente".

Está claro que una toma de decisiones automatizada podría llegar a ser discriminatoria, arbitraria, y vulnerar derechos fundamentales. Es por ello que la legislación europea en materia de protección de datos, ha establecido límites al respecto. Destacar que ya en 1992 la LORTAD reconocía[74] un derecho similar al plasmado en 1995 en la Directiva, la cual previó un arma de defensa para los interesados que se vieran afectados por la toma de decisiones automatizadas que suponga una evaluación de la personalidad.

Así, la Directiva 95/46 ya reconocía[75] el derecho de las personas "a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que

---

[73] https://info.bbva.com/es/noticias/ciencia/marco-bressan-reto-pasar-del-big-data-las-experiencias-personalizadas/

[74] Artículo 12 LORTAD: *Impugnación de valoraciones basadas exclusivamente en datos automatizados* "El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad".

[75] artículo 15 de la Directiva 95/46 "*Decisiones individuales automatizadas*:

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado".

les afecte de manera significativa, *que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc*", el cual fue casi reproducido en el artículo 13 de la LOPD[76], salvo que expresamente no hace referencia a un tratamiento "automatizado", sino que establece que "los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, *que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad*". En su desarrollo reglamentario, en lugar de hablar de "impugnación de valoraciones", el RLOPD habla de un "derecho de oposición a las decisiones basadas únicamente en un tratamiento *automatizado* de datos".

El artículo 36 del RLOPD[77] reproduce las excepciones mencionadas por la Directiva 95/46, que no fueron plasmadas en la LOPD, lo cual a

---

[76] Artículo 13 LOPD: *Impugnación de valoraciones* "1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

[77] Artículo 36 RLOPD: *derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos* 1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado cuando dicha decisión:

juicio de APARICIO SALOM[78], parece ser una transposición imperfecta, pues la Directiva no configura este derecho de forma absoluta, sino sólo cuando no concurran las mencionadas excepciones. Por tanto, es necesaria la existencia de dos requisitos como presupuestos necesarios para el ejercicio del derecho:

1) "Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa"; como bien pone de manifiesto PUYOL MONTERO[79], tal y como está redactado el precepto, al igual que en la Directiva y el RLOPD, hace alusión a una "hipótesis jurídica extremadamente amplia, que puede abarcar relaciones jurídicas de carácter público del sujeto, así como las de carácter meramente privado". Siguiendo al mismo autor, la expresión "afección significativa" se trata de un concepto jurídico indeterminado, que además, exige analizar las concretas circunstancias del caso, pues el grado de afección deberá valorarse en relación a las circunstancias personales del sujeto.
2) "que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta"; la LOPD simplemente hace referencia a que el tratamiento automatizado de datos tenga por finalidad "evaluar determinados aspectos de su personalidad". El RLOPD incorpora los ejemplos mencionados por la Directiva (rendimiento laboral, crédito,

---

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

[78] ZABÍA DE LA MATA, J., *op. cit.*, p. 327.

[79] PUYOL MONTERO, J., en ZABÍA DE LA MATA, J., *op. cit.*, p. 327.

fiabilidad o conducta), pero no por ello el ámbito objetivo del derecho queda reducido, pues puede abarcar cualquier aspecto de la personalidad de un sujeto.

El problema que plantea este artículo, es la dificultad para el interesado de probar que concurren los presupuestos necesarios para su ejercicio, es decir, deberá probar que en base a un tratamiento automatizado de datos, exclusivamente, se han obtenido determinadas valoraciones de su personalidad, que le han afectado de manera significativa o han sido las causantes de determinada decisión jurídica. Dificultad que radica no sólo por tratarse de conceptos jurídicos indeterminados, sino porque quizá no tiene la información necesaria, es decir, desconoce si se ha realizado un tratamiento automatizado de datos del cual se ha obtenido una valoración de aspectos relativos a su personalidad. En palabras de PUYOL MONTERO[80], "(...) en el caso del responsable del tratamiento, (la situación) es justo la contraria, lo que le va a posibilitar el tener los mejores instrumentos jurídicos para poder defenderse y neutralizar el ejercicio del derecho por el afectado". Quizá ayude en este sentido el párrafo tercero del artículo 13 de la LOPD, que establece el derecho del afectado a obtener información del responsable sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto, aunque quizá habría sido más garantista establecerlo como una obligación del responsable, sin que el afectado tenga que solicitar la información.

En relación a las excepciones recogidas por la Directiva y el RLOPD, es decir, los casos en los que los afectados podrán verse sometidos a este tipo de decisiones:

a) "Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1

[80] *Op. cit.*, p. 329.

y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato".

Por tanto, no bastará que el interesado solicite la celebración o ejecución de un contrato en el que se tomen este tipo de decisiones automatizadas, sino que el responsable deberá informarle de esta circunstancia *previamente* y de forma "clara y precisa", para que el interesado pueda alegar lo que estime oportuno.

Nos llama poderosamente la atención, que para el caso en que el interesado solicite la celebración de un contrato que implique la toma de este tipo de decisiones, se establezca la obligación para el responsable de informarle previamente sobre dicha circunstancia, y para el resto de casos, en los que no existe una petición de contratación por parte del interesado, y por tanto, sea mayor su posible desconocimiento, no se establezca la misma obligación, cuando pueden existir consecuencias jurídicas o que afecten significativamente al interesado.

Respecto a la obligación de cancelar los datos por parte del responsable en el caso de que no llegue a celebrarse el contrato, no deja de ser una consecuencia del Principio de calidad, por el que deberán ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados. No obstante, a pesar de no ser necesaria dicha mención, dada la tipología de datos, consideramos acertado el recordatorio del deber de cancelación.

b) "Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado";

Esta excepción supone la existencia de una norma con rango de Ley, que prevea la toma de decisiones automatizadas que supongan valoración de la personalidad, con consecuencias jurídicas para el interesado o que le afecten significativamente. Además, esta Ley deberá establecer medidas que garanticen el interés legítimo del interesado, es decir, que se adopten las salvaguardas necesarias. Se trata de una excepción poco concreta, y como apunta PUYOL

MONTERO[81], "el riesgo que se corre es que dichas medidas cubran meramente aspectos formales, desatendiendo los efectos materiales o las consecuencias que se puedan irrogar al interesado por las valoraciones efectuadas".

Por su parte, el RGPD también reconoce este derecho de manera muy similar a su plasmación en la Directiva 95/46. Así, en su artículo 22, párrafo primero, establece que "*todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*". Entre las excepciones[82], además de las reconocidas por la Directiva 95/46, añade el consentimiento explícito del interesado. También establece que las decisiones no podrán basarse en categorías especiales de datos personales (artículo 9.1 RGPD).

En realidad, el RGPD no prohíbe la creación de perfiles, sólo su utilización en un determinado contexto, por lo que *a contrario sensu* parece admitir la existencia de perfiles sobre nuestra persona, construidos a partir de datos obtenidos con el consentimiento del interesado u obtenidos legítimamente en base a otro fundamento

---

[81] *Op. cit.*, p. 330.

[82] Artículo 22.2 RGPD: el apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el derecho de la unión o de los estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses_legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. en los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado".

jurídico. Esto en cualquier caso, supondría un tratamiento de datos no consentido por el interesado, ya que como establece el Considerando 60 del RGPD "(…) el responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración (…)". Por su parte, y aunque parezca una obviedad, el Considerando 72 establece que "*La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos (...)".* De la lectura conjunta de ambos considerandos, en primer lugar queda claro que la elaboración de perfiles queda sometida a la normativa de protección de datos, pero además, se dice que "deberá informarse sobre la existencia y elaboración de perfiles..", ¿quiere esto decir que no es necesario el consentimiento de la persona para la elaboración de perfiles? Entendemos que si la elaboración de perfiles queda incluida en el ámbito objetivo de aplicación de la normativa, no se puede prescindir del consentimiento del interesado para su elaboración. Por tanto, queda claro que para la elaboración de perfiles es necesario informar previamente al interesado y obtener su consentimiento, y por tanto, en nuestra opinión la redacción del artículo 22 del RGPD es bastante desafortunada y confusa.

Algunos autores (HILDEBRANDT, KOOPS[83]) critican que quedaría fuera del ámbito de aplicación del RGPD la utilización de perfiles, no ya referidos a una persona, sino a un grupo de personas, ya que no constituirían datos personales. En nuestra opinión, de ser así, equivaldría a la prohibición de utilizar técnicas de *big data* aplicadas a personas genéricamente, por lo que no estamos de acuerdo con dicha observación, pues no se ha utilizado un perfil personalizado para

[83] KOOPS, B. K., 'The trouble with European data protection law', *International Data Privacy Law*, 2014, doi: 10.1093/idpl/ipu023, p. 10.

tomar una decisión en relación a ese concreto individuo, sino una simple técnica de *big data* en relación a conjuntos de personas.

Siguiendo con el análisis del artículo 22, ¿quiere decir que podemos oponernos a toda decisión basada únicamente en un tratamiento automatizado? La respuesta es afirmativa, ya que la literalidad del RGPD no deja mucho lugar a la interpretación, pero deberán darse unos requisitos:

1) que la decisión se base únicamente en un tratamiento automatizado; de forma que si existe algún tipo de intervención humana para llegar a dicha decisión, este presupuesto no se vería cumplido.
2) que dicha decisión produzca efectos jurídicos o le "afecten significativamente de modo similar".
3) que la decisión no sea necesaria para la ejecución de un contrato entre el interesado y un Responsable del tratamiento
4) que la decisión esté autorizada por el Derecho de la unión o de los estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado
5) que el interesado no haya dado su consentimiento explícito,

y como un pre-requisito, añadiríamos, que el interesado sea consciente de ello, porque, si una empresa utiliza un determinado algoritmo para decidir a qué persona despedir, ¿realmente el trabajador despedido será informado de que la decisión la tomó un programa informático?

Recordemos que el RGPD[84] incluye dentro del contenido del derecho de información, la obligación de informar sobre "la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado".

La *obligación* que establece nuestro RLOPD sobre el responsable de informar previamente al afectado, de forma clara y precisa, sobre el

[84] Artículo 13.2 f) RGPD.

hecho de que la celebración del contrato solicitado por el interesado implica la toma de este tipo de decisiones, para que el interesado pueda alegar lo que estime oportuno, ahora queda diluida, ya que simplemente dice que el responsable "adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión". Bien es cierto que ya no se reduce a los casos en que el interesado solicite la celebración del contrato, por tanto, es aplicable a cualquier contrato que celebren las partes y cuando el tratamiento se base en el consentimiento explícito del interesado, pero no es menos cierto que el responsable no tiene la obligación de informar previamente y de manera "clara y precisa", sino que bastará que adopte las "medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado", entre las que se encuentran, como cita el propio artículo, el derecho a obtener una respuesta (humana) por parte del responsable y a impugnar la decisión. Obviamente, no es lo mismo el derecho a obtener una respuesta, que la obligación de proporcionar de manera previa determinada información, lo cual tiene mucha trascendencia de cara al derecho de impugnación del interesado. Y tampoco es lo mismo impugnar una decisión que dejarla sin efecto (anularla).

Pero además, el párrafo tercero deja muy claro que la obligación del responsable de "adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión", se aplica a los supuestos a) y c) del párrafo segundo (es decir, cuando la decisión es necesaria para la celebración del contrato o cuando se base en el consentimiento explícito del interesado), por lo que nos preguntamos qué obligaciones tendrá el responsable en el resto de los casos, es decir, todos los comprendidos en el párrafo primero, o lo que es lo mismo, qué obligaciones concretas tiene el responsable cuando la decisión basada en procesos automatizados no encaje en los supuestos exceptuados en el párrafo segundo.

Por otro lado, la decisión de incluir como una de las excepciones el consentimiento explícito del interesado, quizá abra la puerta a legitimar la elaboración de perfiles o este tipo de tratamientos, "escondiendo" o incluyendo dicha finalidad entre los términos de uso de cualquier aplicación, contrato o similar.
Consideramos que, se ha mejorado ligeramente la redacción de este artículo en relación con el correspondiente de la Directiva, pero a pesar de sus buenas intenciones, creemos que adolece de importantes defectos tal y como hemos puesto de manifiesto.
Creemos que debería existir la correspondiente obligación de los Responsables de tratamiento de informar al interesado previamente, y como establece el RLOPD, de forma "clara y precisa", de cuándo una decisión va a ser tomada exclusivamente por medios automatizados, para que realmente el interesado pueda ejercer su derecho de impugnación. Pero es que aun existiendo dicha obligación, nada obsta a que se añada una última fase en la toma de dicha decisión que implique intervención humana, y así el responsable evite la aplicación de este artículo, lo cual en último término implicaría el cercenamiento *ab initio* de este derecho.

2.6 Privacidad por defecto

La privacidad por defecto (*privacy by design*) no es un riesgo originado por la utilización de técnicas de *big data* pero resulta interesante analizar en este punto su viabilidad o encaje con respecto a las mismas.
El RGPD[85] establece que "El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la *cantidad de datos* personales recogidos, a la *extensión de su tratamiento*, a su *plazo de*

[85] Artículo 25.2 RGPD.

conservación y a su *accesibilidad*. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

Esta previsión, en perfecta consonancia con la protección de la privacidad de los interesados, resulta aparentemente difícilmente conjugable con las técnicas de *big data*, que precisamente requieren de lo contrario, captar cuantos más datos mejor, conservarlos durante el tiempo que el responsable considere necesario, y utilizarlos para unos fines que quizá el responsable todavía ni siquiera conoce.

Una respuesta rápida y simplista, vendría a decir que si los datos se anonimizan, ya no sería de aplicación la normativa de protección de datos, y por tanto, la privacidad por defecto, pero como hemos visto, no es tan sencillo.

ENISA, la Agencia Europea de Seguridad de las Redes y de la Información, publicó un Informe[86] en el que sostiene precisamente que los principios de la privacidad desde el diseño son aplicables al *big data*. ENISA aborda el concepto de la privacidad desde el diseño[87] a través de ocho estrategias:

-MINIMIZACIÓN: la cantidad de datos personales recogidos debe ser la mínima posible

-OCULTACIÓN: los datos personales y sus interrelaciones deben ser ocultados, no expuestos a plena vista.

-SEPARACIÓN: Los datos personales deben ser procesados de forma distribuida, en compartimentos separados siempre que sea posible;

-AGREGACIÓN: Los datos personales deben ser procesados en el más alto nivel de agregación y con el menor detalle posible en el que (todavía) sean útiles.

---

[86] ENISA, "Privacy by design in Big Data", diciembre 2015.

[87] ENISA, "Privacy and Data Protection by design", 2014. Disponible en https://www.enisa.europa.eu/activities/identity- and-trust/library/deliverables/privacy-and-data-protection-by-design

-INFORMACIÓN: los interesados deben ser adecuadamente informados de cualquier tratamiento (transparencia);
-CONTROL: los interesados deberán consentir sobre el tratamiento de sus datos.
-CUMPLIMIENTO: deberá haber una política de privacidad que cumpla los requisitos legales y deberá ejecutarse
-DEMOSTRACIÓN: los responsables deberán poder demostrar el cumplimiento con la política de privacidad en vigor y con cualquier otro requerimiento legal.
En la siguiente tabla, elaborada por ENISA[88], se analiza cómo cada una de estas estrategias que conforman el concepto de privacidad en el diseño, pueden implementarse en cada una de las fases de la cadena de valor de los tratamientos masivos de datos.

[88] ENISA, "Privacy by design in Big Data", diciembre 2015, p. 26.

	BIG DATA VALUE CHAIN	KEY PRIVACY BY DESIGN STRATEGY	IMPLEMENTATION
1	Data acquisition/collection	MINIMIZE	Define what data are needed before collection, select before collect (reduce data fields, define relevant controls, delete unwanted information, etc), Privacy Impact Assessments.
		AGGREGATE	Local anonymization (at source).
		HIDE	Privacy enhancing end-user tools, e.g. anti-tracking tools, encryption tools, identity masking tools, secure file sharing, etc.
		INFORM	Provide appropriate notice to individuals – Transparency mechanisms.
		CONTROL	Appropriate mechanisms for expressing consent. Opt-out mechanisms. Mechanisms for expressing privacy preferences, sticky policies, personal data stores.
2	Data analysis & data curation	AGGREGATE	Anonymization techniques (k-anonymity family, differential privacy).
		HIDE	Searchable encryption, privacy preserving computations.
3	Data storage	HIDE	Encryption of data at rest. Authentication and access control mechanisms. Other measures for secure data storage.
		SEPARATE	Distributed/ de-centralised storage and analytics facilities.
4	Data use	AGGREGATE	Anoymisation techniques. Data quality, data provenance.
5	All phases	ENFORCE/ DEMONSTRATE	Automated policy definition, enforcement, accountability and compliance tools.

Así, siguiendo el Informe, aunque el principio de minimización de datos aparentemente contravenga la recogida masiva de datos, nos permitirá obtener unos datos mejores y más útiles. Por su parte, las estrategias de ocultación, agregación y separación, permitirían la utilización de datos personales para realizar analíticas sin afectar a la privacidad. La estrategia de información apoyaría mejores mecanismos para la información de los usuarios y transparencia, y la estrategia de control, apoyaría nuevas formas prácticas para expresar consentimiento y las preferencias de privacidad. Las estrategias de

cumplimiento y demostración, ayudarían a los responsables a aplicar sus políticas de privacidad, en línea con el Principio responsabilidad en el cumplimiento (*accountability*).
Por tanto, y al menos sobre el papel, queda claro que los principios de privacidad desde el diseño pueden aplicarse al *big data*.
Como corolario a todos estos riesgos que el *big data* introduce respecto a la privacidad, hemos de mencionar la dificultad en localizar y por tanto, sancionar, estas prácticas, dada la cantidad de actores que pueden intervenir en el tratamiento de la información y la imposibilidad de trazar la cadena de responsabilidades que pudiera existir.

2.7 Requisitos para el tratamiento

Como hemos mencionado anteriormente, el primer requisito es la **legitimidad**, referida tanto a la forma en la que se recogen los datos como a los efectos o finalidades del tratamiento. Como muy bien señala el ICO[89], "todo tratamiento de datos debe ser legítimo, pero si las analíticas son utilizadas para tomar decisiones sobre los individuos, la evaluación del requisito de legitimidad debe ser incluso más riguroso".
Así, el artículo 5 del RGPD establece que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia") y recogidos con fines determinados, explícitos y legítimos.
El artículo 6 establece que el tratamiento sólo será lícito si se basa al menos en uno de los siguientes fundamentos jurídicos[90], de los cuales

[89] Informe del ICO "Big data and data protection", p 16.
[90] artículo 6.1 RGPD: "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

para el supuesto de tratamiento de datos masivos, en nuestra opinión y en términos generales, el fundamento que mejor encajaría es el consentimiento del interesado, pero obtenido de manera correcta, pues como afirma el GT29[91] "si se utiliza incorrectamente, el control del interesado resulta ilusorio y el consentimiento constituye un fundamento inadecuado para el tratamiento".

Para que el **consentimiento** sea un fundamento jurídico válido para el tratamiento masivo de datos, éste debe obtenerse mediante una "manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (artículo 4.11 RGPD). Es decir, no podrá inferirse o deducirse el consentimiento de cualquier manera, ya que, deberá ser inequívoco, es decir, sin dejar lugar a dudas y fruto de una declaración o acción afirmativa.

Para que despliegue toda su eficacia, además, deberá ser específico e informado, y por tanto, entre otros extremos, deberá informarse sobre la realización de tratamientos de datos masivos y con qué finalidad. Y todo ello con independencia de si ya disponíamos de los datos o no,

---

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

[91] Dictamen 06/2014 sobre el concepto de interés legitimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de Abril de 2014, disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf p. 19.

pues para la realización de técnicas de *big data* deberemos solicitar el consentimiento nuevamente, y además especificar las finalidades de dicho tratamiento, incluyendo si obtendremos datos personales de otras fuentes (e.g redes sociales) y/o incluiremos los datos inferidos en posteriores tratamientos de datos. Además, para que el consentimiento sea informado, deberá darse la posibilidad al interesado de acceder a su perfil y a los criterios de decisión que han llevado al desarrollo de ese concreto perfil. En palabras del GT29 "esta es una salvaguarda fundamental y la más importante en el mundo de *big data*"[92]. Y esto es así, porque no son tanto los datos recogidos sino las inferencias que se obtienen de los mismos y la manera en que esas inferencias son interpretadas, las que pueden suponer un daño para el interesado. Precisamente por este riesgo de inferencias incorrectas o inadecuadas, el GT29 afirma que los interesados puedan actualizar o corregir sus perfiles[93].

En el capítulo siguiente se profundizará más en estas cuestiones. Lo importante es que no será suficiente para obtener el consentimiento incluir simplemente "la utilización de técnicas de *big data*", sino que deberemos incluir para qué finalidades (propias, de terceros, exclusivamente para el servicio objeto de contratación o no etc) y de manera que el interesado entienda qué se va a hacer con sus datos para que tenga efectiva validez el consentimiento que preste. Como apunta el ICO[94] este consentimiento puede ser granular, es decir, un proceso en el que solicitar el consentimiento gradualmente. Además, deben tener la opción real de prestar o no el consentimiento para dicho tratamiento, y poder revocar el consentimiento en cualquier momento.

No obstante, y dado que puede haber casos en que los tratamientos masivos de datos se fundamenten en el **interés legítimo** del

---

[92] Dictamen 03/2013 sobre limitación del fin, p. 47.

[93] Según el GT29 (Dictamen 03/2013 sobre limitación del fin p. 47), salvaguardas tales como dar acceso directo a los interesados a sus datos en un formato portátil, fácil de usar y legible por máquina, puede ayudar a potenciar su papel y corregir el desequilibrio económico entre las grandes corporaciones y los interesados/consumidores en el ámbito de los tratamientos masivos de datos.

[94] Informe del ICO "Big data and data protection" p. 18.

Responsable, analizaremos a continuación dicho fundamento jurídico para el tratamiento.

Respecto al interés legítimo del Responsable "o de un tercero", (letra f), no puede confundirse el concepto de "interés legítimo" con el derecho a realizar una determinada actividad. El GT29 ha afirmado[95], aunque en relación al artículo 7 f) de la Directiva 95/46 pero teniendo muy presente el proyecto de RGPD y la necesidad de armonizar criterios en este aspecto, que no deberá utilizarse como "un último recurso" para situaciones raras o inesperadas en las que se considere que no son aplicables otros fundamentos jurídicos para el tratamiento, y que "no deberá automáticamente ni deberá en su uso de manera indebida basándose en la percepción de que es menos restrictivo que los demás fundamentos".

En relación al sector público, resaltar que el artículo 6.1f) del RGPD, a diferencia de la Directiva 95/46 (artículo 7 f), excluye expresamente al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones, lo cual quiere decir que el interés legítimo no podrá utilizarse como fundamento jurídico del tratamiento, debiendo recurrir a otros supuestos como por ejemplo el e)[96].

Para que el "interés legítimo" constituya fundamento jurídico de un tratamiento, debe realizarse una prueba de sopesamiento. Seguiremos en este punto la opinión del GT29 vertida en el Dictamen 06/2014.

En primer lugar, "interés" no es sinónimo de "finalidad" aunque lógicamente estén estrechamente relacionados. El interés se refiere al beneficio que se pueda obtener del tratamiento. Para que la prueba de sopesamiento se pueda realizar correctamente, el interés deberá ser

---

[95] Dictamen 06/2014 sobre el concepto de interés legitimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE.

[96] Cfr. interpretación ofrecida por el GT29 en el Dictamen 06/2014 p. 28, según la cual una interpretación literal ("estricta"), podría no excluir a las autoridades públicas de la utilización del interés legítimo como fundamento jurídico, ya que el tratamiento para la gestión y el funcionamiento adecuados de estas autoridades publicas no quedaría incluido en el "tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

"real y actual", no sirviendo intereses "demasiado vagos o especulativos". Los intereses puede ser de muy diversa naturaleza, y todos ellos pueden ser legítimos *a priori*, pero para que ese "interés legítimo" constituya el fundamento jurídico para un tratamiento de datos, siguiendo al GT29, deberá ser lícito; articulado con la claridad suficiente para permitir la prueba de sopesamiento en contraposición a los intereses y los derechos fundamentales del interesado; y un interés real y actual. Además, como en todos los supuestos de tratamiento de datos (excepto los fundamentados en el consentimiento), el tratamiento ha de ser *necesario,* en este caso para la satisfacción del interés legítimo, no existiendo otros medios menos invasivos para la satisfacción de dicho fin, en cuyo caso, dicho tratamiento no sería por tanto, *necesario.*

Con respecto a los "intereses o los derechos y libertades fundamentales del interesado" con los que se ha de sopesar el interés legítimo del responsable (o del tercero), deben interpretarse en sentido amplio[97], al igual que el concepto de "interés legítimo" del Responsable.

Para realizar la prueba de sopesamiento, siguiendo al GT29, deberá analizarse la naturaleza y la fuente del interés legítimo del Responsable y su impacto en los intereses o derechos del interesado. Si como resultado de dicho análisis obtenemos un equilibrio, o ante la duda de que éste se mantenga, es necesario adoptar determinadas medidas adicionales de garantía.

El interés legítimo del Responsable o de un tercero, puede originarse en el ejercicio de un derecho fundamental del mismo o bien en el interés del público o de la comunidad en general. También puede haber otros supuestos de interés legítimo, derivados de los otros casos

[97] Como bien señala el GT29 en el Dictamen 06/2014 p 36, " (…) a diferencia del caso de los intereses del responsable del tratamiento, el adjetivo «legítimo» no precede aquí´ al término «intereses» de los interesados. Esto implica un ámbito más amplio de protección de los intereses y derechos de las personas".

en que puede fundamentarse el tratamiento (e.g ejecución de un contrato, obligación jurídica etc).

En relación al impacto del tratamiento en el interesado, deberán analizarse cuestiones como la naturaleza de los datos personales (si se trata de datos sensibles o de "categorías especiales de datos", si fueron puestos a disposición del público con anterioridad o no), la manera en que se trata la información (si se tratan o combinan con otros datos, si se tratan a gran escala etc), la probabilidad del riesgo, la gravedad de las consecuencias en caso de materializarse el riesgo, las expectativas razonables de los interesados, si existe o no una posición "dominante" del Responsable y cualquier consecuencia del tratamiento de datos. Como afirma el GT29 sobre el concepto de impacto, "es un concepto mucho más amplio que daño o perjuicio a uno o más interesados en concreto". Es muy importante el carácter preventivo de la prueba de sopesamiento, es decir, que el tratamiento sólo se lleve a cabo una vez se ha llegado a la conclusión de que los tratamientos "no conllevan riesgo o conllevan un riesgo muy bajo de impacto negativo indebido sobre los intereses o los derechos y libertades fundamentales de los afectados".

Para una valoración global de la prueba de sopesamiento, deberán analizarse también las garantías adicionales adoptadas por el Responsable en su caso, tales como la eliminación posterior de los datos, la anonimización de los mismos, el establecimiento de un derecho del interesado de exclusión etc.

El GT29 destaca tres cuestiones en relación a la valoración en conjunto de la prueba de sopesamiento:

1. La relación entre la prueba de sopesamiento, la transparencia y el principio de responsabilidad:

El tratamiento basado en el interés legítimo se basa en el Principio de Responsabilidad por lo que el Responsable deberá analizar cuidadosamente todas las cuestiones vistas anteriormente en relación a la prueba de sopesamiento. "El concepto de responsabilidad está íntimamente ligado al de transparencia", por lo que el Responsable deberá poner en conocimiento de los interesados las razones por las

que considera que sus intereses prevalecen, las garantías adoptadas y, en su caso, el derecho de exclusión voluntaria.

2. El derecho de oposición al tratamiento por parte del interesado, y más allá de la oposición, la posibilidad e exclusión voluntaria sin la necesidad de justificación:

De la misma manera que el artículo 14 a) de la Directiva 95/46, el artículo 21.1 del RGPD establece el derecho del interesado a oponerse al tratamiento basado en el interés legítimo (artículo 6.1 f) del RGPD) en cualquier momento, "por motivos relacionados con su situación particular". Este derecho de oposición necesitará de una justificación del interesado de los "motivos relacionados con su situación particular", lo cual requerirá de un nuevo análisis. No obstante, a diferencia de la Directiva que únicamente contempla excepciones a este derecho de oposición derivadas de la legislación nacional, el RGPD introduce un nuevo supuesto en el que el Responsable podrá seguir tratando los datos a pesar del ejercicio del derecho de oposición del interesado, consistente en la acreditación de "motivos legítimos imperiosos" para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Consideramos que sobretodo en supuestos que excepcionan los derechos del interesado, no es en absoluto conveniente la utilización de términos jurídicos indeterminados, máxime en supuestos que legitiman el tratamiento de datos basados en los intereses legítimos del Responsable y a pesar de una oposición del interesado.

No obstante, el Responsable puede incluir, como una garantía adicional, un derecho de exclusión del interesado, que no necesite de ninguna justificación por su parte.

3. La portabilidad de los datos y la existencia de otros mecanismos para que el interesado acceda, modifique, elimine, transfiera o de otro modo reutilice sus propios datos.

Una vez vistos los posibles fundamentos jurídicos en los que puede basarse el tratamiento de datos masivos, continuaremos con los requisitos que deben adoptar dichos tratamientos.

El artículo 5.1 b) del RGPD establece que los datos personales deberán ser "recogidos con fines determinados, explícitos y legítimos, y *no serán tratados ulteriormente de manera incompatible con dichos fines*". Ya en el apartado cuarto del Capítulo I del presente trabajo se trató esta cuestión, pero resaltar que el párrafo cuarto del artículo 6 del RGPD no debe entenderse como un nuevo supuesto que legitime el tratamiento de datos, razón por la cual el GT29[98] abogaba por su supresión, ya que "así se asegura de que el requisito de uso compatible en el artículo 5 y la legalidad del tratamiento en virtud del artículo 6 continúan funcionando como **requisitos acumulativos**".

El GT29 en su Dictamen 03/2013 sobre limitación del fin, analiza cuándo un tratamiento de datos posterior debe considerarse incompatible. El GT29 establece en dicho Dictamen que el concepto de limitación de la finalidad tiene dos vertientes principales: los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, (fines específicos) y no pueden 'ser tratados posteriormente de manera incompatible' con esos fines (uso compatible). Respecto al "uso compatible", lo que se establece es una prohibición de realizar tratamientos ulteriores incompatibles con las finalidades para las que fueron originalmente recogidos los datos. El GT29 considera que al prohibir la incompatibilidad en lugar de exigir la compatibilidad, significa que el legislador ha querido dotar de cierta flexibilidad a los tratamientos posteriores. Un tratamiento posterior para un uso diferente, no tiene por qué implicar automáticamente la incompatibilidad ya que la compatibilidad necesita ser analizada caso por caso, afirma el GT29. En relación a la "evaluación de la compatibilidad", el GT29 se inclina por una evaluación sustantiva (en contraposición a una evaluación puramente formal), es decir, que tenga en cuenta la forma en que las finalidades deben ser entendidas, analizando todas las circunstancias relevantes, tales como:

-la relación entre las finalidades originarias del tratamiento y las finalidades del tratamiento posterior proyectado;

---

[98] Documento de 17/06/2015 disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

-el contexto en el que los datos personales fueron recogidos y las expectativas razonables de los interesados en relación a ese uso posterior;
-la naturaleza de los datos personales y el impacto que ese tratamiento posterior tendrá en los interesados;
-las medidas adoptadas por el Responsable para asegurar un tratamiento justo y para prevenir cualquier impacto indebido en los interesados.

Vemos cómo estos puntos, a pesar de la opinión del GT29 sobre su ubicación sistemática, se han incluido en el párrafo cuarto[99] del artículo 6 del RGPD.

En relación a posteriores tratamientos que utilicen técnicas de *big data*, para analizar si dichos tratamientos posteriores son compatibles, deberá realizarse la "evaluación de la compatibilidad" explicada anteriormente. Además, en el caso de *big data*, deben diferenciarse dos supuestos; en primer lugar aquellos tratamientos que únicamente buscan correlaciones en la información; en segundo lugar, aquellos tratamientos que buscan analizar a los individuos, sus preferencias y comportamientos. En el primer caso, el GT29 afirma que el concepto

---

[99] Artículo 6.4 RGPD: "Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".

de separación funcional puede ser un factor importante a la hora de decidir si dichos tratamientos posteriores son compatibles. Para el segundo caso, será necesario solicitar el consentimiento del interesado, tratado al comienzo del presente epígrafe.

CAPÍTULO V : APLICACIÓN DE LA REGULACIÓN ACTUAL: PROBLEMÁTICA

1.Control sobre nuestros datos personales

Como se analizó en profundidad en el capítulo I del presente trabajo, el derecho fundamental a la protección de nuestros datos de carácter personal, se basa en el poder de control de su titular sobre los mismos.
No obstante, y llegados a este punto, ¿realmente tenemos control sobre nuestros datos? ¿cómo podemos controlar algo que no sabemos que existe o que se está realizando?
En ocasiones se ha hablado de la "paradoja de la privacidad", consistente en que mientras los sujetos estamos concienciados sobre nuestra privacidad en línea y exigimos ser informados sobre cómo nuestros datos son manejados o explotados, a la vez estamos dispuestos a revelar información personal muy detallada a cambio de cualquier ganga o incluso por nada, en nuestras redes sociales[1]. Todo esto no hace sino aumentar esta "información auxiliar" o externa que puede ser utilizada para la reidentificación o la obtención de inferencias.
De hecho, algunos autores denominan "ilusión de control"[2], a la sensación de control que experimenta el usuario sobre el acceso por

[1] LAZARO, C., y LE MÉTAYER, D., "The control over personal data: True remedy or fairy tale?", Project-Teams Privatics, Research Report n. 8681, 13 abril de 2015, pp. 4 y 5.
[2] BRANDIMARTE, L., ACQUISTI, A., LOEWENSTEIN, G., y BABCOCK, L., (2009) "Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis", https://www.ideals.illinois.edu/handle/2142/15344

terceros a la información cuando es él mismo quien publica, confundiendo publicación con acceso.

Pero siguiendo a LAZARO y LE MÉTAYER[3], aun en el hipotético caso de que el responsable haya cumplido perfectamente con sus deberes de información y consentimiento, el interesado haya leído y por tanto, sea consciente del tratamiento que se va a realizar de sus datos, el sistema de privacidad basado en el control por parte del interesado asume que esa revelación de información no ha causado ningún daño a la privacidad. Es decir, estos autores señalan que la complejidad del entorno digital es tal que no podemos esperar que los interesados sean expertos en privacidad y soporten todos los riesgos y responsabilidades de la privacidad por sí solos. Por tanto, para ellos el control sobre la información no podrá ser efectivo mientras no se conciba e implemente como un compromiso compartido entre los diferentes actores implicados (humanos y no humanos).

En este sentido, los autores señalan que el RGPD ha introducido elementos en esta línea imponiendo nuevas obligaciones a los responsables, como por ejemplo el principio de responsabilidad en el cumplimiento (*accountability*), la obligación de realizar informes de impacto, la obligación de notificar brechas de seguridad (tanto a la autoridad de control como al propio interesado), y teniendo en cuenta también las situaciones donde hay un desequilibrio entre las partes (el Considerando 43 establece que el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento).

Muchas veces se afirma que dado que la normativa de protección de datos europea data de los albores del comienzo de internet, era necesario actualizarla, pero, ¿realmente ha conseguido este propósito? A la vez que se sostiene la necesidad de actualizar la normativa, se afirma[4] que los principios básicos de protección de datos establecidos, son adecuados para un contexto de big data; que "afirmar que los

[3] LAZARO, C., y LE MÉTAYER, D., *op. cit.,* pp. 23 y 24.
[4] ICO, *op. cit.,* p. 41.

Principios actuales no son adecuados, subestima su inherente flexibilidad".
A continuación analizaremos si la normativa en materia de protección de datos, y concretamente, el RGPD, ofrece las garantías suficientes para hacer frente a los nuevos retos que la sociedad de la información plantea.

2.Globalización

Llegados a este punto, somos conscientes de que todos los habitantes de esta sociedad de la información, con independencia de nuestra nacionalidad, somos objeto de los mismos problemas y sufrimos las consecuencias cuando nuestra privacidad se ve dañada. De hecho, a raíz de la irrupción del *big data*, a ambos lados del Atlántico, es cuando se está produciendo un debate sobre la efectividad de la anonimización o sobre el propio concepto de dato personal en Europa o *personal identifiable information* (PII) en EE.UU.
Esto, además de poner de manifiesto la universalidad del problema, está dejando entrever las fortalezas y debilidades de las diferentes concepciones jurídicas en torno al derecho de la protección de datos, principalmente la europea y la estadounidense.
Por tanto, ante un problema universal, necesitamos una solución, o al menos protección, global, lo cual actualmente, no existe, tal y como pone de manifiesto el Supervisor Europeo de Protección de Datos (SEPD)[5] "cuando los datos son comercializados o intercambiados a través de diferentes fronteras y jurisdicciones, la rendición de cuentas respecto al tratamiento de la información deviene nebulosa y difícil de determinar o hacer cumplir bajo la normativa de protección de datos sobre todo en ausencia de cualquier norma internacional" (la

[5] Opinion 4/2015 del Supervisor Europeo de Protección de Datos, *Towards a new digital ethics, data, dignity and technology*, de 11 de septiembre de 2015, p. 6, disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf

traducción es nuestra). Por tanto, la falta de una normativa aplicable a nivel internacional, es la primera deficiencia.

Además, la normativa existente, en Europa y EE.UU., ofrece muy diferentes niveles de protección. En EE.UU. como vimos en el capítulo III del presente trabajo, el derecho a la privacidad está configurado de forma muy diferente a Europa. La regulación se ha concebido de manera sectorial, por lo que no existe una regla general aplicable a cualquier tipo de dato personal lo cual supone que la normativa no es tecnológicamente neutra. Esto afecta enormemente en el ámbito del *big data*, que supone la necesidad de revisar[6] globalmente toda la regulación americana en materia de privacidad.

El GT29[7] ha manifestado su opinión en este sentido, afirmando (la traducción es nuestra) que, cuando sea necesario, iniciará labores de cooperación a nivel internacional con otros reguladores relevantes, para asegurar que la normativa europea de protección de datos se está aplicando de la mejor manera en relación al desarrollo del *big data*.

El GT29 afirma que es más que consciente de que la competencia internacional en materia de *big data* significa que los distintos marcos nacionales, regionales e internacionales de protección de datos y privacidad se pueden aplicar de forma simultánea a nivel mundial, lo cual puede conllevar importantes retos en términos de cumplimiento. En este sentido, el GT29 considera que es necesaria una mayor cooperación entre las autoridades de protección de datos y otras autoridades competentes a nivel mundial en estos temas. Esta cooperación es necesaria para proporcionar una guía unificada y respuestas operativas sobre la aplicación de las normas de protección

---

[6] Así se pone de manifiesto en el Informe *Big Data: Seizing opportunities, preserving values*, Executive Office of the President, Mayo 2014, disponible en https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf pp. 58 a 67.

[7] 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, 16 de septiembre de 2014, disponible en inglés en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

de datos a los jugadores globales, así como para implementar el cumplimiento conjunto de estas normas, siempre que sea posible. De este modo, el GT29 considera que promover la cooperación entre los reguladores internacionales en *big data* debe basarse firmemente en los diferentes marcos legales aplicables. En Europa, (siguiendo al GT29), los derechos concedidos a los interesados (transparencia, derechos de acceso, rectificación, cancelación, oposición, derecho al olvido) resultan de un derecho fundamental. Por tanto, son de aplicación general y sólo con limitadas excepciones previstas por la ley.

Vemos por tanto cómo el GT29 es consciente y está dispuesto a la cooperación internacional, siempre que se respeten los estándares europeos de privacidad.

En nuestra opinión, sería el escenario más favorable para el viejo continente, pero entendemos que la solución no pasa por la convivencia de diferentes regímenes legales en esta materia, que, como hemos visto, difieren en gran medida, tanto respecto a su concepción como a los niveles de protección que otorgan, ya que las fricciones serán constantes y la capacidad de hacer cumplir las diferentes normativas siempre quedará diluida o dificultada por muchos factores. La única solución factible y coherente, pasa por establecer un instrumento vinculante a nivel internacional (no una sucesión de principios y directrices de buenas prácticas), fruto de la cooperación de las diferentes partes implicadas, que sea jurídicamente vinculante para todas ellas.

En este sentido, estamos plenamente de acuerdo con RECIO GAYO[8] cuando, en relación a la protección de datos y la innovación, aboga por un "instrumento vinculante de carácter internacional, fácilmente adaptable, que sea resultado de la participación más amplia posible entre todas las partes interesadas y no meramente la propuesta de una o varias partes sin contar con las demás". Se trata de una solución para nada sencilla, ya que intentar crear un instrumento internacional que aúne y satisfaga a dos culturas jurídicas tan dispares en este punto,

[8] RECIO GAYO, M., Protección de Datos Personales e Innovación ¿(in) compatibles?, Reus, 2016, 1ª ed., p. 159.

resulta todo un reto, pero en nuestra opinión, es preferible a la imposición de normas o al establecimiento de mecanismos de cooperación o similares, ya que como afirma BRUENING[9] (la traducción es nuestra), ha quedado claro que los intentos de imponer las sensibilidades en materia de privacidad o los regímenes de protección de un país o región a otra, suelen resultar frustrados. Pero los Principios para una justa información de las prácticas (*Fair information practices Principles),* reconocidos a nivel internacional, siguen proporcionando un lenguaje común sobre la protección de datos y privacidad que ha servido a las naciones, regiones , empresas e individuos de todo el mundo, sin exigir una desviación de los valores locales de privacidad. Y cuando hay un fallo de privacidad o protección de datos, proporcionan una herramienta para medir el nivel de adecuación a la normativa (*compliance*) y un medio para exigir su cumplimiento.

Es por ello que, al menos, tal y como se ha visto en capítulo II del presente trabajo, tendríamos como punto de partida común las Directrices de la OCDE[10]. En este sentido también RECIO GAYO afirma que "el instrumento no partiría de cero, sino que puede y debe basarse en la amplia experiencia acumulada a lo largo de los años en la aplicación de normas tales como las Directrices de la OCDE o el Convenio 108 del Consejo de Europa, o en la adopción de otros instrumentos, como por ejemplo la Resolución de Madrid".

Como hemos afirmado anteriormente, ante un problema universal se requiere una solución también universal para que sea efectiva. Cuanto antes sean conscientes de ello las autoridades implicadas, antes obtendremos la solución a los retos/riesgos que para la privacidad plantea la sociedad de la información actual.

---

[9] BRUENING, P., "Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy", 19 octubre de 2014, disponible en http://blogs.intel.com/policy/2014/10/19/rethink-privacy-2-0-fair-information-practice-principles-common-language-privacy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IntelPolicy+%28Policy%40Intel%29

[10] Recordemos que tanto la OCDE como el Consejo de Europa revisaron la declaración original americana de las *Fair Information Practices (FIPs)*.

Ya lo dijo la Comisión Europea[11] "Dealing with personal data across borders requires a **clear and harmonised legal framework** that provides the right balance between individuals' potential privacy concerns and the exploitation of the potential of the reuse of large amounts of data", sólo que estaba pensando a nivel europeo, la armonización que traerá el RGPD.

3.Problemas con actuales figuras

El ICO afirma[12] tajantemente que "No aceptamos el argumento de que los principios de protección de datos no son adecuados para sus fines en el contexto de grandes volúmenes de datos. Big data no es un juego que se juega con reglas diferentes. Hay cierta flexibilidad inherente a los principios de protección de datos. Ellos no deben ser vistos como un obstáculo para el progreso, sino como el marco para promover los derechos de privacidad y como un estímulo para el desarrollo de enfoques innovadores a la información y a la participación del público".
Estamos de acuerdo con la afirmación de que el *big data* no debe ser una excepción en el cumplimiento de la normativa de protección de datos. No obstante, con respecto a la aludida flexibilidad de los principios de protección de datos, veremos como ésta no es suficiente para garantizar los derechos de las personas, pues ¿acaso no se ha aprobado un nuevo RGPD para actualizar la normativa que había quedado obsoleta ante la realidad de los nuevos tratamientos de datos? Si los Principios existentes son lo suficientemente flexibles como para acoplarse a las nuevas realidades y tratamientos actuales y futuros,

[11] *A European strategy on the data value chain*, European Commission DG CONNECT, disponible en inglés en http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=3488 , p. 18.
[12] Informe del ICO, *op. cit.*, p. 4, epígrafe 17 (la traducción es nuestra).

¿dónde queda esa necesidad de adaptación o modificación de la normativa?

Una de las conclusiones del Consejo Europeo de octubre de 2013[13] era "fomentar la confianza de los ciudadanos y de las empresas en la economía digital. La adopción a su debido tiempo de un *sólido marco general de la UE para la protección de datos* y de la Directiva sobre ciberseguridad es esencial para la realización del Mercado Único Digital para 2015".

Así, la propia Comisión Europea[14] afirmaba en 2014 que "El paquete de reformas de la Comisión tiene como objetivo construir un *marco de protección de datos único, moderno, robusto, coherente y exhaustivo para la UE*. Mediante el fortalecimiento de la confianza de los individuos en el entorno digital y la mejora de la seguridad jurídica, se proporcionará un marco normativo esencial para el desarrollo de bienes y servicios de datos innovadores y sostenibles".

La Comisión afirmaba también que "La legislación horizontal sobre consumidores y mercadotecnia se aplica también a los productos basados en la tecnología de macrodatos. La Comisión velará por que las pyme y los consumidores, proveedores y usuarios reciban toda la información necesaria, no sean inducidos a error y puedan contar con contratos justos, especialmente en lo que se refiere a la utilización de los datos que se les recogen. Estas medidas construirán la confianza necesaria para explotar todo el potencial de la economía de los datos".

Analicemos a continuación las novedades introducidas por el RGPD y si constituye el mencionado "marco de protección de datos único, moderno, robusto, coherente y exhaustivo para la UE" que otorgue la mencionada confianza a los usuarios y seguridad jurídica a todos los

---

[13] EUCO 169/13, Conclusiones del Consejo Europeo, 25 de Octubre de 2013, disponible en http://data.consilium.europa.eu/doc/document/ST-169-2013-INIT/es/pdf

[14] COM/2014/0442 final, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Hacia una economía de los datos próspera*, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014DC0442&from=EN

intervinientes, tan necesarias para el desarrollo de la innovación con respeto a los derechos fundamentales de las personas.

3.1 Concepto de dato personal

El Supervisor Europeo de Protección de Datos manifestó[15] que "la propia noción de datos personales podría cambiar radicalmente a medida que la tecnología permita cada vez más reidentificar a los individuos a partir de datos supuestamente anónimos".
El RGPD[16] mantiene la tradicional definición de "datos personales" ("toda información sobre una persona física identificada o identificable") pero además precisa que se considerará "identificable" cuando su identidad pueda establecerse "mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".
El Considerando 30, en la misma línea establece que "Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas". Resulta extraordinariamente revelador que la Propuesta de Reglamento[17]

[15] Dictamen 4/2015 Hacia una nueva ética digital. Datos, dignidad y tecnología, 11 de septiembre de 2015, p. 16, disponible en castellano en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_ES.pdf
[16] Artículo 4.1 RGPD.
[17] Según la Propuesta del Consejo de la UE, de 11 de junio de 2015. En versiones anteriores "De ello se deduce que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos no

incluyera una última frase "*Los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos no deben ser considerados datos de carácter personal cuando no sirvan para identificar o hacer identificable a un individuo*", que la versión definitiva eliminó por completo. Con ello, podemos concluir que no se ha querido dejar lugar a duda de que los identificadores, etiquetas y similares, son considerados datos de carácter personal. De hecho, el GT29[18] recomendaba la modificación de dicha frase justo en el sentido contrario al que constaba en la Propuesta: "los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos deben, por norma ser considerados datos de carácter personal" .

Siguiendo a KOOPS[19], este autor sostiene que el hecho de incluir en la definición a los identificadores de reconocimiento ("*recognition identifiers*"), dará lugar a un gran debate sobre si los identificadores en línea (e.g. las cookies) deben considerarse o no datos personales, aunque, como hemos visto, a partir de una interpretación literal de la norma queda claro que sí. KOOPS sostiene que, aunque el uso de identificadores de reconocimiento puede suscitar cuestiones que afecten a la privacidad, no todos los identificadores funcionan igual y que tendría sentido por tanto que la normativa diferenciase los diferentes tipos de identificadores. Sostiene que lo que establece el RGPD es una aproximación tipo del "todo o nada" (o es dato personal o no lo es), sin tener en cuenta situaciones intermedias. En este

---

necesariamente tienen que ser considerados datos de carácter personal en toda circunstancia".

[18] El GT29, en su Dictamen 8/2012, p 7, afirma que "la última frase podría dar lugar a una interpretación indebida restrictiva del concepto de datos personales en relación, por ejemplo, con las direcciones IP o la identificación de los chivatos (cookies). El Grupo de Trabajo recuerda que todos los datos personales se refieren a una persona identificable: «(un) dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en se la trata o se la evalúa »

[19] KOOPS, B. J., 'The trouble with European data protection law', *International Data Privacy Law*, 2014, DOI: 10.1093/idpl/ipu023, p. 9.

sentido KOOPS considera[20] que la normativa de protección de datos sería más productiva si, en lugar de tratar de establecer una frontera entre lo que se considera dato personal y lo que no, creásemos categorías de datos cuyo tratamiento causa ciertos efectos en las personas, independientemente de si se refieren o no a individuos identificables.

En relación a "nuevas" categorías de datos, ABRAMS[21] realiza un interesantísimo análisis que expondremos a continuación.

Tradicionalmente se ha puesto el énfasis en los datos que provienen del individuo, de modo que el origen del dato y su recogida se producían en el mismo momento, cumpliendo entonces con el derecho de información y principio del consentimiento. ABRAMS realiza una clasificación de categorías de datos en función de su origen, del modo en que fueron originados, distinguiendo cuatro principales categorías y diferentes subcategorías:

- datos "facilitados" (provided): obtenidos de acciones realizadas directamente por el interesado y por tanto, éste es plenamente consciente de la generación de datos.

A su vez, distingue tres subcategorías, los datos "de inicio" (initiated) refiriéndose a los creados cuando se comienza una relación contractual, registro en una página web, solicitud de un préstamo etc.; los datos "transaccionales" (transactional) en relación a los generados durante una transacción, e.g. compraventa mediante una tarjeta de crédito, responder a un cuestionario etc. En estos casos el individuo puede no estar pensando que se están generando unos datos pero entiende que la transacción sea grabada en un archivo. Por último, los datos "publicados" (posted) en relación a todos aquellos datos creados y publicados voluntariamente por el interesado (e.g. publicaciones en redes sociales).

- datos "observados" (*observed*): aquellos que son observados y grabados. Distingue a su vez tres subcategorías, los datos

---

[20] KOOPS, B. J., *op. cit.,* p. 13.

[21] Hacia un nuevo derecho europeo de protección de datos, RALLO LOMBARTE, A. (coord.), GARCÍA MAHAMUT, R. (coord.), Tirant lo Blanch, 1ª ed., 2015, Data origin and the proposed regulation, MARTIN, ABRAMS pp. 85 a 101.

"involucrados"(*engaged)* en referencia a los generados en una conexión de internet, los obtenidos a través de cookies, tarjetas de fidelización, vestibles (*weareables*) etc*,* datos "no anticipados" *(not anticipated)* los captados a través de sensores en el denominado Internet de las cosas; "datos pasivos"*, (passive)* englobando todos aquellos supuestos en los que es muy difícil para el individuo ser consciente de que está siendo observado y a la vez, creando datos (e.g. cámaras en un sitio público combinadas con un sistema de reconocimiento facial).

- datos "derivados" (*derived*): para ABRAMS son aquellos datos derivados de otros datos de forma mecánica creando por tanto nuevos datos sobre el individuo. Distingue dos subcategorías, los datos derivados "computacionales" (*computational*) que son los generados a partir de procesos aritméticos a partir de datos numéricos existentes (e.g. en una tienda en línea, calcular el tiempo medio de cada visita un médico calcula la probabilidad de contraer una determinada enfermedad basada en la genética del concreto individuo etc.) en definitiva, aquellos casos en que el individuo no sería consciente de la creación de estos nuevos datos y los datos derivados "hipotéticos" (*notional*), datos creados a partir de la inclusión del individuo dentro de un grupo con el que comparte determinadas características, es decir, los grupos de segmentación característicos del marketing.
- datos "inferidos" (*inferred*): aquellos datos productos de un proceso analítico basado en la probabilidad. Dentro de los datos inferidos, distingue dos subcategorías, los datos "estadísticos" (*statistical*) en referencia a los obtenidos a partir de un proceso estadístico (e.g. calificación de riesgo crediticio, riesgo de fraude etc.), en los que el individuo no está al corriente y los datos "analítica avanzada" (*Advanced Analytical*) en relación a los obtenidos a través de técnicas de *big data.*

Según ABRAMS, los datos "provistos" y los "observados" proceden directamente del interesado, mientras que los "derivados" e

"inferidos" son producto del tratamiento de otros datos existentes, pero una vez generados, todos ellos conforman la base para la creación de nuevos futuros datos. ABRAMS opina que los datos inferidos sustituirán a los derivados, por lo que el individuo no será consciente ni por tanto, podrá mitigar su efecto a través del ejercicio de sus derechos o consentimiento. En este sentido, ABRAMS pone de manifiesto que el RGPD, al igual que la Directiva 95/46, centra toda su atención en el momento de la recogida de datos, que asocia con la creación, el origen de los datos, y por tanto, los datos inferidos quedarían fuera, pues no hay referencia a la creación de los datos, sino a cuándo estos son recogidos. ABRAMS apunta a que el Principio de Finalidad del artículo 5 del RGPD ("los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines") puede interpretarse en el sentido de que las finalidades al crear nuevos datos a partir de los datos recogidos, deben no ser incompatibles con las finalidades especificadas en el momento de la recogida, por lo que cualquier inferencia adicional sería incompatible con dichas finalidades originarias. Tampoco el artículo 6 que hace referencia a las bases legales para un tratamiento lícito menciona expresamente el concepto de datos generados, y el Principio de transparencia, gira en torno a las finalidades específicas y el consentimiento del individuo, por lo que según ABRAMS, en relación a los datos derivados, la transparencia sólo puede existir cuando se especifique entre las finalidades del tratamiento, la generación de nuevos datos como una de las finalidades.

En el mismo sentido, SEMPERE[22] citando a CAO, resaltan la diferencia entre los conceptos "dato de carácter personal" e "información de carácter personal". Así, CAO pone de manifiesto que al agregar a un fichero que contiene datos de carácter personal, información que en sí misma no constituye propiamente datos de carácter personal, se consigue "correlacionar datos" que permiten inferir o deducir "informaciones nuevas" sobre la persona. CAO afirma que "al añadir

[22] SEMPERE SAMANIEGO, F. J., *op. cit.*, pp. 162 y 163.

un conjunto de datos no personales que sirven para "etiquetar o colorear" los datos existentes, conseguimos más que la suma de las partes originales". En este sentido también se manifiesta la Autoridad de protección de datos de Reino Unido, ICO, (la traducción es nuestra) "la analítica de *big data* también tiene el potencial de crear nuevos datos de carácter personal. Por ejemplo, las redes sociales (social media) y otros datos acerca de un individuo podrían ser analizados para averiguar sobre el estilo de vida de esa persona como un factor en la determinación de su calificación de crédito, o si están en riesgo de desarrollar una enfermedad. Del mismo modo, los sensores en los automóviles ofrecen grandes cantidades de datos sobre el coche, pero esto también se pueden utilizar para identificar los patrones de comportamiento de conducción de las personas, que pueden ayudar en la toma de decisiones acerca de sus primas de seguro"[23].

En relación a los datos suministrados por el afectado y los datos "inferidos o calculados", al igual que ABRAMS, CAO, afirma que "afectaría al deber de información dado que al usuario habría que indicarle que ciertos datos que vaya a suministrar serán transformados en información que permitirá la explotación de otras finalidades".

No podemos estar más de acuerdo con estos autores y esta es una de las principales cuestiones que planteamos en el presente trabajo.

Quizá no sea necesaria una categorización de los datos tan exhaustiva como la realizada por ABRAMS, pero lo que está claro es que el concepto de "dato personal" puede encerrar matices suficientes como para plantearnos la creación de nuevas categorías de datos, que permitan adoptar diferentes medidas, tanto en la creación como en la recogida y tratamiento de los datos, en definitiva, tratar de manera diferente lo que no es igual, dada la amplitud y expansión actual del concepto de "datos personales".

En relación al concepto de dato de carácter personal, el RGPD no ha aportado ninguna "innovación" o nueva categoría de datos, sino que

---

[23] Informe de ICO, *UK Information Commissioner's Office*, "*Big data and data protection*", 28 de Julio de 2014, disponible en https://ico.org.uk/media/1541/big-data-and-data-protection.pdf p 11, epígrafe 38.

se ha limitado a ampliar su definición (e.g. identificadores en línea). Como afirma ABRAMS, el RGPD ha sido redactado sin tener en cuenta las nuevas categorías de datos, o, añadimos, las especificidades que plantean los nuevos tratamientos de datos. Para BERGKAMP[24], la legislación sobre privacidad busca proteger la privacidad pero ampliando la cantidad (el concepto) de datos identificables incrementa los riesgos para la misma.

Si pensamos en los orígenes del derecho a la protección de datos, en cómo y cuándo apareció este derecho, vemos que fue cuando la amenaza que iban suponiendo los avances tecnológicos para la intimidad de los individuos, fue creando un riesgo considerable para la libertad y libre desarrollo de los individuos, obviamente dignos de protección.

En la actualidad, el riesgo no procede sólo de "la informática" en sí misma considerada sino de lo que podemos hacer a través de ella. De lo anterior podría argüirse que en aquel momento también se estaba protegiendo "de lo que la informática pudiera hacer", pero nos referimos a que quizá podríamos estar ante una nueva situación en la que no sólo se vean afectados los datos de carácter personal, sino una nueva manera de acumular y tratar la información sobre las personas que, sin afectar supuestamente a sus datos de carácter personal, o al menos, no directamente, esté produciendo una injerencia en un aspecto de su personalidad digna de protección.

Ello nos lleva a plantearnos que podríamos estar ante un nuevo derecho fundamental o ante una evolución del derecho a la protección de datos de carácter personal lo que supondría la aparición de una nueva categoría de "datos" o derecho afectado.

Por el contrario, podemos concluir también que lo anterior carece de sentido, pues desde el momento en que pueda vincularse determinada información a una persona, entrará en acción el derecho a la protección de datos de carácter personal y para el caso en que los

---

[24] BERGKAMP, L., "The privacy fallacy: adverse effects of europe's data protection policy in an information-driven economy", *Computer Law & Security Report*, vol. 18, n. 1, 2002, p. 37.

datos o la información no sean relativos a, ni se puedan vincular a una persona, no hay nada digno de protección, por lo que carece de sentido crear un nuevo derecho o un nuevo significado o vertiente en el derecho a la autodeterminación informativa o protección de datos de carácter personal. Siguiendo este argumento, la clave radica en garantizar el anonimato de forma que sea absolutamente irreversible. Pero, ¿estamos en disposición de poder garantizar algo así? Máxime si tenemos en cuenta el vertiginoso avance y posibilidades que las tecnologías pueden llegar a ofrecernos, siendo plenamente conscientes de que algunas de esas posibilidades son inimaginables a día de hoy.

Entonces, quizá convenga extender la protección del derecho a la protección de datos a toda "información" referente a una persona, sea o no un dato de carácter personal, es decir, la haga identificable o no, de la misma manera que en el pasado se extendió la protección del derecho a la intimidad, a lo no íntimo, a través del derecho a la protección de datos de carácter personal. Todo ello siempre amparándonos en el mandato establecido por el artículo 18 párrafo cuarto de nuestra Carta Magna, *limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

Es decir, del mismo modo que se comenzó a proteger la información personal, fuera ésta íntima o no íntima, en la actualidad debemos plantearnos si es necesario proteger no sólo la información personal (relativa a una persona identificable), **sino la información relativa a personas, sean o no éstas identificables.** Es decir, no se trata de ampliar el concepto de dato personal, sino de establecer medidas de protección sobre aquella información que, sin encajar propiamente en el concepto de "dato personal", pueden llegar a serlo.

Y la razón de este argumento, vendría dada por los riesgos que para la privacidad pueden suponer las posibilidades que la tecnología (ya no "la informática") puede llegar a conseguir y de las que no somos conscientes ahora. No se trata de proteger una injerencia "futurible", sino de proteger esa categoría de información que puede llegar a convertirse en "datos personales" pero que de momento no lo son y

aparentemente no lo serán nunca por considerarse "irreversiblemente" anonimizados.

A priori puede parecer un argumento descabellado y carente de toda lógica o sistemática, pero si pensamos en un incidente, no es lo mismo que se hayan seguido unas determinadas pautas para la recogida y tratamiento de esa información, que la total falta de control en lo que respecta a la información, caso en el que todo quedaría en un "mero" incidente de seguridad sin consecuencias aparentes, mientras que en el escenario planteado, podríamos reclamar responsabilidades al Responsable de dichos datos o fichero de información. ¿Quiere lo anterior decir que siempre que estemos ante tratamientos de información relativas a personas habrá un responsable de todo posible ataque sufrido por dicha información? Lógicamente no. Incluso la persona puede haber rechazado de origen verse implicada, rechazando que sus datos participen y sean utilizados para análisis masivos de información. Lo cual a su vez podría llevarnos a que dichos análisis sean menos fiables al verse considerablemente reducida la muestra o la representatividad de la muestra obtenida.

Todo lo cual nos lleva a plantearnos la ineficacia de la regulación actual a la vista de su incapacidad de protección ante el fenómeno del *big data.*

Del mismo modo que fue la informática la que nos descubrió el derecho fundamental de protección de datos de carácter personal, llegando a abarcar a los datos no automatizados actualmente, los tratamientos de datos masivos (*big data*) pueden estar descubriéndonos un nuevo derecho o como mínimo, una *nueva* forma de injerencia en la privacidad de las personas. Y para proteger debidamente los derechos de los interesados, resulta necesario en nuestra opinión crear una **nueva categoría de información protegible**, sin necesidad de ampliar el ya de por sí amplio concepto de "dato personal". Bien podría considerarse que, si esta nueva categoría de información protegible lo es porque puede llegar a constituir "dato personal", podría quedar englobada en el concepto de "dato personal" por ser "identificable" y por tanto, no sería necesario crearla; pero como apuntamos, esto constituiría una expansión

injustificada del concepto de dato personal que nos llevaría a considerar dato personal a toda información relativa a personas, sólo por el mero hecho de poder llegar a ser un día identificables, no por serlo actualmente.

Entonces el problema radica en trazar la delimitación entre "información protegible" y "dato personal". Una posible solución podría ser, como apunta KOOPS[25], en lugar de tratar de delimitar dicha frontera entre dato personal y no personal, establecer aquellas categoría de datos o información que pueden tener efectos sobre las personas, con independencia de si son relativos a personas identificables o no.

O tratar como "información protegible", toda aquella que pueda afectar a las personas, sin constituir dato personal porque "teniendo en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona[26] para identificar directa o indirectamente a la persona física" y "todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos", se concluye que no existe una "probabilidad razonable de que se utilicen medios para identificar a una persona física" (Considerando 26 RGPD).

Hay autores (BERGKAMP, MAYER) que consideran que en lugar de poner el énfasis en el concepto de dato personal, éste debe situarse en el "tratamiento", es decir, en la utilización del dato. Consideran que los datos ya no son el epicentro sobre el que se desarrolla la normativa de protección de datos, sino que dicho epicentro es la **utilización** del

---

[25] KOOPS, BJ., , *op. cit*., p. 13, "Just as light sometimes acts as a particle and sometimes as a wave, data sometimes act as personal data and at other times as non-personal data, and we simply cannot always predict which of the two occurs. For certain types of data processing, such as the use of tracking cookies, profiling, and Big Data Analytics, it does not matter that much whether data are particles or waves, if they can be treated jointly as light that is canalised in certain ways".

[26] Nótese que además del Responsable del tratamiento, el RGPD menciona a "cualquier otra persona", lo que pone de manifiesto 1) la preocupación del RGPD por asegurar la no identificabilidad 2) la posibilidad de exigir responsabilidades a personas distintas del Responsable.

dato, las **finalidades** del tratamiento. Si el interesado consiente a unas finalidades determinadas y no a otras, será indiferente la potencialidad del dato, es decir, si por ejemplo una cookie se utiliza para recordar las preferencias de navegación de un usuario por una determinada web, no podrá utilizarse para identificar al individuo u obtener otro tipo de información vinculada a su persona.
En otras palabras, por qué tratar a una cookie como un dato de carácter personal, cuando no va a ser utilizada para otras finalidades distintas a las consentidas, y que, en su caso, justificarían su categorización como dato personal. Ahora bien, aquí el párrafo cuarto del artículo 6 del RGPD que permite tratamientos para fines distintos pero "compatibles" a los consentidos en el momento de la recogida, pondría en tela de juicio este razonamiento y lo haría inviable.

3.2 El individuo no decide

El derecho fundamental a la protección de datos, como vimos en la parte I del capítulo II, otorga un haz de facultades al individuo que le permitan ejercer un poder de disposición sobre sus datos. Es por ello que el consentimiento es el principal cimiento en el que se basa la normativa.
No obstante, los retos que la evolución tecnológica, y en concreto, el *big data*, plantean a la normativa actual en materia de protección de datos, hacen que muchas veces no sea posible obtener ese consentimiento previo que legitime la recogida y tratamiento de datos. En otras palabras, la capacidad de control del individuo es inversamente proporcional a la innovación tecnológica, ¿cómo pedir consentimiento sobre un tratamiento que no sé que realizaré en un futuro? ¿cómo pedir consentimiento a todas aquellas personas cuyos datos obtuve en principio anonimizados o seudoanonimizados?
Como pone de relieve ABRAMS[27], internet ha facilitado el crecimiento exponencial de lo que este autor denomina "*observational data"*, es decir, información sobre el comportamiento del individuo que no

[27] RALLO LOMBARTE, A., *op. cit.*, p. 89.

precisa de ser facilitada por éste en forma de datos personales (rellenando un formulario por ejemplo), sino que son los micropasos que conducen a esas acciones la información (observada) que es recogida y procesada. ABRAMS resalta que la combinación de información obtenida en el mundo físico junto con la observada en internet, han facilitado la expansión masiva de los datos observacionales. En estos casos, el individuo no ha contribuido a la originación de esos datos.

Es por ello que, en determinados casos, el consentimiento no es viable y por ello, el individuo ni decide, ni puede decidir.
¿Significa ello que hemos de resignarnos ante la evolución tecnológica y admitir por defecto que hay una parte de nuestra privacidad que no podemos controlar?
En nuestra opinión, la respuesta no puede ser afirmativa, no podemos admitir una "pérdida de privacidad colateral" sólo porque no sepamos, o no queramos, establecer las medidas de protección oportunas. Tal y como afirma el ICO, "La aparente complejidad del análisis de grandes volúmenes de datos no debe convertirse en una excusa para dejar de obtener el consentimiento cuando así se requiera. Las organizaciones deben encontrar el punto en el que explicar los beneficios de los análisis y ofrecer al usuario una elección significativa -y luego respetar esa elección cuando se están procesando sus datos personales"[28].
En el caso de los datos inferidos, tal y como comentamos anteriormente, coincidimos plenamente con ABRAMS y CAO en el sentido de que es posible, y debe hacerse así, obtener el consentimiento del interesado para utilizar datos provenientes de otras fuentes externas, o para otras finalidades, que permitan al Responsable obtener una mayor y más específica información sobre el interesado, que redunde en una mayor personalización y por tanto efectividad para el Responsable.

---

[28] Informe de ICO, *UK Information Commissioner's Office*, "*Big data and data protection*", 28 de julio de 2014, disponible en https://ico.org.uk/media/1541/big-data-and-data-protection.pdf p. 19, epígrafe 60.

Para aquellos casos en que el consentimiento ya no pueda ofrecernos todas las respuestas, deberemos introducir **nuevas medidas destinadas a garantizar la protección de este derecho fundamental**. Estas nuevas medidas pueden poner el centro de atención en el Responsable, exigiéndole determinadas garantías en relación a la anonimización, basándonos en el Principio de responsabilidad en el cumplimiento. Otras medidas serían de carácter preventivo, evitando la recopilación de datos que funcionen o puedan funcionar como identificadores, como por ejemplo, el número único[29] que puede generarse a partir del nivel de batería restante del dispositivo que es recogido por la página web para, en principio, desactivar determinadas funcionalidades que reduzcan la duración de la batería y así generar más tiempo de navegación para el usuario.

Estas "nuevas medidas" destinadas a garantizar el derecho fundamental de protección de datos que vendrían a suplir la no adecuación del consentimiento para todos los supuestos que se plantean en el mundo actual, deberán recaer exclusivamente sobre el Responsable de dicho tratamiento, ya que la participación del individuo es imposible, con la única excepción de que existiera un derecho de exclusión para este tipo de tratamientos masivos.

Por tanto, deberán extremarse las precauciones en lo referente a la anonimización de los datos, realizar revisiones periódicas de las técnicas de anonimización, y establecer prohibiciones respecto a las bases de datos seudonimizadas, como por ejemplo que no puedan integrarse diferentes bases de datos seudoanonimizadas, ya que de lo contrario daríamos lugar a un riesgo de reidentificación.

En cuanto a la posibilidad de que el interesado pudiese manifestar *a priori* la negativa a que sus datos sean objeto de tratamientos masivos de datos (*big data*) como una suerte de *opt-out* o lista de exclusión.

---

[29] OLEJNIK Ł., ACAR G., CASTELLUCCIA C., DÍAZ C. (2016) "The Leaking Battery", en GARCÍA-ALFARO, J., NAVARRO-ARRIBAS, G., ALDINI, A., MARTINELLI, F., SURI, N., "The leaking battery, A Privacy Analysis of the HTML5 Battery Status API", (eds.) Data Privacy Management, and Security Assurance. DPM 2015, QASA 2015. Lecture Notes in Computer Science, vol. 9481. Springer, Cham, disponible en http://eprint.iacr.org/2015/616.pdf

Pero si pensamos en llevar esta medida a la práctica, además de que iría en detrimento de la fiabilidad de las conclusiones obtenidas a través de técnicas de *big data*[30], nos damos cuenta de que resulta inviable. Podríamos pensar que habilitar tal derecho de exclusión significaría la creación de una base de datos de incalculable magnitud que los Responsables tuvieran que cruzar antes de realizar tratamientos de datos masivos, lo cual resulta absurdo a todas luces, sobretodo si los datos personales se encuentran seudoanonimizados. Es por ello que en lo que sí podríamos pensar es en un **derecho de exclusión técnico y a priori**[31]**.**

La exclusión técnica requeriría que los protocolos informáticos con los que se construyen los sistemas de comunicaciones y publicación de información contemplaran la posibilidad de que el usuario manifestara su voluntad de que sus datos no sean objeto de tratamientos masivos. Esta posibilidad no es para nada remota, pues ya en 2009 se ofreció la posibilidad a los usuarios de los navegadores de que pudieran especificar su deseo de no ser rastreados mediante el mecanismo Do Not Track (DNT)[32].

Como muy bien afirma ÁLVAREZ GARCÍA, "el mecanismo DNT, al no formar parte de los estándares HTTP y HTML presenta una adopción irregular e inconsistente en los diferentes navegadores y además ha sido cuestionado por haber sido implementado como mecanismo de *opt-out* cuya configuración por defecto es la que permite el rastreo, y por tanto no sigue el paradigma del *privacy by design"*. Si bien actualmente el mecanismo DNT no forma parte de los estándares, está propuesto como candidato a ser incluido en los estándares sobre los

---

[30] Como afirma SEMPERE, F. J.,"a mayor información, más oposición y menos beneficio económico" en *op. cit.*, p. 170.

[31] Agradecer la inestimable ayuda para la redacción de este apartado a ÁLVAREZ GARCÍA, R., Ingeniero de Sistemas y consultor de PRODAT CATALUNYA.

[32] Mecanismo Do Not Track (DNT) propuesto en el año 2009 por varios investigadores (http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html), que permite a los usuarios de los programas de navegación en Internet especificar que no quieren que su actividad en línea sea rastreada, tratamiento frecuentemente realizado con finalidades de publicidad comportamental en línea.

que se construye el WWW definidos por el consorcio W3C (https://www.w3.org/TR/tracking-dnt/).

Trasladando esta idea al tratamiento de datos masivos, vemos cómo es perfectamente posible que los usuarios de internet puedan manifestar su negativa a que sus datos se utilicen en tratamientos masivos. Estos mecanismos podrían formar parte del navegador (que podría avisar al usuario del envío de datos a Internet, el posible tratamiento masivo de éstos y la posibilidad de negarse a ello) o bien de la página web (que podría permitir al usuario indicar si autoriza o se niega a que su comentario sea utilizado en tratamientos masivos). Una modificación del estándar HTML permitiría indicar si un bloque de información debe ser o no utilizado en un tratamiento masivo de datos.

De este modo, los motores de recolección de datos deberían ser modificados para contemplar la posibilidad de excluir los bloques marcados para no ser tratados masivamente.

Respecto al tratamiento masivo de datos obtenidos de los dispositivos conectados a redes o internet, desde ordenadores, dispositivos móviles, hasta cualquier objeto conectado al "Internet de las cosas", los usuarios que no desearan que los datos de conexión o tráfico de sus dispositivos fueran tratados masivamente, deberían poder especificarlo en la "configuración" del dispositivo. Para hacer efectivos estos mecanismos de "consentimiento" o de "manifestación de voluntad" deberían ser incorporados en los estándares de comunicaciones de Internet.

Por tanto, vemos cómo técnicamente es posible establecer los mecanismos para que los usuarios puedan manifestar su deseo de no participar en tratamientos masivos de datos. No obstante, dependerá de multitud de factores que esto se llegue a implementar. Pensemos que el mecanismo DNT todavía no está implantado a nivel de todos los navegadores, por lo que queda mucho camino por recorrer.

3.3 Vigencia del principio del consentimiento

El Principio del consentimiento, tal y como ha sido explicado en el capítulo II[33], sigue estando plenamente vigente con el RGPD, ya que éste sigue siendo el principal supuesto para que el tratamiento de datos sea lícito (artículo 6.1 a). Pero como hemos visto anteriormente, hay supuestos en los que el individuo no decide ni puede decidir.

El RGPD define el consentimiento como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".
A diferencia de la Directiva 95/46[34], el RGPD[35] no exige que el consentimiento sea "inequívoco", simplemente se dice que "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su *consentimiento* para el tratamiento de sus datos personales para uno o varios fines específicos", lo cual tampoco tiene mayor trascendencia si acudimos a la definición de consentimiento dada por el RGPD, que exige que sea una manifestación de voluntad *inequívoca*, específica y manifestada mediante una declaración o una clara acción afirmativa. No obstante lo anterior, destacar que para el tratamiento de categorías especiales de datos, sí se especifica que el consentimiento sea "explícito"[36].
El RGPD establece una serie de condiciones[37] para que el consentimiento sea válido. Para empezar, la carga de la prueba de que

[33] Ver concretamente el apartado 1.2.2.4.3.
[34] Artículo 7 Directiva 95/46 "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a)el interesado ha dado su consentimiento de forma inequívoca (…)".
[35] Artículo 6.1 a).
[36] Artículo 9.2 a) RGPD "a) el interesado dio su consentimiento *explícito* para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
[37] artículo 7 RGPD: "Condiciones para el consentimiento:
1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

el interesado prestó su consentimiento, recae en el Responsable. En cuanto a la forma en que puede prestarse, el RGPD apuesta por la libertad de forma, estableciendo simplemente que si se recoge por escrito, mediante un documento en el que se traten además otros asuntos, la solicitud de consentimiento deberá distinguirse claramente de los demás asuntos, presentarse de forma inteligible y de fácil acceso y utilizar un lenguaje claro y sencillo.

Siguiendo con requisitos en cuanto a su forma, si acudimos al Considerando 32[38], también se especifica que ha de ser un *acto afirmativo*, por lo que no cabe ninguna duda de que el consentimiento tácito no es válido en materia de protección de datos pues como se

---

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

[38] Considerando 32: "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

afirma en el propio Considerando "el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento".

El consentimiento ha de ser *claro,* que refleje una manifestación de voluntad libre, específica, informada, e inequívoca de aceptar el tratamiento de datos de carácter personal que le conciernen. Como ejemplos cita el Considerando una declaración por escrito, incluidos los medios electrónicos, o una declaración verbal. Respecto a una declaración verbal, ésta entendemos que debería grabarse o utilizar cualquier medio que pueda probar que obtuvo el consentimiento, pues como hemos visto la carga de la prueba recae sobre el Responsable.

Como comentábamos en el capítulo II, el Principio del consentimiento tiene una importancia capital en la normativa de protección de datos, ya que permite al interesado ejercer el control sobre sus datos (autodeterminación informativa), pero para poder hablar de consentimiento, es requisito *sine qua non* que se haya cumplido correctamente con los principios de información y finalidad, pues en caso contrario, éste podría considerarse nulo, o como mínimo, viciado.

En este sentido, el RGPD[39] establece (aunque en el contexto de recogida del consentimiento mediante una declaración escrita) que "no será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento".

Hasta aquí, ninguna novedad. Se continúa con el modelo de recogida de datos y obtención del consentimiento en el mismo momento, como diría ABRAMS, cuando la recogida y el origen o generación del dato coinciden.

Pero como hemos visto anteriormente, ¿qué ocurre con los datos inferidos o los generados a partir de otros datos? ¿cómo obtenemos el consentimiento del interesado en el ámbito del *big data*? Y lo que es más grave en nuestra opinión, ¿cómo consentir a aquellos tratamientos para un "fin *distinto* de aquel para el que se recogieron los datos personales"?

El ICO adopta una postura "tradicional" ya que manifiesta[40] que "Si una organización se basa en el consentimiento como la condición para

---

[39] Artículo 7.2 *i.f.*

[40] Informe de ICO, *op. cit.,* p. 18, epígrafe 56.

el tratamiento de sus datos personales, el consentimiento debe ser libre, específico e informado. Esto significa que las personas deben ser capaces de entender lo que la organización va a hacer con sus datos y tiene que haber una clara indicación de que dan su consentimiento para ello. Si una organización ha recogido datos personales para un propósito y luego decide empezar a analizarla para fines completamente diferentes (o ponerla a disposición para que otros lo hagan), entonces tiene que hacer que sus usuarios sean conscientes de ello. Esto es particularmente importante si la organización tiene la intención de utilizar los datos para un propósito que no es evidente para el individuo, ya que no está, obviamente, conectado con el uso de un servicio. Por ejemplo, si una compañía de medios sociales vende los datos personales de sus usuarios a otra compañía para otros fines".

Recordemos que el artículo 1 b) del RGPD establece que los datos personales serán "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera *incompatible* con dichos fines". Precisa y paradójicamente, quien se encargará de determinar si el tratamiento con otro fin es *compatible* con el fin para el cual se recogieron inicialmente los datos será el propio Responsable, que "deberá tener en cuenta, entre otras cosas":

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Este artículo 6.4 (tratamiento para un fin distinto pero compatible) supone una quiebra frontal del Principio del consentimiento[41], recordemos que el propio GT29 abogaba por su supresión, y de cualquier seguridad jurídica, pues no se establece ni siquiera ninguna obligación para el Responsable de documentar dicho análisis o cualquier tipo de deber de información *a posteriori.* Esto supone por tanto, una rebaja de los estándares establecidos por la Directiva 95/46 que supone un grave detrimento de los derechos de los interesados.

Resulta paradójico y sorprendente, que el RGPD exija que el consentimiento provenga de una acción del usuario eliminando así la posibilidad del consentimiento tácito, que sea claro y en lenguaje comprensible etc y luego se dé carta de naturaleza al tratamiento para fines ulteriores distintos, eso sí, siempre que sean *compatibles*[42] (si se me permite la ironía).

Como hemos visto anteriormente, el consentimiento no da todas las respuestas que los tratamientos de datos actuales y futuros demandan, pero en nuestra opinión, tampoco las puede dar, por varios motivos, 1) el Responsable puede no conocer en el momento de solicitar el consentimiento, todas las finalidades para las que utilizará los datos 2) aun suponiendo que lo supiera, el "interesado medio" no sería capaz de comprender los términos o las consecuencias del consentimiento que en su caso esté prestando. Además, si pensamos en la ampliación del contenido del derecho de información operada por el RGPD, lo más probable es que el "interesado medio" consienta sin ni siquiera leer. Una suerte de sobreinformación que conduce precisamente al resultado que se pretende evitar, que el interesado acepte sin leer y por tanto, sin comprender realmente a qué está otorgando su consentimiento.

---

[41] Ver apartado 1.2.2.4.3. del Capítulo II del presente trabajo.

[42] En cuanto a los vocablos "incompatible" y "diferente" nos remitimos a lo dicho en el apdo 2.2.4.1. del capítulo I y en especial a la SAN 845/2004, de 11 de febrero de 2004, Rec Núm 119/2002, FD 4º.

No obstante lo anterior, como novedad el RGPD[43] introduce la posibilidad de informar en combinación con iconos normalizados, lo cual, y a la espera de su implementación, vislumbra ser una medida positiva.

Respecto al hecho de que el usuario acepte sin leer, puede deberse tanto a que no comprenda lo expresado en el aviso de privacidad, como a que no le interese el uso posterior que se realice de sus datos. Esta segunda postura es mantenida por aquellos que piensan que los usuarios cada vez comparten más información personal en redes sociales. En cualquier caso, no puede afirmarse simplemente que el hecho de que los usuarios acepten sin leer, equivale a que no les interesa lo que se pueda hacer con sus datos, lo cual por otro lado, en nada afecta a la obligación del Responsable de informar, de manera que el usuario pueda entender, qué tratamientos y acciones se van a realizar con sus datos.

Es cierto que el deber de información y obtención del consentimiento en el ámbito de los datos masivos, supone ciertos retos para el Responsable, ya que como comentábamos, puede no conocer todas las finalidades para la que se utilizarán los datos (e.g. usos posteriores compatibles), así como las fuentes de donde los obtendrá. Además, dado que no sólo se tratarán los datos facilitados directamente por el usuario (e.g. datos observados, inferidos), es de vital importancia que el Responsable cumpla fielmente con este deber de información y obtención del consentimiento.

En conclusión, siguiendo a LAZARO y LE Métayer[44], entendemos que el control sobre la información no podrá ser efectivo mientras no se

---

[43] Artículo 12 RGPD: "7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados".

[44] LAZARO, C., y LE MÉTAYER, D., *op. cit.*, pp. 23 y 24.

conciba e implemente como un compromiso compartido entre los diferentes actores implicados.

La misma idea subyace en la afirmación de MAYER-SCHÖNBERGER y CUKIER[45] cuando afirman "tenemos que proteger la privacidad desplazando la responsabilidad de los individuos hacia los usuarios de datos: es decir que rindan cuentas por su uso".

Y el Principio de responsabilidad en el cumplimiento (*Accountability*)[46] establecido por el RGPD es un paso realmente importante hacia ello, cuya efectividad dependerá de cómo se

[45] MAYER-SCHÖNBERGER, V. y CUKIER, K., *op. cit.*, p. 236.

[46] Artículo 5 RGPD: "Principios relativos al tratamiento:

1. Los datos personales serán:

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

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

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

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

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

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

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

configure su exigencia, si como una obligación de medios o de resultado.

El SEPD ha afirmado[47] que la rendición de cuentas en el tratamiento de datos personales implica:

1. políticas privacidad y protección de datos internas transparentes, aprobadas y avaladas por el más alto nivel de dirección de la organización ;
2. Informar y formar a todas las personas en la organización sobre la manera de poner en práctica dichas políticas ;
3. responsabilidad al más alto nivel para el seguimiento de esta implementación, demostrando a las partes interesadas externas y a las autoridades la calidad de la implementación;
4. Procedimientos para corregir deficiencias en el cumplimiento y brechas de seguridad.

El propio GT29 en 2010[48] recalcó que los principios y obligaciones de protección de datos en la UE no se reflejan suficientemente en medidas internas y prácticas concretas, razón por la que el marco normativo de la UE precisaba de medidas complementarias, de modo que plantea una propuesta concreta de introducción del principio de responsabilidad en la Directiva 95/46, "que reclamaría de los responsables del tratamiento de datos la aplicación de medidas apropiadas y eficaces que garantizaran la observancia de los principios y obligaciones que dispone la Directiva y la demostraran cuando se lo solicitaran las autoridades de control". Recuerda que el Principio de Responsabilidad no es un concepto nuevo, ya que las directrices sobre privacidad adoptadas en 1980 por la OCDE ya lo reconocían :"Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios [materiales] expuestos". Asimismo resalta que recientes instrumentos como las Normas

---

[47] *EDPS launches Accountability Initiative*, disponible en https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-06-07_Accountability_factsheet_EN.pdf

[48] Dictamen 3/2010 sobre el Principio de Responsabilidad disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf

Internacionales de Madrid, desarrolladas por la Conferencia Internacional de Comisarios de Protección de Datos y Privacidad y la ISO 29100, que establece un marco de privacidad, han incorporado este Principio.

A pesar de que el Dictamen propugna la modificación de la Directiva 95/46 para la introducción del Principio de Responsabilidad, lo cierto es que lo dicho podemos aplicarlo al Principio de Responsabilidad introducido por el RGPD.

El GT considera que el Principio de Responsabilidad debe centrarse en dos elementos:

i) la necesidad de que el responsable del tratamiento adopte **medidas adecuadas** y **eficaces** para aplicar los principios de protección de datos;

Estas medidas adecuadas, no es necesario que se especifiquen *a priori*, sino que pueden ser concretadas posteriormente, bien por el GT29, bien por la Comisión. De hecho, el GT29 afirma que el Principio de Responsabilidad general, evita voluntariamente detallar el tipo de medidas que deban aplicarse. No obstante, ofrecen una lista de medidas[49] que podrían adoptarse.

---

[49] Dictamen 3/2010, p 12: ejemplos de medidas comunes de responsabilidad:

- establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.);
- establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p.ej., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas;
- cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento de datos;
- nombramiento de un funcionario de protección de datos y otras personas responsables de la protección de datos;
- oferta adecuada de protección de datos y formación a los miembros del personal; esto debe incluir a los procesadores (o responsables del proceso) de datos personales (como los directores de recursos humanos) pero también a los administradores de tecnologías de la información,

En relación a su eficacia, el GT29 menciona diversos modos para la evaluación de las medidas adoptadas: seguimiento, auditorías internas y externas, etc.

ii) la necesidad de demostrar, si así quiere, se han adoptado medidas adecuadas y eficaces; el responsable del tratamiento de datos deberá **aportar pruebas** de (i).

En cuanto a si se trata de una obligación de medios o de resultado, como comentábamos anteriormente, el GT29 afirma que "la observancia del principio de responsabilidad no implica necesariamente que el responsable del tratamiento de datos cumpla los principios materiales establecidos en la Directiva, es decir, no ofrece presunción jurídica de cumplimiento ni sustituye a ninguno de dichos principios. Un responsable del tratamiento de datos puede haber aplicado y verificado las medidas que ha puesto en practica y, pese a ello, hallarse en una situación de irregularidad". Así, el hecho de adoptar medidas para cumplir con los Principios "no debe en ningún caso eximir a los Responsables del tratamiento de actuaciones ejecutorias por parte de las Autoridades de protección de datos". Ello parece apuntar a que estamos ante una obligación de resultado, aunque como menciona el GT29, "al evaluar las sanciones relacionadas con

---

conceptores y directores de unidades comerciales; deben asignarse recursos suficientes para la gestión de la privacidad, etc...;

- establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas;
- establecimiento de un mecanismo interno de tratamiento de quejas;
- establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad;
- realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas;
- aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean solo nominales sino que se apliquen y funcionen en la práctica (auditorias internas o externas, etc.).

las infracciones en la protección de datos, las autoridades de protección de datos podrían sopesar la aplicación (o inaplicación) de las medidas y su verificación".

Veremos cómo se articula el Principio de responsabilidad en el cumplimiento en la práctica, pues al estar incardinado entre los "Principios relativos al tratamiento", el Responsable deberá ser capaz de demostrar por ejemplo, que disponía del consentimiento del interesado para finalidades de *big data*, o demostrar las técnicas de anonimización utilizadas así como las revisiones de las mismas. Esto va a suponer una gran "carga" para los Responsables sobre quienes recae la carga (valga la redundancia) de la prueba del cumplimiento de todos los aspectos que integran los Principios relativos al tratamiento de datos, aunque el GT29 considera que dado que los Responsables están obligados a cumplir los Principios y obligaciones de la Directiva, para ello "es intrínsecamente necesario establecer, y posiblemente verificar, procedimientos de protección de datos", por lo que el Principio de Responsabilidad "no representa una gran novedad y, en lo esencial, no impone requisitos que no estuvieran ya implícitos en la legislación vigente".

En cualquier caso, coincidimos con el SEPD cuando afirma que, "la rendición de cuentas va más allá de cumplimiento de las normas - implica un cambio de cultura".

Retomando la cuestión de la vigencia del Principio del Consentimiento, consideramos que para que éste sea efectivo, la forma en la que la información se proporciona al interesado, debería evolucionar en el sentido de ofrecer la información realmente trascendente para el interesado; una buena opción sería la propuesta por SEMPERE[50] de utilizar un formato tipo esquema, ya que facilitaría la comprensión así como la rápida localización de la información que el interesado considere relevante, evitando así largas y confusas cláusulas que produzcan lo que hemos denominado "rechazo por sobreinformación". El ICO afirma[51] que la información sobre privacidad no necesariamente tiene que facilitarse de una determinada

[50] SEMPERE, F. J., *op. cit.*, p. 205.
[51] Informe ICO, *op. cit.*, p. 35.

manera, sino que puede utilizarse una combinación de varios métodos. Considera que en este aspecto será necesaria la innovación para dar cobertura a los diferentes tipos de recolección de datos. Todo un reto para los responsables, tanto en la teoría como en la práctica, pues podemos plantearnos si realmente será posible aplicar la voluntad del interesado con respecto a los tratamientos de datos masivos, es decir, si el Responsable podrá realmente (técnicamente) respetar la voluntad del interesado en cada momento.

El Principio del consentimiento únicamente puede evolucionar en la manera en que éste se recoge y presta. En el caso de los datos masivos, la evolución de este Principio radica precisamente en asumir que no sirve para cubrir estos nuevos supuestos que la datificación y los datos masivos nos plantean o los que puedan existir en un futuro.

Como pone de manifiesto ABRAMS[52], no todos los datos personales son obtenidos directamente del interesado, por lo que el tradicional esquema de obtención del consentimiento en el momento de su recogida, no puede funcionar en todos los casos.

Solamente siendo conscientes de que el consentimiento no cubre ni puede cubrir todos los supuestos, se plantea la necesidad de introducir nuevos instrumentos que respeten los derechos de los interesados, pasando por la evolución del concepto clásico de "dato personal".

Consideramos que el RGPD no ha asumido que el Principio del Consentimiento, al igual que otros conceptos, deben evolucionar introduciendo los mencionados instrumentos para cubrir los nuevos retos que nos plantea la evolución tecnológica, pero es que además, el Principio del consentimiento no se ha respetado en absoluto en relación a tratamientos posteriores para fines distintos, dando carta de naturaleza a tratamientos que actualmente están prohibidos por la Directiva 95/46, y por tanto, rebajando los estándares de protección.

---

[52] ABRAMS, M., *Data origin and the proposed regulation*, en RALLO LOMBARTE, A., y GARCÍA MAHAMUT, R., y otros, *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015, pp. 85-101.

3.4 Derecho olvido y anonimización

En el capítulo anterior vimos los problemas que la anonimización plantea en el entorno *big data*. Veamos qué puede aportar el "derecho al olvido", denominado finalmente "derecho a la supresión" por el RGPD, aunque se incluyan referencias al "derecho al olvido" en el propio RGPD[53].

En primer lugar, consideramos que no podemos hacer una equiparación entre el (incorrectamente) denominado derecho al olvido y el finalmente denominado derecho a la supresión, pues aunque en realidad se trata de derechos distintos, en el RGPD entendemos no se ha positivado un "nuevo" derecho al olvido. La utilización del término "supresión" resultaría cuando menos inadecuada en relación al derecho al olvido, pues no siempre conllevaría la supresión de la información (e.g. la no indexación no significa la supresión de los datos de la fuente original). En este sentido, muy acertadamente, PAZOS CASTRO[54] aboga por utilizar una "denominación diferente y especifica para el derecho que consiste en exigir la eliminación de uno de los resultados de la lista ofrecida por el motor de búsqueda, para el caso de que se lleve a cabo una búsqueda a partir del nombre de una persona, cuando esta persona desea que uno de los resultados no sea mostrado (porque le sea perjudicial o no), y siempre que no haya un interés público en que ese resultado se mantenga fácilmente accesible a los internautas". El autor propone el término "derecho a la oscuridad digital".

---

[53] El Considerando 65 establece "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento (…)"; Considerando 66 "A fin de reforzar el «derecho al olvido» en el entorno en línea (…)".

[54] PAZOS CASTRO, R., *El mal llamado derecho al olvido en la era de internet*, *BMJ* n. 2183, noviembre 2015, ISSN: 1989-4767 - www.mjusticia.es/bmj, p. 54.

En nuestra opinión, realmente no estamos ante la configuración de un nuevo derecho, sino ante la plasmación de la evolución de los derechos de cancelación y oposición, por lo que podemos afirmar que el "derecho al olvido" no existe. Así, RALLO LOMBARTE[55] afirmaba en 2014 que "hoy por hoy, el derecho al olvido no existe. Ninguna norma reconoce y regula tal hipotético y específico derecho. Es más, no puede existir porque ni siquiera nos hallamos ante un concepto jurídico pacíficamente delimitado".

Recordemos que la propia Directiva 95/46 ya hablaba de "la *supresión*[56] o el *bloqueo* de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos" (artículo 12 b) Directiva 95/46). Coincidimos por tanto con PAZOS CASTRO[57] cuando afirma que "una lectura del precepto permite constatar que el derecho al olvido queda englobado en la supresión o cancelación de datos, la cual se relaciona a su vez con otros derechos como el de oposición al tratamiento de datos personales y, en general, con cualquier incumplimiento de las normas sobre protección de datos".

No obstante lo anterior, siguiendo a PAZOS CASTRO [58], "en realidad, la vinculación entre los derechos de oposición y cancelación con el derecho al olvido es sencilla de establecer si se toman como premisas que, a los efectos de la Directiva sobre protección de datos, los motores de búsqueda llevan a cabo un tratamiento de datos personales y que el gestor del motor es un responsable del tratamiento", pero "la vinculación deja de ser tan clara, pudiendo apreciarse de forma más evidente el carácter autónomo del derecho al olvido, si se cuestionan estos dos aspectos".

---

[55] RALLO LOMBARTE, A., "El derecho al olvido en internet Google versus España", *Cuadernos y debates*, n. 233, Centro de Estudios Políticos y Constitucionales, Madrid, 2014, p. 23.

[56] La legislación española en materia de protección de datos optó por el término "cancelación" para referirse al derecho a la supresión.

[57] PAZOS CASTRO, R., *op. cit.*, pp. 52 y 53.

[58] *Ibíd.*, p. 44.

Sin ahondar ahora más en el carácter autónomo del "derecho al olvido", en cuanto a las razones de por qué no consideramos este artículo como la configuración de un nuevo derecho, quedarán puestas de manifiesto cuando analicemos a continuación el contenido del artículo 17.

Ciñéndonos al tenor literal del RGPD[59], el derecho a la supresión comportará que el Responsable suprima "sin dilación indebida" los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

El RLOPD (artículo 31.2) establece que "El ejercicio del derecho de cancelación dará lugar a que se *supriman* los datos que resulten ser *inadecuados* o *excesivos* sin perjuicio del deber de bloqueo conforme a este reglamento". La Directiva 95/46 habla del derecho a obtener la supresión o bloqueo de los datos a causa del carácter *incompleto o inexacto* de los datos" (artículo 12 b).

Vemos por tanto cómo el RGPD ya no hace referencia al carácter inadecuado, incompleto o inexacto del dato, sino al Principio de Finalidad, lo cual es en nuestra opinión muy acertado, pues como indicábamos en la primera parte de este trabajo en relación a los Principios, es la finalidad la que determina si los datos deben ser o no cancelados, pues todo tratamiento tiene una duración determinada, sin que sea necesario exigir una determinada cualidad (incompleto, inexacto, excesivo o inadecuado) al dato.

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

¿Acaso la retirada del consentimiento no debería comportar la cancelación o supresión de los datos de oficio, una vez eliminado el fundamento jurídico para su tratamiento?

---

[59] Artículo 17 RGPD.

Lógicamente, como establece el artículo 7.3 RGPD, "la retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada". El artículo 5.1 e) establece la "limitación del plazo de conservación" ya que los datos personales serán "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales", y por tanto, *a sensu contrario* debemos entender que dado que no hay ninguna finalidad que cumplir pues se ha retirado el consentimiento, los datos no deben conservarse y por tanto, deben suprimirse de oficio por el Responsable.

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

Si el interesado tiene derecho a obtener la supresión de sus datos cuando ha ejercitado el derecho de oposición únicamente en los dos supuestos establecidos en los párrafos primero y segundo del artículo 21 (tratamientos basados en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones, y tratamientos con fines de mercadotecnia directa), quiere decir que el interesado ha de solicitar dicha supresión y que ésta no se realiza por defecto tras el ejercicio del derecho de oposición; de hecho, el RGPD[60] cuando se refiere al derecho de oposición habla de que el Responsable "dejará de tratar"[61] lo cual no conlleva necesariamente una supresión de los datos.

---

[60] Artículo 21.1 RGPD "El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".

[61] Podría argumentarse que la mera conservación del dato es una operación de tratamiento, pero mediante el derecho de oposición el interesado se está oponiendo a

¿Quiere decir *a sensu contrario* que el ejercicio del derecho de oposición en el resto de supuestos del artículo 21 no permite solicitar la supresión de dichos datos? ¿es necesario ejercitar el derecho de oposición como requisito previo para solicitar la supresión? entendemos que no, pues la retirada del consentimiento para el tratamiento es uno de los supuestos en que se puede solicitar la supresión de dichos datos. En cualquier caso, no entendemos por qué se alude expresamente a los dos primeros párrafos del artículo 21 RGPD y no al resto, salvo que sea con la intención de aclarar o reforzar la existencia del derecho de supresión en esos casos.

d) los datos personales hayan sido tratados ilícitamente;

Si los datos han sido tratados ilícitamente, o bien así se ha declarado previamente por el organismo correspondiente tras un procedimiento sancionador, o bien dicha ilicitud se descubre por el interesado y motiva el ejercicio del derecho de supresión. Entendemos que en el supuesto de declaración previa de un tratamiento ilícito, la supresión debería darse sin necesidad de solicitud por parte del interesado, que no tiene por qué conocer de la existencia del tratamiento, por lo que entendemos que este supuesto se refiere al "descubrimiento" de un tratamiento (ilícito) que ha motivado la solicitud de supresión.

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

Nuevo supuesto en el que existe una ley que obliga a la supresión de los datos, que ha sido incumplida por el Responsable. La supresión debería haberse producido de oficio por tanto.

---

una determinada finalidad y la conservación del dato es necesaria para el cumplimiento de otras finalidades a las que el interesado no se opone. La Directiva 95/46 (artículo 14) habla del derecho del interesado a "oponerse … a que los datos que le conciernan sean objeto de tratamiento (…)".

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1[62]

Vemos pues cómo estamos ante supuestos en los que el Responsable ya no tiene un fundamento jurídico para continuar con el tratamiento de datos, bien porque no ha cumplido con sus deberes de supresión como Responsable y estamos ante un tratamiento ilícito o bien porque el interesado retira el consentimiento, y por tanto, procede la solicitud del interesado de supresión de los datos. Nada nuevo. Simplemente se especifican los supuestos en los que procede solicitar la supresión de los datos. Lo "novedoso" del llamado "derecho al olvido" (para diferenciarlo del derecho a la supresión) es que supone dar respuesta a una demanda social a través de los instrumentos existentes en la normativa de protección de datos. Es la única razón por la que sostenemos que no se trata de un derecho diferenciado, pero ello no significa que no deba existir o que no exista en un futuro. Es por ello que en la realidad no puede afirmarse que el RGPD recoja un *nuevo* derecho.

Siguiendo con el análisis del artículo 17 del RGPD, como elemento de vital importancia para garantizar la efectividad del derecho a la supresión, el párrafo segundo establece que "*Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica*

[62] Artículo 8.1 RGPD "Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años".

de los mismos"[63]**.** Es decir, recae sobre el Responsable el deber de "adoptar medidas razonables" para informar a todos aquellos otros Responsables que estén tratando los datos, de la solicitud de supresión del interesado.
GARRIGA DOMINGUEZ[64] afirma que "el derecho al olvido va más allá de la mera exigencia de la supresión o borrado de los datos personales estableciendo la obligación accesoria del responsable del tratamiento que deba hacer efectivo el derecho de supresión, de informar a otros responsables (…)". No obstante, la Directiva 95/46 ya recogía en su artículo 12 c) la obligación de notificar "a los terceros a quienes se hayan comunicado los datos de toda rectificación, *supresión* o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado".

Sobre esta obligación accesoria, nada dice el RGPD salvo que deberá adoptar "medidas razonables", por lo que podríamos plantearnos cuándo se entenderá cumplida esta obligación o cuándo estaremos ante un incumplimiento del Responsable. En cualquier caso, entendemos que el Responsable, con vistas a poder demostrar la "razonabilidad" de las medidas adoptadas, deberá conservar prueba de las medidas adoptadas.
El problema práctico evidente es que el "Responsable que haya hecho públicos los datos" desconoce concretamente quiénes son "los Responsables que están tratando los datos".

---

[63] En el mismo sentido se pronuncia el Considerando 66 "A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales".
[64] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Dykinson, Madrid, 2016, p. 241.

Coincidimos plenamente con GARRIGA DOMÍNGUEZ cuando afirma[65] que "Esta obligación parece insuficiente si verdaderamente se quiere garantizar el olvido digital y si bien, esta obligación es imprescindible para garantizar la efectividad del derecho al olvido, hemos de ser conscientes de las dificultades reales de que cualquier información desaparezca definitivamente de la red", ya que aunque insuficiente y con las dificultades inherentes reales, no deja de ser una obligación necesaria en aras a garantizar el derecho a la supresión.

Este derecho de supresión no es ilimitado[66], y de hecho el propio artículo 17, párrafo tercero, introduce una serie de supuestos que prevalecerán frente a la solicitud de supresión del interesado:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Otro problema que plantea el derecho a la supresión, es que ante una petición, el Responsable tenderá a suprimir aunque pudieran darse alguna de las condiciones que acabamos de ver (i.d. libertad de expresión) únicamente por el "miedo" a una sanción o publicidad

---

[65] Ibíd.

[66] Vid. SEMPERE SAMANIEGO, F. J., *op. cit.*, pp. 219 a 221, que muy acertadamente pone de relieve el "derecho al olvido sobre actos beneficiosos del titular de los datos" no contemplado expresamente por el RGPD.

negativa. Esto se debe a que es el propio Responsable el que ha de realizar la ponderación, y aunque posteriormente puedan intervenir las Autoridades nacionales de protección de datos o Tribunales para corregir o realizar el examen de los intereses en juego realizado por el Responsable, muchos casos no llegarán a plantearse en dichas instancias pues el Responsable ya habrá suprimido. Debemos tener en cuenta que la parte que pretenda hacer valer su derecho a la libertad de expresión, puede no llegar a enterarse de que se ha eliminado la información o el acceso a la misma. Quizá sería recomendable establecer una suerte de procedimiento "contradictorio", no dejando toda la responsabilidad y riesgo en el Responsable, para aquellos casos en que el Responsable tenga dudas y así todas las partes involucradas puedan hacer valer sus derechos, garantizando una solución lo más justa posible.

Si a las dificultades que el derecho a la supresión *a priori* plantea, sumamos las derivadas de un entorno *big data,* la problemática está servida. KOOPS[67] realizó ya en 2011 un interesantísimo análisis sobre esta problemática.

En el mundo de *big data* en el que estamos inmersos, donde siguiendo a KOOPS [68], las sombras digitales forman al menos una parte tan importante como las huellas digitales, este autor distingue tres maneras o conceptualizaciones en las que puede aparecer este derecho:

1. derecho a que los datos se borren "en su debido momento" (*due time*)
2. una reivindicación de la Sociedad a hacer borrón y cuenta nueva ("*clean slate*")
3. un interés individual en expresarse libremente en el aquí y el ahora.

Respecto a esta última conceptualización, KOOPS admite que, a pesar de su importancia como lección, poco tiene que ver como un derecho

---

[67] KOOPS, B. J., "Forgetting footprints, shunning shadows. a critical analysis of the "right to be forgotten", *Big Data Practice*, vol. 8, Issue 3, December 2011, CC BY-NC-ND.

[68] *Ibíd*., p. 236.

legal como tal, como un derecho a ser olvidado como entidad separada.

Por tanto, las dos primeras visiones son las dos perspectivas del derecho al olvido. El derecho a que los datos se borren a su debido tiempo, resulta una manifestación del derecho a la autodeterminación informativa, dado que es el propio individuo quien decide y solicita al Responsable qué datos quiere que se supriman. No obstante, KOOPS [69] afirma que un análisis más profundo revela dificultades prácticas derivadas de las propias limitaciones del derecho a la protección de datos (la excepción doméstica, en el caso de usuarios que suben datos relativos a otros usuarios en redes sociales, y la limitación a las solicitudes de borrado de datos inexactos o tratados ilegalmente) y también a tensiones intrínsecas en el derecho a suprimir. El autor se refiere en este punto a si el interés legítimo del interesado en borrar sus datos debe prevalecer sobre el interés legítimo de otros Responsables que tratan los datos. Según KOOPS la respuesta afirmativa estaría en consonancia con el enfoque centrado en la autodeterminación informativa, pero se apartaría considerablemente de las actuales disposiciones sobre protección de datos, que tienen un enfoque más equilibrado de posibles conflictos de intereses entre los interesados y los responsables del tratamiento de datos.

En nuestra opinión no puede ser de otra manera. Si estamos hablando de un derecho fundamental de las personas, debe existir la posibilidad de solicitar la supresión de los datos, siempre que se den los presupuestos legales para ello. Es más, tal y como comentamos anteriormente, consideramos que la plasmación legal del derecho a la supresión en el RGPD, parece más bien una corrección ante el incumplimiento del Responsable del Principio de limitación de la finalidad[70], Minimización de datos[71] y Limitación del plazo de

---

[69] *Ibíd*., p. 254.

[70] Artículo 5.1 b) RGPD "los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines".

[71] Artículo 5.1 c) "los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

conservación[72], que una solicitud del interesado, ya que deben darse algunas de las seis circunstancias mencionadas en el artículo 17, siendo sólo una de ellas la retirada del consentimiento del interesado.
Respecto a la segunda perspectiva de KOOPS del derecho al olvido, (la reivindicación de la Sociedad a hacer borrón y cuenta nueva o "pizarra limpia"), el autor afirma[73] que esta visión no se centra en medidas globales dirigidas a que los individuos puedan controlar genéricamente la información existente, sino más bien a medidas específicas para controlar cómo otras partes pueden usar la información cuando toman decisiones concretas que afectan a las personas. Puede efectuarse en parte a través de los derechos legales existentes, pero debido a la evolución de Big Data, tal vez tenga que extenderse para cubrir más áreas en las que las personas son más vulnerables a tener que lidiar con información perjudicial sobre su pasado. Por tanto, esta visión más que un derecho del interesado KOOPS la configura como una obligación del Responsable.

KOOPS [74] realiza la siguiente comparativa entre ambas perspectivas del derecho al olvido:

	right to delete in due time	**right to a clean slate**
object	deletion of data	blocking use of data
type	data subject right	data processor obligation
focus	data collection and storage	data use in decision-making
scope	generic	specific
legal area	data-protection law	sector-specific law
enforcement	enforcement-by-design	legal measures for oversight

[72] Artículo 5.1 e) "los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales".
[73] *Ibíd*., p. 255.
[74] *Ibíd*., p. 256.

KOOPS afirma que elegir una de las dos visiones es una cuestión de perspectiva. Afirma que se considera escéptico respecto a la primera visión global, basada en el control del usuario, y más proclive respecto a la segunda visión, más detallada y limpia.

En nuestra opinión no se trata de elegir una u otra visión, sino, siendo coherente con los principios en materia de protección de datos, no podemos sino albergar ambas, pero no como manifestación del derecho a la supresión del interesado, sino como resultado del cumplimiento de las obligaciones del Responsable y del derecho del interesado a solicitar la supresión de sus datos.

Es decir, si existe la obligación de tratar los datos únicamente por el tiempo necesario para la finalidad para la que fueron recabados y existen unos plazos legales pasados los cuales la información deberá ser destruida, no estamos ante un *derecho a* la supresión del interesado, sino ante la *exigencia del cumplimiento del deber del Responsable.*

En un entorno de *big data*, resulta sumamente interesante la segunda visión de KOOPS, como medida preventiva, de establecer obligaciones para el Responsable tendentes a evitar que otras partes pueden usar la información para tomar decisiones concretas que afecten a las personas sin su pleno conocimiento.

Por todo lo expuesto en el presente apartado, consideramos que el RGPD no introduce un nuevo derecho ("al olvido") sino que concreta los supuestos en que se puede solicitar la supresión. Introducir un verdadero derecho "al olvido" supondría desvincularlo de los rígidos esquemas de la protección de datos, pues no podemos pretender que un derecho a la supresión de datos de carácter personal sirva para todos aquellos casos en que se desee que una determinada información desaparezca de la red, y porque no siempre estaremos ante un Responsable de tratamiento. Como afirma PAZOS CASTRO[75],

[75] PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible?", *Revista INDRET* 1/2001, Barcelona, enero 2015, disponible en http://www.indret.com/pdf/1118_es.pdf p. 40.

"este derecho (en referencia al derecho a la supresión del artículo 17 RGPD) no constituye un genuino derecho al olvido, puesto que solo se otorga al interesado, de acuerdo con el propio artículo 17.1 de la Propuesta de Reglamento, cuando se produce alguna de las circunstancias (establecidas en dicho artículo)".

Además, otro de los problemas con los que se encuentra el derecho a la supresión del RGPD, es la **territorialidad**, es decir, cuando se solicita la supresión de un enlace frente a un buscador, no puede ejercitarse frente a cualquier dominio, sino únicamente frente a aquellos dominios europeos. No obstante lo anterior, el GT29 en sus Directrices[76] para la implementación de la Sentencia TJUE C-131/12 recomienda que se incluyan todos los dominios relevantes. Así, el GT29 afirma (la traducción y la negrita es nuestra) que "las decisiones de exclusión deben aplicarse de manera que garantice la protección efectiva y completa de estos derechos y que la legislación de la UE no pueda eludirse fácilmente. En ese sentido, **la limitación de la exclusión de la lista a los dominios de la UE**, alegando que los usuarios tienden a acceder a los motores de búsqueda a través de sus dominios nacionales, **no puede considerarse un medio suficiente para garantizar satisfactoriamente los derechos de los interesados** según la sentencia. En la práctica, esto significa que, en cualquier caso, **la eliminación de la lista también debe ser efectiva en todos los dominios relevantes, incluyendo .com**".

Está claro que el Derecho Comunitario, en principio, no puede extralimitarse[77] en su aplicación, pero también lo es que la eficacia de

---

[76] Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, de 26 de noviembre de 2014, disponibles en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf pp. 3 y 9

[77] para ahondar en esta cuestión, Vid. VAN ALSENOY, B., & KOEKKOEK, M., "The extra-territorial reach of the EU's "Right to be forgotten", Working Paper n. 152, marzo 2015, disponible en https://ghum.kuleuven.be/ggs/publications/working_papers/new_series/wp151-160/wp152-alsenoy-koekkoek.pdf

un derecho al olvido en internet no puede tener límites territoriales, los cuales desconoce.

Cabe resaltar que Google ya está implementando la eliminación de resultados a nivel global[78].

Realmente estamos ante una nueva necesidad, originada por el no olvido de internet, que probablemente necesite de una respuesta en forma de derecho ("al olvido"). Como magistralmente afirma MAYER SCHÖNBERGER, en el ámbito digital se invierten las cualidades humanas relativas a recordar y olvidar, es decir, los seres humanos olvidamos fácilmente y nos cuesta recordar, mientras que en el ámbito digital se recuerda por defecto y la excepción es el borrado, el olvido. ¿Quién es la misma persona hoy que hace veinte años? Obviamente somos la misma persona pero con un aprendizaje fruto de las experiencias vividas, entre las cuales se incluyen errores y aciertos. Hay experiencias difíciles de olvidar y otras que a duras penas conseguimos recordar. También con el tiempo cambia nuestra percepción sobre los hechos vividos, porque sencillamente evolucionamos, crecemos (en el mejor de los casos, claro). Si cada día de nuestra vida tuviéramos que recordar las experiencias vividas quizá no las habríamos "olvidado" y no seríamos las mismas personas hoy. Esta es la idea que subyace en el argumento de MAYER SCHÖNBERGER y por eso aboga por el establecimiento de plazos de borrado ("*expiration dates*[79]"). Así, con independencia de las más o menos complejas formas de borrado digital automático que se puedan adoptar, MAYER SCHÖNBERGER afirma que (la traducción es nuestra) "todas estas variaciones, sin embargo, comparten un elemento principal. Están diseñadas para confrontarnos con (y por tanto, recordarnos) la "finitud de la información", en otras palabras, que la información está inexorablemente ligada a un punto (o período) en el

---

[78] "Google reforzará la aplicación del derecho al olvido" publicado en *Expansión* http://www.expansion.com/juridico/actualidad-tendencias/2016/01/27/56a89cc4ca474139368b45e0.html. Consultado el 10 de diciembre de 2016.

[79] MAYER-SCHÖNBERGER, V., *The virtue of forgetting in the digital age*, Oxford University Press, 2009, pp.171-173.

tiempo, y que conforme el tiempo pasa, la mayoría de la información pierde su valor informacional (…)". Así, el autor habla de pasar de una realidad en la que se recuerda por defecto y de manera generalizada a un sistema de olvido controlado por los humanos (*human controlled forgetting*). MAYER SCHÖNBERGER recalca que establecer fechas de expiración no significa imponer el olvido, sino reflexionar sobre la utilidad o conveniencia de conservar determinada información.

KOOPS argumenta[80] que la idea de establecer plazos de expiración para los datos funciona con respecto a nuestra huella digital pero no respecto a lo que el autor denomina "sombra digital" o "sombras de datos" (*data shadow*), es decir, información no generada directamente por el individuo pero que existe en internet; el autor se plantea ¿cómo puede establecer un usuario una fecha de expiración sobre información relativa a él pero generada por otros sin su conocimiento o implicación? A lo que responde que (la traducción es nuestra) "para abordar el problema de la caducidad automática de las sombras de datos, es posible que tengamos que recurrir a obligaciones legales con terceros para fijar fechas de caducidad que tengan en cuenta el interés de los interesados" (y no sólo el suyo propio). KOOPS pone sobre la mesa determinadas cuestiones que deben ser tenidas muy en cuenta:

1) el derecho al olvido no puede basarse sólo en datos "obsoletos", pues el daño también puede ocurrir durante un período en el que el tratamiento es legítimo. Para evitar esto, el sistema debe garantizar que los Responsables borren los datos que ya no es necesario mantener, posiblemente reforzados por la fijación de una fecha de caducidad fijada por los usuarios.
2) El problema de las sombras de datos (*data shadow*) y la excepción doméstica, no quedaría resuelto aun cuando se implantasen fechas de expiración.

---

[80] Cfr KOOPS, B. J., "Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten", *Big Data Practice,* vol. 8, Issue 3, December 2011, CC BY-NC-ND, p. 243.

3) En la era del *big data*, no es fácil establecer cuándo los datos son obsoletos, si tenemos en cuenta los usos secundarios o sobrevenidos.

La idea de MAYER SCHÖNBERGER de establecer *expiration dates* estaría relacionada, aunque indirectamente, con el *opt-out* del que hablábamos anteriormente. El usuario decide que determinada información no sea tenida en cuenta, se cancele, y por tanto, tampoco a efectos de *big data*.

En el mismo sentido, KEELE[81] aboga por introducir un Principio denominado *Privacy by deletion* (Principio del borrado) en los esquemas normativos de protección de datos, ya que de no introducirse, ningún esquema regulatorio e protección de datos quedaría completo (en palabras del propio autor, "*the missing data deletion Principle*"). KOOPS[82] también destaca que en la Carta Europea de derechos fundamentales no se menciona expresamente el derecho a la supresión o borrado.

Todo lo cual nos lleva a plantearnos la efectividad del derecho a la supresión del RGPD en este ámbito y la necesidad de incluir un nuevo derecho, desvinculado de la protección de datos de carácter personal y

---

[81] KEELE, B. J., "Privacy by Deletion: The Need for a Global Data Deletion Principle", *Indiana Journal of Global Legal Studies*, vol. 16: Issue 1, Article 14, 2009, p. 366.

Para KEELE no parece suficiente el Principio de finalidad que limita el plazo de conservación de los datos, al menos de manera identificable. KEELE aboga establecer un nuevo Principio que obligue a la supresión directamente, ya que de otra manera los datos estarían expuestos a un posible mal uso, aunque admite una destrucción de los posibles identificadores para que una vez hecha anónima la información pueda ser utilizada posteriormente.

[82] KOOPS *op. cit.,* p. 247. Artículo 8 de la Carta Europea de Derechos Fundamentales: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

no sólo aplicable frente a un concreto buscador, que verdaderamente nos ayude a que toda la huella digital que dejamos a lo largo de nuestra vida, fruto de los diferentes momentos y fases que todos atravesamos, no nos estigmatice[83] o la vuelta a lo "analógico" será la única opción, que desde hace tiempo vaticinamos será una nueva "moda".

KOOPS da en la diana cuando afirma[84] que es palpable la discrepancia entre el análisis del problema (básicamente, el hecho de que los usuarios no tienen control sobre los datos personales en el mundo de *Big Data*) y la solución proyectada (dar a los usuarios los derechos y medios para controlar sus datos personales en el mundo de *Big Data*). El autor concluye que (la traducción es nuestra) "esta solución no funcionará simplemente ofreciendo derechos y herramientas a los usuarios, si los mecanismos subyacentes del problema no se abordan simultáneamente. Esto requiere un análisis mucho más cuidadoso de los mecanismos que subyacen a *Big Data* que los que se ofrecen actualmente".

Lo que está claro es que llegue a positivizarse este nuevo derecho al olvido o no, éste deberá ser un complemento de otras obligaciones que colaboren en su mismo objetivo: que determinada información sobre un sujeto pueda ser eliminada y no persiga al individuo durante toda su vida. Por la misma razón que comentábamos en capítulos anteriores, que el poder de control del individuo no es en sí mismo suficiente para garantizar la autodeterminación informativa o derecho fundamental a la protección de datos, sino que necesita como complemento imprescindible que el Responsable del tratamiento cumpla con determinadas obligaciones, produciéndose un desplazamiento de la responsabilidad.

---

[83] en este sentido, RALLO LOMBARTE, A., afirma "(…) hoy por hoy sigue viva la convicción social de que resulta intrínseco a la garantía de la dignidad humana olvidar en determinados ámbitos-especialmente sensible resulta el criminal (…)" en "*El derecho al olvido en internet Google versus España", Cuadernos y debates,* n. 233, Centro de Estudios Políticos y Constitucionales, Madrid, 2014, p. 24.

[84] KOOPS, *op. cit.,* p. 250.

Vemos por tanto, cómo el RGPD no ha introducido un derecho al olvido como "nuevo mecanismo" para que los individuos se enfrenten a los riesgos que una sociedad digitalizada e inmersa en el mundo de los datos masivos, entraña para el libre desarrollo de la personalidad.

3.5 Derecho de oposición a decisiones automatizadas

En el capítulo anterior se analizó el artículo 22 del RGPD y la regulación existente sobre la toma automatizada de decisiones en la Directiva 95/46 así como su transposición en la normativa española en materia de protección de datos (LOPD y RLOPD).
Recordaremos someramente los cambios introducidos por el RGPD, aunque en líneas generales, no difiere excesivamente de la regulación establecida por la Directiva 95/46.
En primer lugar, y siguiendo las recomendaciones del GT29[85], contamos por primera vez con una definición legal del concepto de "elaboración de perfiles" (*profiling*). Así el RGPD define en su artículo 4.4 como "elaboración de perfiles": *toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;*
En segundo lugar, se añade el "consentimiento explícito" como fundamento jurídico para la realización de este tipo de tratamiento de datos.
En tercer lugar, no se podrán tomar decisiones individuales automatizadas, que se basen en categorías especiales de datos, salvo consentimiento explícito del interesado o cuando el "tratamiento sea

[85] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13 mayo de 2013 disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

necesario por razones de un interés público esencial que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Como apuntamos en el capítulo anterior, que el interesado tenga derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, no significa que el Responsable deba solicitarle el consentimiento previo. Es decir, el RGPD no introduce la obligación para los Responsables de tratamiento de solicitar el consentimiento del interesado, sino únicamente de informar (artículo 13.2f) "*sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado"*.

Por tanto, únicamente en los casos del párrafo primero y cuarto, deberá informar sobre sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Teniendo en cuenta que el párrafo primero incluye la regla general de que todo interesado tendrá "derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar" y el cuarto recoge la prohibición de utilizar categorías especiales de datos salvo consentimiento del interesado y adopción de medidas adecuadas por parte del responsable, nos surgen las siguientes cuestiones: f¿qué ocurre en aquellos casos en que la decisión adoptada basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, no produzca efectos "jurídicos" en el interesado o no le afecte "significativamente de modo similar"?

Como muy bien apunta el GT29[86], el artículo 22.1 sigue centrándose únicamente en el resultado de la elaboración de perfiles, (i.e. que produzca efectos jurídicos o le afecte de manera significativa) en lugar de en la elaboración de perfiles como tal, es decir, la creación y utilización de perfiles personales por parte de los responsables del tratamiento de datos, antes de adoptar una medida o incluso una decisión que afecte al interesado. De hecho, el derecho de oposición, en palabras del propio GT29[87], en relación a los medios de control de que dispone el interesado, "constituye un instrumento diferente que debe ejercerse en otra fase del tratamiento, una vez que el tratamiento ha comenzado, y tiene un fundamento jurídico diferente" .

En relación al control del comportamiento, el Considerando 24 establece que "(…) Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive 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". Obsérvese cómo aquí no se habla de que dicho tratamiento produzca "efectos jurídicos" o que le afecten "significativamente", sino simplemente de adoptar decisiones sobre él o analizar o predecir sus preferencias, comportamientos y actitudes. Por tanto, si estas actividades pueden considerarse un tratamiento que controla el comportamiento, ¿por qué establecer requisitos superiores (exigencia de que se produzcan efectos *jurídicos* o que afecten *significativamente*) a la hora de regularlos?

En relación a la pregunta inicial de qué ocurre cuando la elaboración de perfiles no afecte significativamente o no produzca efectos

---

[86] *Ibíd*., p. 3

[87] Dictamen 15/2011 sobre la definición de consentimiento, 13 de Julio de 2011, WP187 disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf

jurídicos, el propio GT29[88] da la respuesta: (la traducción es nuestra) "Cuando la elaboración de perfiles no afecte de manera significativa a los intereses, derechos o libertades del interesado, el artículo 20 no es aplicable y la legalidad del tratamiento debe evaluarse a la luz de otras disposiciones del Reglamento. Sin embargo, dada la amplitud del término "afectar significativamente", se necesita un mecanismo para interpretar y especificar esta frase para su aplicación práctica. Este mecanismo no sólo deberá tener en cuenta el alcance del derecho básico a la protección de datos. También debe evaluar los intereses de los Responsables y comprender un análisis de los posibles y reales impactos de las tecnologías de elaboración de perfiles en los derechos y libertades de los interesados".

No estamos de acuerdo con que cuando la elaboración de perfiles no afecte significativamente a los derechos y libertades del interesado no se aplique el artículo 22 del RGPD, por varias razones, la primera porque donde se regula lo más, se regula lo menos, por tanto no tiene ningún sentido acudir a otro artículo que no hable específicamente de elaboración de perfiles o toma automatizada de decisiones, cuando ya hay un artículo que lo regula. Pero también porque en palabras del propio GT29[89] "debido a la amplia disponibilidad y posibilidad de vincular datos en Internet y al hecho de que los dispositivos técnicos cuyo funcionamiento se basa en el procesamiento de datos personales impregnan nuestra vida cotidiana, el mundo en línea puede presentar uno de los mayores retos al derecho a la protección de datos personales en el siglo XXI, considerando, por ejemplo, las capacidades de localización geográfica de los dispositivos móviles que la mayoría de nosotros llevamos con nosotros la mayor parte del tiempo. Además, el telón de fondo del *big data* debe tenerse en cuenta aquí".

Por otro lado, ese mecanismo que demandaba el GT29 para poder interpretar el "afectar significativamente" y por tanto, aplicar el artículo en la práctica, no se ha desarrollado, al menos en el RGPD.

---

[88] *Ibíd*., p. 4.
[89] *Ibíd*., p. 2.

Y porque como el propio GT29 observa, se regula más bien el resultado de la elaboración de perfiles al requerir una afectación significativa o que produzca un efecto jurídico sobre el afectado, no al tratamiento de los datos que originarían (o no) ese resultado. En ambos casos necesitaremos tratar el mismo tipo de datos.

En consecuencia, y dado que como el propio RGPD establece en su considerando 24, la elaboración de perfiles supone un tratamiento que implica control del comportamiento, sin necesidad de que le "afecte significativamente", pues ya supone una afección significativa en sí misma, en nuestra opinión el artículo 22 debe aplicarse a cualquier tipo de elaboración de perfiles y/o toma de decisiones automatizadas.

- ¿qué otros supuestos pueden quedar englobados en el apartado primero? teniendo en cuenta que el tratamiento basado en el consentimiento, o cuando sea necesario para la ejecución/celebración de un contrato quedan comprendidos en el apartado segundo.
- En los supuestos comprendidos en el párrafo segundo (consentimiento del interesado o necesario para la ejecución/celebración de un contrato), ¿no es necesario informar sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado? El artículo 13.2f) dice claramente que se informará "al menos en tales casos", y por tanto, como mínimo en esos casos, refiriéndose exclusivamente a los apartados 1 y 4.

Consideramos que, ya que no se está solicitando el consentimiento del interesado para la realización de este tipo de tratamientos, el deber de información debería extenderse a todos los supuestos del artículo 22, ya que como el propio artículo 13.2 establece, "el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria *para garantizar un tratamiento de datos leal y transparente*".

Además, recordemos que la realización de este tipo de tratamientos basado en el consentimiento, se establece en el párrafo segundo, por lo que con más motivo debería cumplirse con el deber de información en estos casos.

Consideramos que, como tratamientos que implican un control del comportamiento como el propio RGPD establece y sobre los que pesa la obligación de realizar una evaluación de impacto, la elaboración de perfiles así como la toma automatizada de decisiones, son tratamientos en los que, como mínimo, se ha de cumplir con el derecho de información de la manera más amplia sin introducir excepciones.

Por último, recordar que "las decisiones basadas en la elaboración de perfiles" son uno de los puntos[90] sobre los que el Derecho de la Unión o de los Estados miembros puede imponer restricciones.

Con independencia de la regulación normativa y como indicábamos en el capítulo anterior, nada obsta a que se añada una última fase en la toma de dicha decisión que implique intervención humana, y así el responsable evite la aplicación de este artículo, lo cual en último término implicaría el cercenamiento *ab initio* de este derecho.

Por tanto, vemos cómo el RGPD no introduce nuevos instrumentos que doten a los interesados de un mayor control sobre sus datos, y además, los existentes (derecho de oposición a decisiones automatizadas, derecho a la supresión) no son suficiente para abordar con eficacia los nuevos retos que se plantean en esta sociedad de la información actual en la que el big data y otras técnicas, están siendo utilizadas.

[90] Vid. Considerando 73 del RGPD.

CONCLUSIONES

1-CAMBIO DE PARADIGMA

El *big data* ha irrumpido en nuestras vidas. Podemos hablar de un cambio de paradigma a nivel tecnológico, pues hemos evolucionado hasta el punto de ser capaces de datificar todos los aspectos de la vida y ser capaces de analizar dicha información y obtener nuevos datos, nueva información que aporte valor; Incluso a nivel científico, se habla de *Big Data* como el "cuarto paradigma", junto a los dos paradigmas tradicionales del método científico, la experimentación (*paradigma empírico*) y la teoría (*paradigma teórico*), y el posteriormente añadido, la simulación computacional o *paradigma de la simulación*. Consideramos que no se trata, en propiedad, de un cambio de paradigma en el modelo de investigación científico, pues no se desecha el paradigma previo, como vaticinó ANDERSON, sino que simplemente estamos ante la irrupción del *big data* en el ámbito científico y de investigación, que como bien indica LYNCH, permite la integración de los primeros tres paradigmas y su mutuo fortalecimiento. Por tanto, podemos hablar de un "cambio de paradigma" en el sentido disruptivo que el *big data* causará en nuestras vidas a todos los niveles, incluyendo el de la investigación científica, pero no en el sentido de crear un nuevo paradigma del método científico. Sea como fuere, estemos ante un cambio de paradigma o no, lo que es indiscutible es que la forma de investigar así como de publicar lo investigado, sí que ha cambiado (o debería cambiar) gracias a internet y al tratamiento de datos masivos, pero sin que ello suponga en absoluto el "fin de la teoría".

Pero también se produce un cambio de paradigma a nivel sociológico y humano, con consecuencias que no podemos obviar. El tratamiento de datos masivos puede aportarnos grandes beneficios a todas las personas, a nivel global, es decir, el *big data* puede ser muy

beneficioso para todos, cuando se utiliza para la búsqueda de un bien común, pudiendo hablar de *big data* como "bien público". No obstante lo anterior, como todas las cosas, el *big data* también puede tener un "lado oscuro" y creemos que no sólo debe analizarse el impacto de los tratamientos masivos de datos a un nivel estrictamente jurídico, pues la privacidad de las personas es un elemento muy importante para garantizar el libre desarrollo de la personalidad y, en último término, la libertad y la dignidad de las personas. No es casualidad que una de las conclusiones de la 36a Conferencia Internacional de Autoridades de Protección de Datos y Privacidad hiciera un llamamiento a todas las partes que utilizasen el *Big Data* para que las decisiones respecto al uso del *Big Data* sean justas, transparentes y responsables.

De hecho, el Consejo de Europa, a través del Comité consultivo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), ha publicado en 2017 unas *Directrices sobre la protección de los individuos en relación al Tratamiento de datos personales en un mundo de Big Data,* con el objeto de proporcionar un marco general para que las Partes apliquen las políticas y medidas adecuadas para hacer efectivos los principios y disposiciones del Convenio 108 en el contexto de *Big Data*. Las Directrices recomiendan medidas que las partes implicadas deberían adoptar para prevenir los posibles efectos negativos del *big data* sobre la dignidad humana, los derechos humanos y las libertades fundamentales individuales y colectivas, en particular en lo que respecta a la protección de datos personales. Así, se propugna un *Uso ético y social de los datos*, por el que los responsables y encargados deben tener debidamente en cuenta el probable impacto del tratamiento de *big data* y sus implicaciones éticas y sociales más amplias para salvaguardar los derechos humanos y las libertades fundamentales y garantizar el respeto del cumplimiento de las obligaciones en materia de protección de datos establecidas en el Convenio 108. El tratamiento de datos personales no debe estar en conflicto con los valores éticos comúnmente aceptados en la comunidad o las comunidades relevantes y no debe utilizarse en

detrimento de los intereses, valores y normas de la sociedad, incluida la protección de los derechos humanos. En relación a las *políticas preventivas y de valoración del riesgo*, deberán considerar el impacto legal, social y ético del uso de *Big Data*, incluido el derecho a la igualdad de trato y a la no discriminación. Las Directrices también contemplan el papel de la *intervención humana en las decisiones apoyadas por Big Data*, estableciendo que el uso de Big Data debe preservar la autonomía de la intervención humana en el proceso de toma de decisiones. La persona que intervenga en la toma de decisiones, sobre la base de argumentos razonables, deberá tener la libertad de no confiar en los resultados proporcionados a través de *big data*, con el objetivo de evitar la discriminación directa o indirecta basada en el análisis de Big Data.

Como señalan MAYER-SCHÖNBERGER y CUKIER, "puede que el día de mañana las generaciones siguientes tengan una conciencia de datos masivos: la presunción de que hay un componente cuantitativo en todo cuanto hacemos, y de que los datos son indispensables para que la sociedad aprenda", pero nuestra tarea hoy es preservar los derechos y libertades individuales otorgando al *big data* su justa posición, garantizando el debido equilibrio entre evolución tecnológica y el respecto a los derechos y libertades fundamentales, porque sólo así estaremos ante una sociedad justa y libre.

2- EL DIFERENTE ENCUADRE JURÍDICO DEL BIG DATA NO DEBE TRATARSE DE MANERA AISLADA

En relación al encuadre jurídico del *big data*, debemos distinguir dos escenarios o perspectivas: la perspectiva de la protección de un derecho fundamental, en la que se aplicará por tanto la normativa de protección de datos de carácter personal y un segundo escenario en el que el valor de los datos es el núcleo de la "futura economía de los datos", por tanto, desde la perspectiva de un bien económico.

Ambas perspectivas abordan la protección de bienes jurídicos e intereses diferentes, pero queda claro en cualquier caso, cuál es el bien jurídico de protección preferente, por tratarse de un derecho

fundamental de las personas. Esta situación conlleva que, en la práctica, se ha de ser muy cuidadoso en cuanto a las tipologías de datos tratados, no pudiendo excluir a priori de manera general la aplicación de la normativa de protección de datos.

En el contexto de la llamada economía digital, los datos juegan un papel de capital importancia, hasta el punto de hablar de la economía de los datos o economía basada en los datos. En relación a los datos generados por máquinas o el Internet de las cosas, con el objetivo de aprovechar al máximo este tipo de datos, la Comisión Europea considera imprescindible facilitar a los agentes del mercado el acceso a estos conjuntos de datos, lo cual es complicado pues, según la Comisión, los productores de los datos son los únicos con acceso, lo cual puede restringir su utilización en mercados descendentes. La Comisión es partidaria de crear un marco europeo para regular el acceso a estos conjuntos de datos, para evitar la fragmentación normativa dentro de Europa ya que sería negativa para el desarrollo de la Economía de los datos, y plantea cuestiones que deberán debatirse entre las diferentes partes implicadas. Dichas cuestiones tales como el acceso a los datos *anónimos* generados por máquinas, el intercambio de datos, la protección de las inversiones y los activos, y la protección de la confidencialidad, son de capital importancia y consideramos que no deben tratarse aisladamente como si no tuvieran incidencia sobre el derecho fundamental de protección de datos y relegando de cualquier decisión sobre la información al usuario, que es al fin y al cabo quien ha generado los datos. La Comisión propone incluso, entre otras medidas, llegar a crear un derecho real o una especie de derecho de propiedad sobre la información no personal para el "productor" de los datos no personales o anónimos, que no es el titular. Es por ello que, además de la importancia de dichas cuestiones por su potencial repercusión en la privacidad de las personas, consideramos que debe dotarse al análisis de la Comisión de una coherencia jurídica que permita el encaje de todas las cuestiones mencionadas, pues en nuestra opinión no deben tratarse como compartimentos estancos la información de carácter personal y la que no lo es, pues al fin y al

cabo, se trata de información, y no puede dotarse a la misma de una naturaleza jurídica diferente en uno u otro caso.
Coincidimos con la postura del Parlamento Europeo que considera que la posición de la Comisión Europea está muy impulsada por el comercio y la economía, prestando poca atención a los retos legales y sociales clave y que si bien *Big Data* se presenta como una oportunidad de mercado que no debe perderse, la privacidad y la protección de datos, así como los riesgos mencionados anteriormente sobre Big Data, se abordan sólo marginalmente.

3-MISMOS PROBLEMAS, DIFERENTES NORMAS

Como se puso de manifiesto en los capítulos segundo y tercero, el derecho a la protección de datos de carácter personal o el derecho a la privacidad, han tenido una génesis e historia muy diferente en Europa y en EEUU, lo que ha conducido a la existencia de dos regímenes muy dispares, donde ni siquiera el concepto de "dato de carácter personal" es unívoco.
En un mundo globalizado, todos nos vemos afectados por los nuevos riesgos que la Sociedad de la información actual plantea, lo cual se pone de manifiesto con el tratamiento de datos masivos o *big data*. El desarrollo tecnológico no ha hecho sino poner de relieve estos riesgos y los diferentes enfoques que cada legislación realiza de los mismos problemas. Esta situación conduce a que se puedan adoptar soluciones muy dispares, que ningún sentido tienen en un mundo en el que no existen las fronteras, el mundo digital.
Como manifestó la propia Comisión Europea en su Comunicación al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, *Un enfoque global de la protección de los datos personales en la Unión Europea,* COM(2010) 609 final, "El tratamiento de datos es un proceso a escala mundial y requiere la elaboración de normas universales para la protección de las personas por lo que respecta al tratamiento de los datos personales" .
Así lo ponen de manifiesto determinados autores (KUNER, CHRISTOPHER, CATE, FRED H., MILLARD, CHRISTOPHER Y SVANTESSON,

DAN JERKER B., "The challenge of 'big data' for data protection", *International Data Privacy Law*, 2012, vol. 2, n. 2) con los que coincidimos plenamente cuando afirman "dado que los datos personales son universalmente recolectados y compartidos a través de las fronteras sectoriales y nacionales, las leyes de protección de datos inconsistentes plantean amenazas crecientes para las personas, las instituciones y la sociedad".

Por tanto, consideramos que la única vía para garantizar una verdadera protección de los derechos y libertades fundamentales de las personas, a la par que conseguir un verdadero mercado global digital, pasa por la adopción de un instrumento vinculante a nivel internacional, como ya ha propuesto la OCDE, así como por la creación de un organismo internacional que supervise y regule este marco normativo común. Además, no solamente a nivel de protección de datos, sino también sobre protección de los derechos del consumidor, actividades criminales, cuestiones de competencia y cualquier aspecto que pueda afectar al mercado internacional de datos y a los derechos y libertades fundamentales de los individuos.

4-LA CONTINUIDAD DEL RGPD DEL ESPÍRITU DE LA DIRECTIVA 95/46

El RGPD ha creado nuevas obligaciones para los Responsables de tratamiento como los informes de impacto de privacidad, la obligación de notificar brechas de seguridad, el Principio de responsabilidad (*accountability*), entre otras, pero en nuestra opinión no podemos hablar de una profunda reforma de la normativa de protección de datos que nos provea de un nuevo marco jurídico que dote de seguridad jurídica y de confianza a los actores que en él intervienen, dado que conceptos clave como el de "dato de carácter personal" o los principios de protección de datos establecidos por la Directiva 95/46, se mantienen sin apenas cambios.

En relación a los nuevos retos que para la normativa de protección de datos suponen nuevos fenómenos tales como el tratamiento de datos masivos (*big data*), el RGPD ni siquiera lo menciona en su articulado,

salvo que se esté aludiendo a estas técnicas cuando habla de "grandes cantidades de datos" o "tratamientos a gran escala".

Respecto a la evolución de los principios de protección de datos, el Principio del consentimiento únicamente puede evolucionar en la manera en que éste se recoge y presta. En el caso de los datos masivos, la evolución de este Principio radica precisamente en asumir que no sirve para cubrir estos nuevos supuestos que la datificación y los datos masivos nos plantean o los que puedan existir en un futuro. Solamente siendo conscientes de que el consentimiento no cubre ni puede cubrir todos los supuestos, nos plantearemos la necesidad de introducir nuevos instrumentos que respeten los derechos de los interesados. Es por ello que hay autores (MAYER-SCHÖNBERGER y CUKIER) que propugnan un cambio desde la "privacidad por consentimiento" a la privacidad a través de la responsabilidad". En esta línea se enmarca el Principio de Responsabilidad o *Accountability,* pero lo cierto es que en relación al modelo de obtención del consentimiento, lejos de modificarse, se refuerza el sistema tradicional de información-obtención del consentimiento, ampliando el contenido de la información obligatoria como medio para reforzar el carácter informado de dicho consentimiento.
Por otro lado, en relación al Principio de Calidad, resulta muy criticable el párrafo cuarto del artículo 6, por su ubicación sistemática ya que parece dar carta de naturaleza a tratamientos posteriores para fines distintos (*compatibles*), al inducir a confundir compatibilidad con legimitidad. De ser así, es decir, de no exigirse además de superar la prueba de compatibilidad, un fundamento legal para el tratamiento, se estarían autorizando tratamientos que actualmente están prohibidos por la Directiva 95/46, y por tanto, rebajando los estándares de protección.
Podemos concluir que muchos de los objetivos propuestos por la Comisión Europea en la Comunicación COM (2010) 609 final se han conseguido con el RGPD, pero en relación al objetivo de reforzar los derechos de las personas, a pesar de los cambios positivos introducidos como por ejemplo la obligación de notificar brechas de

seguridad, el Principio de Responsabilidad y el derecho de portabilidad, no es lo suficientemente ambicioso como para innovar en conceptos tradicionales como el de "dato personal" ni previsor suficiente en relación a las tecnologías emergentes, como para garantizar los derechos de las personas. ¿Cómo garantizar con las mismas "armas" los derechos de las personas en "distintos" escenarios? Por muy flexibles que sean los Principios rectores en materia de protección de datos, únicamente es posible introduciendo nuevas herramientas y mecanismos, fruto de dicha flexibilización, destinados a garantizar los derechos y libertades de las personas en estos nuevos entornos en los que ya estamos inmersos.

5-LOS AVANCES TECNOLÓGICOS NO PUEDEN OBLIGAR A LA ASUNCIÓN DE UNA PÉRDIDA DE PRIVACIDAD POR DEFECTO

El Principio de la privacidad por defecto es un muy buen punto de partida para garantizar los derechos de las personas. El hecho de que la normativa no pueda evolucionar al ritmo de la tecnología para dar respuesta a los nuevos retos que este nuevo mundo digital nos plantea, no debe repercutir negativamente en las personas, de modo que vean aminorado o afectado de cualquier manera negativamente, su derecho a la protección de datos personales, su derecho a la intimidad, sus derechos y libertades en definitiva. Debemos ser capaces de construir normas tecnológicamente neutrales que salvaguarden los derechos y libertades fundamentales de los individuos y la Directiva 95/46 es buena prueba de ello.

Como decía la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), si los Principios de privacidad no se respetan, el *big data* fracasará. "Por lo tanto, los desafíos de privacidad deben considerarse como oportunidades que, si se manejan adecuadamente, pueden generar confianza en el gran ecosistema de datos en beneficio tanto de los usuarios como de la gran industria de datos".

Disponemos de un nuevo instrumento jurídico, el RGPD, que dota de una protección uniforme a nivel de protección de datos en Europa,

pero los principios de protección de datos deben aplicarse de una manera efectiva y no a sabiendas de que los acontecimientos han superado la protección que dichos principios pueden ofrecer ante la realidad de los tratamientos de datos que a día de hoy se están produciendo, lo cual no es motivo para que los individuos asuman o tengan que asumir una pérdida de privacidad por defecto. En este punto cobra especial importancia el Principio de responsabilidad proactiva (*accountability*) que establece el RGPD.

6- LA EVOLUCION DE LOS PRINCIPIOS DE PROTECCION DE DATOS DEBE CONLLEVAR UN REFORZAMIENTO REAL DE LOS DERECHOS Y LIBERTADES DE LAS PERSONAS

Cuando unos Principios se mantienen vigentes con el paso de los años, ponen de manifiesto su eficacia y actualidad. Ello no quiere decir que no sea necesario introducir modificaciones o nuevos conceptos que solventen los problemas actuales que en el pasado no existían. Hemos visto cómo el RGPD mantiene los tradicionales principios y conceptos, y lejos de actualizar el esquema clásico de información- obtención del consentimiento, lo refuerza y es obvio que hay situaciones que no quedan cubiertas por los esquemas clásicos y Principios concebidos en la era pre-internet.

Big data exige más que nunca reforzar los sistemas que garanticen los derechos fundamentales de las personas dado el riesgo que estas técnicas suponen para los mismos. Ignorar la cuestión y seguir anclados en los viejos esquemas pretendiendo que funcionen para todo tipo de tecnología, supondrá permitir su posible vulneración por lo que no es una opción a tener en cuenta.

A la vez, deberá poner especial cuidado en respetar los derechos y libertades de las personas, para que no se vean afectados en ningún modo por efecto de conclusiones obtenidas de manera automatizada o tratamientos de datos no autorizados o sin las debidas medidas de seguridad y anonimización.

Hay autores (KUNER, CHRISTOPHER, CATE, FRED H., MILLARD, CHRISTOPHER Y SVANTESSON, DAN JERKER B.) que ponen de manifiesto

que lo importante ya no son los datos en sí mismos o la privacidad, sino conceptos tales como la accesibilidad, precisión y fiabilidad de dichos datos. Así, entendemos que es necesario un cambio de enfoque en el que el epicentro no sean los datos sino la tecnología, la utilización del dato, pues tener ingentes cantidades de datos no es sinónimo de obtener la información adecuada. Coincidimos por tanto con BERGKAMP cuando afirma que el foco debería colocarse en la utilización, los usos del dato, no en el dato en sí mismo. Como afirman MAYER-SCHÖNBERGER y CUKIER, "tenemos que proteger la privacidad desplazando la responsabilidad de los individuos hacia los usuarios de datos: es decir que rindan cuentas por su uso". En este punto cobra especial importancia el Principio de responsabilidad proactiva (*accountability*) que establece el RGPD. De este modo, para aquellos casos en que el consentimiento ya no pueda ofrecernos todas las respuestas, deberemos introducir **nuevas medidas destinadas a garantizar la protección de este derecho fundamental**. Estas nuevas medidas pueden poner el centro de atención en el Responsable, exigiéndole determinadas garantías en relación a la anonimización, basándonos en el Principio de responsabilidad en el cumplimiento.

Otras medidas serían de carácter preventivo, evitando la recopilación de datos que funcionen o puedan funcionar como identificadores, como por ejemplo, el número único que puede generarse a partir del nivel de batería restante del dispositivo que es recogido por la página web para, en principio, desactivar determinadas funcionalidades que reduzcan la duración de la batería y así generar más tiempo de navegación para el usuario.

De esta manera, además de consentir un tratamiento actual o presente, deberíamos poder decidir sobre posibles extracciones de datos futuros o predicciones, limitando por tanto *ab initio* determinados usos o finalidades de los datos, estableciendo un **derecho de exclusión.** Podemos por tanto pensar en la posibilidad de que el interesado pueda manifestar a priori la negativa a que sus datos sean objeto de tratamientos masivos de datos (*big data*) como una suerte de *opt-out* o lista de exclusión. Tanto en su vertiente "formal", señalando una casilla por ejemplo, como en su vertiente "técnica", (un derecho de

exclusión técnico), es decir, respecto al tratamiento masivo de datos obtenidos de los dispositivos conectados a redes o internet, desde ordenadores, dispositivos móviles, hasta cualquier objeto conectado al "Internet de las cosas", los usuarios que no desearan que los datos de conexión o tráfico de sus dispositivos fueran tratados masivamente, deberían poder especificarlo en la "configuración" del dispositivo. Para hacer efectivos estos mecanismos de "consentimiento" o de "manifestación de voluntad" deberían ser incorporados en los estándares de comunicaciones de Internet. La exclusión técnica requeriría que los protocolos informáticos con los que se construyen los sistemas de comunicaciones y publicación de información contemplaran la posibilidad de que el usuario manifestara su voluntad de que sus datos no sean objeto de tratamientos masivos. Mientras estas medidas técnicas no formen parte de los estándares HTTP y HTML y no se implementen desde la perspectiva de la privacidad desde el diseño, no podremos hablar de universalidad y adecuación de la medida. Por tanto, vemos cómo técnicamente es posible establecer los mecanismos para que los usuarios puedan manifestar su deseo de no participar en tratamientos masivos de datos. No obstante, dependerá de multitud de factores que esto se llegue a implementar. Pensemos que el mecanismo DNT todavía no está implantado a nivel de todos los navegadores, por lo que queda mucho camino por recorrer

En relación a la introducción de nuevos conceptos, consideramos conveniente incluir una **nueva categoría de información protegible**, sin necesidad de ampliar el ya de por sí amplio concepto de "dato personal". Bien podría considerarse que, si esta nueva categoría de información protegible lo es porque puede llegar a constituir "dato personal", podría quedar englobada en el concepto de "dato personal" por ser "identificable" y por tanto, no sería necesario crearla; pero como apuntamos, esto constituiría una expansión injustificada del concepto de dato personal que nos llevaría a considerar dato personal a toda información relativa a personas, sólo por el mero hecho de poder llegar a ser un día identificables, no por serlo actualmente.

Entonces el problema radica en trazar la delimitación entre "información protegible" y "dato personal". Una posible solución podría ser, como apunta KOOPS, en lugar de tratar de delimitar dicha frontera entre dato personal y no personal, establecer aquellas categoría de datos o información que pueden tener efectos sobre las personas, con independencia de si son relativos a personas identificables o no. Consideramos por tanto, que en lugar de ampliar el concepto de dato de carácter personal, debería crearse una nueva categoría de "información protegible" sobre la cual se tomasen determinadas medidas de seguridad, en lugar de simplemente recibir el tratamiento que se daría a una información anónima o en todo caso, sobre la que no se aplicase la normativa de protección de datos de carácter personal.

Otra medida que garantizaría el respeto a los derechos de las personas, es la configuración de un **verdadero derecho al olvido**, no ligado a la protección de datos personales y por tanto, que sirva para todos aquellos casos (y no sólo en determinados supuestos tasados) en que se desee que una determinada información desaparezca de la red, y porque no siempre estaremos ante un "Responsable de tratamiento".

7- NUEVO MARCO JURÍDICO DE LA ECONOMÍA DE LOS DATOS

Los beneficios y aplicaciones que los tratamientos masivos de datos o *big data* pueden reportar a los individuos y a la sociedad, son innumerables e incluso desconocidos en su totalidad en la actualidad. Podemos plantear la aplicación de técnicas de *big data* a casi cualquier ámbito de la vida, incluído el método científico de investigación, por lo que los beneficios son muy variados, tanto para el sector privado, por la mejora en competitividad y eficiencia para las empresas, debido al mayor conocimiento del cliente y del producto, como para la Administración Pública, que obtendría una mayor eficiencia operativa (debido a una mayor transparencia), aumento de la recaudación de impuestos y reducción del fraude. Todo ello ha llevado a la Unión Europea a querer sentar las condiciones marco

adecuadas para un mercado único de los macrodatos (*big data*) y la computación en nube, para establecer las características de la futura economía de los datos. En 2017, y sobre la base de las conclusiones de la Comunicación COM/2014/0442 final, la Comisión Europea ha adoptado la Comunicación Construyendo una economía europea de datos COM (2017) 9 final, con el objetivo de, tras la aprobación del RGPD y el proyecto de Reglamento sobre privacidad y comunicaciones electrónicas, crear un marco político y jurídico claro, adaptado para la economía de datos, suprimiendo las barreras que subsisten a la circulación de datos y abordando las incertidumbres jurídicas creadas por las nuevas tecnologías basadas en datos. Este nuevo marco jurídico regulará tanto los tratamientos masivos de datos provenientes tanto del sector público, sometido a las normativas sobre reutilización de la información pública (datos abiertos u open data), como del sector privado, donde no existe regulación respecto a los datos no personales o anónimos, ni obligación de poner a disposición de terceros la información de que se dispone. En el sector público se ha establecido la obligación de poner la información a disposición de los diferentes agentes con fines privados o comerciales para "favorecer la circulación de información hacia los agentes económicos y la ciudadanía con el fin de fomentar el crecimiento económico, el compromiso social y la transparencia", tal y como se afirma en la Ley 18/2015 por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público**.** Respecto a la información en poder del sector privado, la Comisión Europea es consciente de que deben incluirse normas que incentiven al sector privado a compartir dicha información, ya que sólo así podremos hablar de una verdadera economía basada en datos.

Además, este nuevo marco jurídico deberá garantizar el derecho fundamental de protección de datos de los individuos, por encima de la creación de nuevos derechos sobre los datos no personales, pues la línea que separa los datos personales de la información no personal o anónima, es cada vez más difusa. Como se ha analizado en el presente trabajo, el diferente encuadre jurídico del *big data*, bien desde la perspectiva de la protección de un derecho fundamental, o bien desde

la perspectiva de un bien económico como epicentro de la llamada "economía de los datos", no puede tratarse de manera aislada o independiente.

El respeto al derecho a la protección de datos de carácter personal, y en general, a la privacidad de las personas, que este nuevo marco jurídico debe tener como premisa, debe ir unido indisolublemente, con un uso ético y social de los datos, para prevenir los posibles efectos negativos del *big data* sobre la dignidad humana, los derechos humanos y las libertades fundamentales individuales y colectivas. Destacar en este sentido las *Directrices sobre la protección de los individuos en relación al Tratamiento de datos personales en un mundo de Big Data*, del Consejo de Europa para hacer efectivos los principios y disposiciones del Convenio 108 en el contexto de *Big Data*. El impacto de los tratamientos masivos de datos no sólo debe analizarse a un nivel estrictamente jurídico, sino que ha de prestarse la debida atención a cuestiones éticas y sociales, pues la privacidad de las personas es un elemento muy importante para garantizar el libre desarrollo de la personalidad y, en último término, la libertad y la dignidad de las personas, pero podrían verse afectados otros derechos humanos y libertades fundamentales.

BIBLIOGRAFÍA

ABRAMS, M., *Data origin and the proposed regulation*, en RALLO LOMBARTE, ARTEMI y GARCÍA MAHAMUT, ROSARIO y otros, *Hacia un nuevo Derecho Europeo de Protección de Datos*, Ed Tirant lo Blanch, Valencia, 2015, pp. 85-101.

APARICIO SALOM, J., Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Navarra, Aranzadi, 2000.

BAJO FERNÁNDEZ, M., *Comentarios a la Legislación penal*, Cobo del Rosal, M., (Dir), Bajo Fernández, M., (Coord.) *Derecho penal y Constitución: Protección del honor y de la intimidad*, Ed. Edersa, Madrid, Tomo I,1982, pp. 97-127.

BANAFA, AHMED "Un lago de datos: ¿una oportunidad o un sueño para el Big Data?", 07 diciembre 2015, disponible en https://www.bbvaopenmind.com/un-lago-de-datos-una-oportunidad-o-un-sueno-para-el-big-data/

BANCO SANTANDER CENTRAL HISPANO, 2000, *Esp@ña on-line, ideas para afrontar la e-conomía*, Madrid, BSCH y Andersen Consulting.

BEANEY, WILLIAM M., *The Right to Privacy and American Law*, 31 Law and Contemporary Problems 253-271 (Spring 1966).

BERGKAMP, LUCAS, "The privacy fallacy: adverse effects of europe's data protection policy in an information-driven economy", Computer Law & Security Report Vol. 18 no. 1, 2002.

BRENDAN VAN ALSENOY & MARIEKE KOEKKOEK, "The extra-territorial reach of the EU's Right to be forgotten", Working Paper no. 152, Marzo 2015, disponible en https://ghum.kuleuven.be/ggs/publications/working_papers/new_series/wp151-160/wp152-alsenoy-koekkoek.pdf

BCaRUENING, P., "Rethink Privacy 2.0 and Fair Information Practice Principles: A Common Language for Privacy", 19 Octubre de 2014, disponible en http://blogs.intel.com/policy/2014/10/19/rethink-privacy-2-0-fair-information-practice-principles-common-language-privacy/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+IntelPolicy+%28Policy%40Intel%29

CALABUIG, O. (2014): "¿Qué es Big Data? Las entrañas de los datos". Dossier para el Institut de la Comunicació de la UAB. Consultable en http://portalcomunicacion.com/monograficos_det.asp?id=261

CAMARGO VEGA, J.J., CAMARGO ORTEGA, J.F., JOYANES AGUILAR, L., "Conociendo Big Data", Revista Facultad de Ingeniería (Fac. Ing.), Enero-Abril 2015, Vol. 24, n 38, pp 63-77.

CAVOUKIAN, A. y CASTRO, D., "Big data and innovation, setting the record straight: de-identification does work". Office of the Information and Privacy Commissioner, Ontario, Junio 2014.

COLES, TODD ROBERT., "Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption", THE AMERICAN UNIVERSITY LAW REVIEW, Vol. 40:957, p 957-1002.

DAGGETT, LYNN M., "FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students", 58 Cath.

U. L. Rev. 59 (2009). Disponible en: http://scholarship.law.edu/lawreview/vol58/iss1/4

EL EMAM, K., y ÁLVAREZ, C., "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", International Data Privacy Law, Oxford University Press (2015) 5 (1): 73-87.

FAYOS GARDÓ, A., Los derechos a la intimidad y a la privacidad en el siglo XXI, Dykinson, Primera edición, 2015.

FRIED, CHARLES, "Privacy" en *Philosophical dimensions of privacy*, Cambridge University Press, 1984, Ferdinand David Schoeman pp 203-222.

FUNDACIÓN TELEFÓNICA, varios autores, *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados,* Fundación Telefónica, Cuaderno 36, Ed Ariel, 2012, CC BY NC-SA 3.0.

GARCÍA-BERRIO HERNÁNDEZ, TERESA; Informática y libertades. La protección de datos personales y su regulación en Francia y España, Colección estudios de derecho, Universidad de Murcia, 2003.

GARRIGA DOMÍNGUEZ, ANA., *Nuevos retos para la protección de datos personales*, Ed DYKINSON Madrid, 2016.

GARZÓN CLARIANA, G., "*La protección de los datos personales y la función normativa del consejo de Europa",* Revista de Instituciones Europeas, Vol 8, n 1, Enero-Abril 1981.

GÓMEZ SÁNCHEZ, Y., "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *Revista Derecho y Salud*, Vol. 16, No Extra 1, 2008, XVI Congreso «Derecho y Salud», pp 59 a 78.

GREENLEAF, GRAHAM, The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?, Edimburgh School of Law Research paper series, No 2012/12, University of Edimburgh.

H. CATE, F., *Privacy in the Information Age*, Brookings Institution Press, 1997.

HEY, T., TANSLEY, S., & TOLLE, K. (Eds.). (2010). *The Fourth Paradigm: Data-Intensive Scientific Discovery*: Microsoft Research http://www.uam.mx/casadelibrosabiertos/libroselectronicos/4toparadigma/4toparadigma/assets/basic-html/page227.html

HERRÁN ORTIZ, ANA ISABEL, "El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales" Ed Dykinson S.L., Madrid 2002.

HERRÁN ORTIZ, ANA ISABEL, "La violación de la intimidad en la protección de datos personales", Ed Dykinson, 1998.

IBM Global Business Services Business, Informe Ejecutivo, en colaboración con la Escuela de Negocios Saïd en la Universidad de Oxford "Analytics and Optimisation, Analytics: el uso de big data en el mundo real *Cómo las empresas más innovadoras extraen valor de datos inciertos",* IBM Corporation 2012, pág 5. Disponible en http://www-05.ibm.com/services/es/gbs/consulting/pdf/El_uso_de_Big_Data_en_el_mundo_real.pdf

KEELE, BENJAMIN J. (2009) "Privacy by Deletion: The Need for a Global Data Deletion Principle," Indiana Journal of Global Legal

Studies: Vol. 16: Iss. 1, Article 14. Disponible en http://www.repository.law.indiana.edu/ijgls/vol16/iss1/14
KOOPS, BERT-JAAP, Forgetting footprints, shunning shadows. a critical analysis of the "right to be forgotten" in big data practice, Volume 8, Issue 3, December 2011, CC BY-NC-ND.

KOOPS, BERT-JAAP, *The Trouble with European Data Protection Law* (August 29, 2014). International Data Privacy Law, doi: 10.1093/idpl/ipu023, Forthcoming; Tilburg Law School Research Paper No. 04/2015.

KRÜGER, K. *El concepto de la 'Sociedad del Conocimiento'*. Biblio 3W, Revista Bibliográfica de Geografía y Ciencias Sociales, Universidad de Barcelona, Vol. XI, nº 683, 25 de septiembre de 2006. Disponible en http://www.ub.es/geocrit/b3w-683.htm

KUNER, CHRISTOPHER, CATE, FRED H., MILLARD, CHRISTOPHER y SVANTESSON, DAN JERKER B., *The challenge of 'big data' for data protection,* International Data Privacy Law, 2012, Vol. 2, No. 2.

LAZARO, CHRISTOPHE y LE MÉTAYER, DANIEL *The control over personal data: True remedy or fairy tale ?* Project-Teams Privatics, Research Report N° 8681, 13 Abril de 2015

LESMES SERRANO, CARLOS y otros, La Ley de Protección de Datos. Análisis y comentario de su Jurisprudencia, Ed LEX NOVA, Febrero 2008.

LUCAS MURILLO, P., El Derecho a la Autodeterminación Informativa, Temas clave de la constitución española, Ed Tecnos, 1990.

MARCHENA GÓMEZ, MANUEL, Intimidad e informática: la protección jurisdiccional del habeas data, Boletín de información del

Ministerio de Justicia e Interior num 1768, 15 Feb 1996, disponible en http://www.mjusticia.gob.es/cs/Satellite/1292344076377?blobheader=application%2Fpdf&blobheadername1=Content

MATÉ JIMÉNEZ, Carlos. *"Big data." Un nuevo paradigma de análisis de datos.* Anales de mecánica y electricidad, ISSN 0003-2506, v. 91, Fasc. 6, 2014, p. 10-16. Consulta 13-07-2016. http://www.revista-anales.es/web/n_29/pdf/10-16.pdf?r=1

MAYER-SCHÖNBERGER, VIKTOR y CUKIER, KENNETH, *Big Data. La revolución de los datos masivos*, Turner Publicaciones SL, Primera edición Junio 2013.

MAYER-SCHÖNBERGER, VIKTOR, *The virtue of forgetting in the digital age*, 2009 Oxford University Press.

MENÉNDEZ MATO, J.C. y GAYO SANTA CECILIA, Ma E., "Derecho e Informática: Ética y Legislación", Ed Bosch, 2014.

MIRALLES LÓPEZ, Ramón, *Aspectos a considerar en relación al Big Data,* Observatorio Iberoamericano de Protección de Datos, 25 de Julio de 2014, consulta 11-03-2017, disponible en http://oiprodat.com/2014/07/25/aspectos-a-considerar-en-relacion-al-big-data/

MIRALLES MIRAVET, S., "Big data, un nou bé jurídic?" Món jurídic, Revista del Colegio de Abogados de Barcelona, ISSN 1135-9196, Núm 293, 2015, pp 18-19, disponible en CAT en http://www.icab.cat/files/242-474995-DOCUMENTO/293b.pdf

MOOR, JAMES H, The Ethics of Privacy Protection, Library Trends, Vol 39, núm 1 y 2, Verano/Otoño 1990, p 69-82

NEIL M. RICHARDS & JONATHAN H. KING, *Three paradoxes of big data,* 66 STANFORD LAW REVIEW ONLINE, Vol. 66:41, September 3, 2013, pgs 41-46.

OHM, PAUL, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* (August 13, 2009). UCLA Law Review, Vol. 57, p. 1701, 2010; U of Colorado Law Legal Studies Research Paper No. 9-12.

OLEJNIK Ł., ACAR G., CASTELLUCCIA C., DIAZ C. (2016) THE LEAKING BATTERY. IN: GARCIA-ALFARO J., NAVARRO-ARRIBAS G., ALDINI A., MARTINELLI F., SURI N., "The leaking battery, A Privacy Analysis of the HTML5 Battery Status API", (eds) Data Privacy Management, and Security Assurance. DPM 2015, QASA 2015. Lecture Notes in Computer Science, vol 9481. Springer, Cham, Disponible en http://eprint.iacr.org/2015/616.pdf

OLOZÁBAL ECHAVARRÍA JJ, "Los derechos fundamentales en la Constitución Española", Revista de Estudios Políticos (Nueva Época) Núm 105, Julio-Septiembre 1999.

ORTEGA ÁLVAREZ, LUIS IGNACIO y otros, "La seguridad integral europea", Ed Lex Nova, Valladolid 2005.

ORTÍ VALLEJO, A., "Derecho a la intimidad e informática. (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)" Ed Comares, Granada 1994.

PAREDES-MORENO, A., (2015). Big Data: Estado de la cuestión. International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC), Vol. 2, Num. 1, pp. 38-59. Consultado el 13/07/2016 en www.ijisebc.com

PAVÓN PÉREZ, JUAN ANTONIO, "La protección de datos personales en el Consejo de Europa: el protocolo adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales" Anuario de la Facultad de

Derecho, Anuario de la Facultad de Derecho, No 19-20, 2001-2002, pág 235 a 252.

PAZOS CASTRO, R., "El mal llamado derecho al olvido en la era de internet", BMJ núm. 2183. Noviembre 2015 - ISSN: 1989-4767 - www.mjusticia.es/bmj

PAZOS CASTRO, R., "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible?", Revista INDRET 1/2001, Barcelona, Enero 2015, disponible en http://www.indret.com/pdf/1118_es.pdf

PIÑAR MAÑAS, J.L., y CANALES GIL, A. *Legislación de protección de datos*, (2ª Ed), Iustel. Madrid, 2011.

PROSSER, WILLIAM L, *Privacy*, 48 Cal. L. Rev. 383 (1960). Disponible en: http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1

RALLO LOMBARTE, ARTEMI (coord.), GARCÍA MAHAMUT, ROSARIO (coord.*), Hacia un nuevo derecho europeo de protección de datos,* Ed Tirant lo Blanch, 1ª edición 2015.

RALLO LOMBARTE, ARTEMI, "Hacia un nuevo sistema europeo de protección de datos las claves de la reforma", UNED *Revista de Derecho Político* Nº 85, Septiembre-Diciembre de 2012, pp. 13-56.

RALLO LOMBARTE, ARTEMI y GARCÍA MAHAMUT, ROSARIO *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia 2015.

RALLO LOMBARTE, ARTEMI, *El derecho al olvido en internet Google versus España,* Cuadernos y debates num 233, Centro de Estudios Políticos y Constitucionales, Madrid 2014.

RECIO GAYO, MIGUEL, Protección de datos personales e innovación: ¿(in) compatibles?, 1ª Edición, Ed Reus SA, 2016.

RICHARDS, NEIL M. y KING, JONATHAN H., "Three paradoxes of big data", (September 3, 2013), 66 Stanford Law Review Online 41 (2013).

RODRÍGUEZ LAINZ, JOSÉ LUIS, "El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre", Diario La Ley, No 8122, Sección Doctrina, 9 Jul. 2013, Año XXXIV, Editorial LA LEY.

ROLLNERT LIERN, GÖRAN. "El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la ley de transparencia", UNED Revista Teoría y Realidad Constitucional, Núm 34, 2014, pp 349-368.

RUBINSTEIN, IRA y HARTZOG, WOODROW, "Anonymization and Risk", August 17, 2015, Washington Law Review, Vol. 91, No. 2, 2016; NYU School of Law, Public Law Research Paper No. 15-36.

RUBINSTEIN, IRA, "Big Data: The End of Privacy or a New Beginning?" (October 5, 2012). International Data Privacy Law (2013 Forthcoming); NYU School of Law, Public Law Research Paper No. 12-56.

SALDAÑA, M.N., "El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego", UNED Teoría y Realidad Constitucional Nº 28, 2011, pp. 279-312.

SEMPERE SAMANIEGO, F.J., "Comentarios prácticos a la propuesta de Reglamento de Protección de Datos de la Unión Europea", Libro publicado mediante licencia Creative Commons Reconocimiento-No Comercial-Compartir igual, CC BY-NC-SA, 7 de Septiembre de 2013.

SCHWARTZ, PAUL M. and SOLOVE, DANIEL J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 N.Y.U. L.Q. Rev. 1814 (2011), Disponible en: http://scholarship.law.berkeley.edu/facpubs/1638
SOLOVE, DANIEL J. *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 (2002).
Disponible en :
http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2

SOLOVE, DANIEL J. "A Brief History of Information Privacy Law". PROSKAUER ON PRIVACY, PLI, 2006; GWU Law School Public Law Research Paper No. 215.

SHATTUCK, JOHN, "Computer matching is a serious threat to individual rights", Communications of the ACM, Junio 1984, Volumen 27, Número 6 (pp. 538-541).

TEJERINA RODRÍGUEZ, OFELIA, *Seguridad del estado y privacidad*, Reus, Madrid, 2014.

TORRES I VIÑALS, JORDI, "Del cloud computing al Big Data", FUOC. Fundación para la Universitat Oberta de Catalunya, Septiembre 2012, CC-BY-NC-ND, disponible en http://www.jorditorres.org/wp-content/uploads/2012/03/Del.Cloud_.Computing.al_.Big_.Data_.Jordi Torres.ES_.pdf

TORRES VENTOSA, JUAN JOSÉ, *La regulación legal de los Secretos Oficiales*. Anuario de la Facultad de Derecho, 1998, no 16, p. 357-388.

USTARÁN, E., *The future of privacy*, Data Guidance 2013.

VILASAU, MÓNICA. 2006 "La Directiva 2006/24/CE sobre conservación de datos del trafico en las comunicaciones electrónicas:

seguridad v. Privacidad" [articulo en línea]. IDP. Revista de Internet, Derecho y Política. No. 3. UOC. [Fecha de consulta: 04/10/2015]. http://www.uoc.edu/idp/3/dt/esp/vilasau.pdf

VIZCAÍNO CALDERÓN, MIGUEL, Comentarios a la Ley Orgánica de protección de datos de carácter personal, Ed Civitas, Madrid 2001, 1ª Edición.

WESTIN, ALAN *Privacy and Freedom*, Atheneum, New York.

ZABÍA DE LA MATA, J. (Coord) y otros autores, *Protección de Datos. Comentarios al Reglamento*, Ed LEX NOVA S.A., 2008.

Informes y documentos

Informe de ICO, UK Information Commissioner's Office, "*Big data and data protection"*, 28 de Julio de 2014, disponible en https://ico.org.uk/media/1541/big-data-and-data-protection.pdf
El 10 de Abril de 2015, se publica un resumen de actualización del Informe, tras un período de consulta pública "*Summary of feedback on Big data and data protection and ICO response*", disponible en https://ico.org.uk/media/for-organisations/documents/1043723/summary-of-feedback-on-big-data-and-data-protection-and-ico-response.pdf

Informe de ICO, UK Information Commissioner's Office, "*Big data, artificial intelligence, machine learning and data protection*", 1 de Marzo de 2017, disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS y Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, *Código de buenas prácticas en protección de datos para proyectos Big Data* disponible en

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf
Licencia Reconocimiento- No comercial- Sin Obra Derivada 4.0 Internacional de Creative Commons

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Orientaciones y garantías en los procedimientos de anonimización de datos personales, 2016, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

Opinion 4/2015 del Supervisor Europeo de Protección de Datos, *Towards a new digital ethics, data, dignity and technology*, de 11 de Septiembre de 2015, https://ec.europa.eu/digital-single-market/en/big-data-value-public-private-partnership

Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, 13 Mayo de 2013 disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

Big Data: Seizing opportunities, preserving values, Executive Office of the President, Mayo 2014, disponible en https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

OECD (2013), working paper "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers, No. 222, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/5k47zw3fcp43-en

OECD (2016), *Perspectivas de la OCDE sobre la economía digital 2015*, Microsoft México, México D.F., pg 283. Disponible en

http://www.oecd.org/sti/ieconomy/DigitalEconomyOutlook2015_SP_WEB.pdf

OECD *La estrategia de innovación de la OCDE. Empezar hoy el mañana* 2010, Organización para la Cooperación y el Desarrollo Económicos (OCDE), París. Es el tercer volumen de un total de siete de la serie Estrategia de Innovación de la OCDE, coeditado con la Organización para la Cooperación y el Desarrollo Económicos. Disponible en castellano en http://www.foroconsultivo.org.mx/libros_editados/estrategia_innovacion_ocde.pdf

Open Data Handbook disponible en http://opendatahandbook.org/guide/es/ Autores: Daniel Dietrich, Jonathan Gray, Tim McNamara, Antti Poikola, Rufus Pollock, Julian Tait, Ton Zijlstra.