El Reglamento General de Protección de Datos (Reglamento 2016/679): aspectos clave

PID_00246865

Joana Marí
Mònica Vilasau

Tiempo mínimo de dedicación recomendado: 6 horas

Universitat Oberta de Catalunya

Índice

Introducción

El Reglamento General de Protección de Datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE, fue publicado en el DOUE del 4 de mayo de 2016 y será plenamente aplicable a partir del 25 de mayo de 2018.

Este texto constituye el marco general de regulación del tratamiento de datos de carácter personal en la Unión Europea. Al tratarse de un Reglamento, esta norma es directamente aplicable y no precisa ni admite transposición por parte de los Estados miembros. Sin embargo, se plantea la cuestión relativa a qué sucede con la legislación existente sobre protección de datos. En el caso español, ello significa principalmente preguntarse acerca del futuro de la LOPD. Si bien esta no puede considerarse derogada por el RGPD, sí que quedaría sin aplicación o desplazada.

De todos modos, es preciso subrayar que el RGPD contiene artículos de diferente naturaleza. Si bien la mayoría de los preceptos son de obligado cumplimiento, existen otros artículos que expresamente dejan a los Estados miembros la potestad para determinar diferentes aspectos. Este es el caso, por ejemplo, de la edad de los menores para consentir el tratamiento de la información personal que les concierne (art. 8.1 RGPD), el hecho de imponer o no sanciones económicas a las AAPP (art. 83.7 RGPD) o el tratamiento de un número nacional de identificación (art. 87 RGPD). De hecho, la legislación nacional constituye el complemento al que se remite en ocasiones el RGPD (considerando 8).

Por otro lado, existen materias excluidas del ámbito de aplicación del Reglamento (art. 2.2 RGPD).

Ante este escenario, el legislador español ha optado por plantear una reforma de la LOPD, que fue presentada el 23 de junio de 2017, tal y como se ha mencionado en el módulo «El nacimiento y la evolución del derecho a la protección de datos» de estos materiales. En la medida en que se trata de un anteproyecto (APLOPD) que sufrirá sin duda alguna muchas modificaciones, en estos materiales se ha optado por hacer solamente algunas referencias a los preceptos del mismo, sin llevar a cabo un análisis exhaustivo de este texto que se halla en un estado embrionario.

A nivel de la Unión Europea, como ya se ha indicado en el módulo «El nacimiento y la evolución del derecho a la protección de datos», junto con esta norma existen otros textos que regulan el tratamiento de la información en

supuestos determinados. Este es el caso, entre otros, de las comunicaciones electrónicas, reguladas por la Directiva 2009/136/CE (objeto de reforma), o el tratamiento de datos por parte de las instituciones y organismos de la UE (Reglamento [CE] n.º 45/2001). También es preciso destacar la existencia de una normativa específica relativa al tratamiento para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales (Directiva 2016/680), y de otra relativa al registro de nombres de pasajeros (PNR), regulados por la Directiva 2016/681.

Reglamento (CE) n.º 45/2001

Se trata del Reglamento (CE) n.º 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. Este reglamento estableció el marco legal de protección de datos a nivel de las instituciones europeas y dispuso la creación del Supervisor Europeo de Protección de Datos, autoridad supervisora independiente a nivel comunitario. El Reglamento General de Protección de Datos mantiene la vigencia del Reglamento 45/2001 (véase art. 2.3 RGPD), si bien, como establece este precepto, se adaptará «a los principios y normas del presente Reglamento de conformidad con su artículo 98».

Directiva 2016/681

Se trata de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Ved también

El tratamiento de datos personales en las comunicaciones electrónicas y las Directivas 2016/680 y 2016/681, serán objeto de estudio en otras asignaturas de este posgrado.

1. Objetivos y características generales

Mònica Vilasau

Los inicios de la reforma de la Directiva 95/46 (DPD en adelante) se remontan a los años 2009 y 2010, con la apertura de consultas acerca de la conveniencia de modificarlo. En enero de 2012 la Comisión presentó la Propuesta de reforma del marco regulador de la protección de datos, que ya incluía una Propuesta de Reglamento y una Propuesta de Directiva. La aprobación del Reglamento 2016/679 y de la Directiva 2016/680, así como las otras disposiciones a las que se ha hecho referencia en la Introducción, comportan que la mayor parte del procesamiento de datos en la UE queda cubierto bajo dicha normativa reguladora.

Sin embargo, existen algunos tratamientos de datos que quedan al margen del RGPD y de las otras Directivas aprobadas en el 2016 sobre tratamiento de información personal.

En la medida en que la seguridad nacional es competencia de cada Estado miembro (art. 4.2 TFUE), el tratamiento de datos relativo a este aspecto queda excluído del ámbito de aplicación del RGPD. Así, dicha norma no resulta aplicable a cuestiones relativas a la seguridad nacional ni tampoco al tratamiento de datos efectuado por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión (considerando 16 RGPD).

1.1. Las razones de una reforma

La reforma de la DPD y la propuesta de un Reglamento que la sustituyera obedecieron a distintos factores.

En primer lugar, los cambios tecnológicos, singularmente el uso generalizado y constante de internet. Si bien en el momento de adoptarse la DPD ya existía internet, el uso que en aquel momento se hacía de la red era aún incipiente. Asimismo, cabe destacar la aparición de nuevas realidades, como pueden ser la internet de las cosas, la generalización de las redes sociales, la computación en la nube, el fenómeno del *big data* o el creciente recurso a la robótica con sofisticados algoritmos que sustituyen la inteligencia humana. Sin embargo, es bastante dudoso que el RGPD pueda dar respuesta a muchos de estos escenarios.

Ved también

Estos nuevos interrogantes que plantean las TIC serán objeto de análisis más detallado en otras asignaturas de este posgrado, como la relativa a «Entornos digitales y nuevos retos para la protección de datos».

El hecho de que el instrumento jurídico adoptado en 1995 fuera una directiva provocó una marcada divergencia normativa entre las legislaciones adoptadas por los Estados miembros. La diferencia en la transposición de la Directiva supuso un sobrecoste para las empresas en la medida en que tenían que adaptarse a las distintas legislaciones nacionales. Un ejemplo paradigmático de esta divergencia lo constituye el régimen sancionador, que en algunos países era

prácticamente inexistente mientras que en otros comportaba la imposición de importantes sanciones económicas, como ocurre, por ejemplo, en el Estado español.

Estas divergencias también han comportado dificultades para las autoridades de protección de datos (AAPD) al tratar de dar respuesta a conflictos que afectaban a distintos Estados con diferentes legislaciones. En ocasiones, resulta complejo determinar qué ley es aplicable o qué autoridad debe intervenir.

Asimismo, la reforma emprendida se incardina en la agenda digital presentada por la Comisión. Se trata de afianzar la confianza en el entorno digital a fin de potenciar y hacer crecer también el comercio electrónico. La finalidad es facilitar un incremento de la competitividad de las empras europeas respecto de otros entornos. Los objetivos son garantizar la seguridad jurídica, simplificar la regulación, eliminar cargas burocráticas, así como establecer reglas claras para las transferencias internacionales de datos.

Web recomendada

Respecto del mercado único digital, puede consultarse: https://ec.europa.eu/digital-single-market/.

1.2. Las características principales de la nueva regulación

En cuanto a las características del RGPD, en primer lugar debe subrayarse, como ya se ha dicho, el hecho de que se trate de un reglamento, lo que implica una novedad en la protección de los derechos fundamentales en la UE. Sin embargo, una crítica que cabe hacer a esta norma es que es excesivamente «reglamentista»[1].

A pesar de tratarse de un reglamento y de su vocación uniformadora, han quedado muchos sectores fuera de su alcance (por ejemplo, el sector regulado por la Directiva 2016/680 o el tratamiento de datos por parte de las instituciones, órganos y organismos de la UE), lo que también es bastante criticable.

Otro de los objetivos de la norma adoptada es que trata de reforzar el papel de las AAPD. De hecho, la regulación de estas, su relación con la Comisión y la búsqueda de un equilibrio entre ellas fue uno de los principales escollos en la negociación del texto definitivo.

Finalmente, otro elemento clave es la adopción de un régimen sancionador, que prevé la imposición de importantes sanciones económicas.

(1)El Reglamento contempla la existencia de actos delegados y actos ejecutivos, y también dispone las remisiones a la regulación por parte de los Estados en determinados preceptos. En cuanto a las características generales de la nueva regulación pueden, consultarse las ponencias de S. Farré y A. Puente, presentadas en la Jornada de 22 de setiembre de 2016, relativa a las principales novedades del RGPD, en el marco del Ciclo de conferencias sobre el nuevo RGPD, organizado por la APDCAT y el ICAB. Véase: http://apdcat.gencat.cat/ca/documentacio/jornades_i_congressos/apdcat/2016/22-setembre/.

2. Ámbito de aplicación

2.1. Ámbito material de aplicación

Joana Marí

Determinar cuál es el ámbito material de aplicación del RGPD exige, en primer lugar, concretar una serie de conceptos que se recogen en su artículo 2.1 y ponerlos en relación con el artículo 1 de la norma. Así, el artículo 2.1 del RGPD establece que el 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».

Por su parte, el artículo 1 señala que tiene por objeto establecer «las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos». Todo ello, con el objetivo de proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, garantizando la libre circulación de los datos personales en la Unión.

Así, este doble objeto –garantía del derecho a la protección de datos y libertad de circulación– determinará el régimen jurídico de garantía del conjunto de los derechos y las libertades de las personas físicas cuando se produzca un tratamiento de datos personales. Este doble objeto ya estaba así regulado en la Directiva 95/46/CE, pero es aún más relevante en la actualidad (y lo será más aún en el futuro), ya que la garantía de la libertad de circulación de los datos personales, en una era en la que los datos son la base del desarrollo social, económico y político, va a marcar muchas de las políticas de la Unión Europea y muchas tienen su fundamento último en la posibilidad de que los datos personales circulen libremente, como puede ser el caso del desarrollo del *cloud computing* o del *big data*. El desarrollo tecnológico y la innovación a partir de su evolución se han convertido en uno de los elementos clave para salir de la coyuntura económica en la que se encuentra Europa; el regulador de la protección de datos en Europa es plenamente consciente de ello, y lo deja plasmado en el considerando 6, en el que indica que:

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

La importancia de no perder esto de vista en la interpretación de la regulación ya se puede ver desde el considerando 2 del RGPD, en el que se recuerda que «pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas».

Vemos, por tanto, que la interpretación de todos los conceptos regulados por el RGPD debe tener siempre como base la garantía del conjunto de derechos y libertades de la personas físicas, teniendo siempre en cuenta que «el tratamiento de datos personales debe estar concebido para servir a la humanidad» (considerando 4) y que, en todo caso, la protección de las personas es el objetivo primordial de la norma.

Como veíamos, el ámbito material de aplicación del RGPD viene recogido en su artículo 2.1, según el cual:

> «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».

Esta regulación no supone ninguna diferencia con la contenida en el artículo 3.1 de la Directiva 95/46/CE.

Para determinar en detalle el ámbito de aplicación material, es necesario analizar los principales conceptos que lo conforman. En concreto, los elementos que marcan la aplicación del RGPD y que deben darse, de forma acumulativa, son estos:

- Dato personal / persona física.
- Tratamiento.
- Fichero.

Veamos, pues, con detalle estos elementos.

2.1.1. Definiciones

Dato de carácter personal

En el artículo 4.1 del RGPD se define **dato personal** como «toda información sobre una persona física identificada o identificable». Y, a su vez, 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».

La definición de lo que debe ser considerado como dato personal no varía mucho de lo que establecía la Directiva 95/46/CE. Pero sí que incluye nuevas referencias, como es el caso de los datos de localización o los identificadores en línea, que nos indican claramente que el regulador es consciente de la nueva situación tecnológica (y por supuesto social) en la que estamos viviendo.

Para delimitar el concepto de dato personal sigue siendo útil el Dictamen 4/2007 sobre el concepto de datos personales (WP 136) del Grupo de Trabajo del Artículo 29, adoptado el 20 de junio. La importancia de delimitar correctamente cuándo nos encontramos ante un dato personal es de suma importancia en un contexto en el que la exponencial evolución de tecnologías emergentes, como el *big data* y la inteligencia artificial, pueden llevarnos a multitud de situaciones en las que una información que en un primer momento no era considerada un dato personal pase a tener esta consideración por la evolución de una tecnología que permite combinar de manera más eficaz la información de la que se dispone.

Grupo de Trabajo del Artículo 29

El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de protección de datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea –que realiza funciones de secretariado. Con el RGPD pasará a ser el Comité Europeo de Protección de Datos (art. 68 del RGPD).

Del análisis realizado por el Grupo del Artículo 29 tres son los elementos clave para poder, en cada caso, concretar cuándo nos encontramos ante datos personales:

- Toda información.
- Identificada o identificable.
- Persona física.

Con la referencia a «toda información» se indica que el concepto que se maneja es amplio y que va a abarcar tanto información objetiva (hechos) como subjetiva (opiniones). Así, en la definición de *dato personal* no va a ser relevante si la información es de carácter sensible, si ha sido hecha pública o a qué

ámbito o faceta de la persona (personal o profesional) afecta, como tampoco va a tener importancia el formato o el soporte en el cual se contenga la información –alfabético, numérico, gráfico, fotográfico, sonoro o, por descontado, en soporte papel. Para el derecho a la protección de datos no hay datos que carezcan de interés ni que sean inocuos.

En cuanto a la mención a «persona física», hemos de tener presente que la normativa de protección de datos solo protege los derechos de las personas físicas, con independencia de su nacionalidad o residencia (así lo reconoce el considerando 2 del RGPD), pero no se aplica a las personas jurídicas ni a las personas fallecidas. Es importante señalar que aunque las personas fallecidas no tengan reconocido el derecho a la protección de datos personales, sí que mantienen otros derechos, como el derecho a la intimidad, al honor y a la propia imagen, regulado por 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. Esta ley indica en su artículo 4 que el ejercicio de las acciones de protección civil de estos derechos queda en manos de la persona que el fallecido haya designado a tal efecto en su testamento. En caso de no existir designación, «estarán legitimados para recabar la protección el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento» (art. 4.2).

Ved también

Véase el apartado «Tratamientos excluidos» de este mismo módulo.

Mayor análisis requiere el concepto de identificable, ya que, como ya se ha indicado, la evolución tecnológica hace que información que en un momento temporal concreto no permita identificar a una persona pueda, por medio de tecnologías mejoradas, llegar a hacerlo. El RGPD se refiere a la identificabilidad de una persona cuando su identidad se pueda determinar, directa o indirectamente, mediante un identificador. Es decir, cuando a partir de la información disponible es posible distinguir a una persona de entre un grupo. Ya hemos señalado que el RGPD menciona una serie de identificadores, como son «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». Pero por supuesto, no es una lista tasada, por lo que cualquier elemento que pueda llevarnos a individualizar a una persona podrá tener esta consideración.

Un caso que generó un enorme debate en su momento fue la consideración o no como dato personal de la dirección IP. Ya en el año 2003, la Agencia Española de Protección de Datos, en su Informe 327/2003, indicaba que:

> «[...] aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos».

En el mismo sentido, el Grupo del Artículo 29, en su Dictamen 4/2007 sobre el concepto de datos personales, se refiere a la dirección IP dinámica indicando que considera las direcciones IP como datos sobre una persona identificable, ya que:

> «[...] los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet».

No obstante, el propio Grupo indica que un caso particular sería «el de algunos tipos de direcciones IP que en determinadas circunstancias y por diversas razones técnicas y organizativas no permiten realmente la identificación del usuario», como sería el caso de las direcciones IP atribuidas a un ordenador instalado en un cibercafé, en el que no se pide identificación alguna a los clientes. En cualquier caso, la evolución de la sociedad hacia el uso de dispositivos móviles nos lleva hacia la plena y constante identificabilidad de los usuarios.

Y, así, en este sentido de prestar atención a la evolución tecnológica, el considerando 26 del RGPD señala que:

> «[...] 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».

Por tanto, las normas del RGPD no serían aplicables a los datos anónimos. Pero debemos tener clara la diferencia de este concepto de datos anónimos con el de **seudonimización**[2], que se refiere a la situación en la que los datos personales se tratan de manera que no puedan atribuirse a una persona concreta sin utilizar información adicional, pero que no pierden por ello su condición de dato personal. Así, la seudonimización es un mecanismo que ayuda a la seguridad de la información pero que no revierte la naturaleza de dato personal, ya que los datos pueden volver a conectarse con una persona individualizada a partir de información adicional, a diferencia de lo que ocurre con los datos anónimos, que no permiten la reidentificación de la persona. En todo caso, para considerar que los datos están seudonimizados, la información adicional debe figurar por separado y estar sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

(2)La definición del concepto de *seudonimización* se puede encontrar en el art. 4.5 del RGPD.

La determinación de si una persona es o no identificable es una cuestión dinámica que debe tener presente el avance tecnológico en el momento del tratamiento y su posible desarrollo durante el periodo en el que es previsible que se traten los datos. Son numerosos los artículos y las investigaciones que muestran la dificultad, cada vez mayor, de mantener los datos anónimos. El Grupo del Artículo 29, en su Dictamen 5/2014 sobre técnicas de anonimización, de

10 de abril, reconoce que «los estudios de caso y las publicaciones científicas muestran la dificultad de crear un conjunto de datos verdaderamente anónimo conservando, sin embargo, toda la información subyacente requerida para la tarea».

Tratamiento

Otra definición importante a los efectos de determinar cuándo nos encontramos sujetos a la aplicación del RGPD es la del concepto de tratamiento, concepto que no es nuevo y que ya existe en la Directiva 95/46/CE en términos muy similares a lo que establece el RGPD, según el cual se entiende por *tratamiento* «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2 del RGPD).

Se añade a esta definición una referencia a la «limitación del tratamiento», definida en el punto siguiente del RGPD como «el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro». Para entender el alcance de esta referencia, hemos de tener presente que el RGPD ha regulado en su artículo 18 el derecho a la limitación del tratamiento. Este derecho otorga al interesado la potestad de obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones reguladas en ese mismo artículo, como por ejemplo que se impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos.

A título de ejemplo, el considerando 67 del RGPD señala que entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio en internet.

En todo caso, cabe recordar que la definición no solo se refiere al tratamiento automatizado de datos, sino que incluye el tratamiento no automatizado de datos (como la actual regulación) y, por tanto, siguiendo lo indicado en el considerando 15 del RGPD, para que el Reglamento sea de aplicación, los datos personales deben estar incluidos en ficheros estructurados conforme a criterios específicos. Por ejemplo, un archivo de expedientes de clientes ordenado alfabéticamente.

Fichero

El concepto de fichero se mantiene y se define en el art. 4.6 del RGPD como «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica». El considerando 27 de la Directiva 95/46/CE añadía que los criterios específicos debían referirse a las personas y permitir acceder fácilmente a los datos personales.

Pese a que se continúa haciendo referencia a este concepto al delimitar el ámbito material de aplicación del RGPD y en la lista de definiciones, no volvemos a encontrar ninguna referencia a él en el resto del articulado, lo que demuestra la tendencia a hablar de tratamientos y operaciones de tratamiento en el momento de determinar las obligaciones y los derechos regulados, incorporando un concepto más amplio vinculado al ciclo de vida de los datos personales.

2.1.2. Tratamientos excluidos

Los tratamientos de datos personales que no quedarán bajo el ámbito de protección del RGPD se encuentran regulados en su artículo 2.2.

Tratamientos del artículo 2.2 del RGPD

1) Tratamientos efectuados en el ejercicio de una actividad no comprendida en el ámbito de aplicación del derecho de la Unión

En aquellos sectores en los que la Unión Europea no tenga competencias, las normas del RGPD no serán de aplicación y, por tanto, deberá, en cada Estado miembro, garantizarse el derecho a la protección de datos personales atendiendo al régimen constitucional establecido. Este sería el caso, por ejemplo, de la seguridad nacional, citado en el considerando 16 del Reglamento.

2) Tratamientos efectuados por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea

En este caso, quedan excluidos los tratamientos de datos personales realizados en el desarrollo de actividades de política exterior y de seguridad común (PESC).

El artículo 21 del Tratado de la UE enumera los objetivos de la PESC, que se centran en el mantenimiento de la paz y el fortalecimiento de la seguridad internacional, el fomento de la cooperación internacional con terceros Estados y el desarrollo y la consolidación de la democracia y el Estado de derecho, así como el respeto de los derechos humanos y las libertades fundamentales.

3) Tratamientos efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas

El considerando 18 del RGPD se refiere a las actividades exclusivamente personales o domésticas como aquellas que no tienen ninguna conexión con una actividad profesional o comercial. Pone además algunos ejemplos, como la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en contextos personales y domésticos.

Sí recuerda el mismo considerando que el Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con esas actividades[3]. Por otra parte, es importante señalar que en determinadas circunstancias se ha considerado que las actividades realizadas en línea por particulares sí entraban dentro del ámbito de aplicación de la normativa de protección de datos. En concreto, tenemos el caso Lindqvist[4], en el que el Tribunal de Justicia de la Unión Europea declaró que los hechos consistentes en publicar en una página web información relativa a diversas personas, identificándolas por su nombre o por otros medios (número de teléfono o información relativa a sus condiciones de trabajo o a sus aficiones), sí constituye un tratamiento de datos personales y no encajaría, por tanto, en la categoría de actividades exclusivamente personales o domésticas, indicando que esta excepción «debe de interpretarse en el sentido que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es este el caso de un tratamiento de datos personales consistente en la difusión de estos datos por Internet de manera que resulten accesibles a un grupo indeterminado de personas». En el caso en concreto, la Sra. Lindqvist, que era catequista, creó una página web para informar a las personas que iban a hacer la confirmación. Pero además, publicó información sobre sus compañeros y su vida personal y familiar.

(3)Dictamen 5/2009 sobre las redes sociales en línea. Adoptado el 12 de junio de 2009.

(4)Sentencia del Tribunal de Justicia en el asunto prejudicial C101/01. Bodil Lindqvist.

Por su parte, la Agencia Española de Protección de Datos en su Informe 0615/2008, en relación con una consulta que planteaba la aplicabilidad de la normativa de protección de datos en el caso de unos padres que compartían fotos de sus hijos realizando actividades extraescolares a través de una página web, señaló que:

> «[...] para que nos hallemos ante la exclusión prevista en el artículo 2 LOPD, lo relevante es que se trate de una actividad propia de una relación personal o familiar, equiparable a la que podría realizarse sin la utilización de Internet, por lo que no lo serán aquellos supuestos en que la publicación se efectúe en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito».

En el ámbito de las redes sociales en línea, el Dictamen 5/2009 del Grupo del Artículo 29 nos recuerda que un gran número de usuarios utilizan las redes en un ámbito puramente personal, poniéndose en contacto con personas que

forman parte de su ámbito personal, familiar o doméstico y que, en estos casos, se considera que se aplica la exención doméstica, y, por tanto, no se aplica la normativa que regula a los responsables del tratamiento de datos. Sin embargo, plantea algunas situaciones en las que no sería aplicable esta exención, por ejemplo cuando la red se utiliza como una plataforma de colaboración para una asociación o una empresa. Así, cuando un usuario actúa en nombre de una empresa o de una asociación, o utiliza la red social como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica. Señala también que un gran número de contactos puede indicar que no se aplica la excepción doméstica y el usuario podría entonces ser considerado como un responsable del tratamiento de datos.

Por su parte, el Tribunal Supremo, en la sentencia número 91/2017 de 15 de febrero, estableció que publicar en un medio de comunicación la fotografía de una persona obtenida de su perfil de Facebook exige de su consentimiento expreso, ya que, en caso contrario, se produce una intromisión ilegítima en su derecho a la propia imagen. Es importante, en este caso, lo indicado por el Tribunal en cuanto a que el hecho de que la persona titular de la imagen la haya hecho pública a través de internet (en un blog, red social, etc.) no conlleva la autorización para hacer uso de esa fotografía y publicarla o divulgarla de una manera distinta, pues no constituye el «consentimiento expreso» que prevé el art. 2.2 de la Ley Orgánica 1/1982.

4) Tratamientos efectuados 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 ámbito debemos remitirnos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión marco 2008/977/JAI del Consejo, publicada el mismo día que el RGPD, pero que, a diferencia de este, exige de una norma de transposición al derecho interno que deberá adoptarse y publicarse, como máximo, el 6 de mayo de 2018.

Esta norma busca garantizar la eficacia de la cooperación judicial y policial en materia penal mediante la creación de un marco uniforme y robusto de protección de los datos personales de las personas físicas, a la vez que se facilita el intercambio de datos personales entre las autoridades competentes de los Estados miembros.

Así, el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, queda excluido del ámbito de aplicación del RGPD y será la norma interna de transposición de la Directiva la que regule esta materia.

El APLOPD, en previsión de que el RGPD entre en vigor y no se haya traspuesto la Directiva (UE) 2016/680, establece en su disposición transitoria quinta que los tratamientos sometidos a dicha Directiva continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al derecho español lo dispuesto en la citada Directiva.

Instituciones, órganos y organismos de la Unión

Las instituciones europeas se rigen, por lo que respecta al tratamiento de datos personales, por el ya mencionado Reglamento (CE) 45/2001[5], que se aplica al tratamiento de datos de carácter personal por parte de las instituciones, los órganos y los organismos de la Unión. Esta norma deberá adaptarse a lo dispuesto en el RGPD con el fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión y permitir que ambos instrumentos puedan aplicarse al mismo tiempo

[5]Reglamento (CE) n.º 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.

El artículo 98 del RGPD, relativo a la revisión de actos jurídicos de la Unión en materia de protección de datos, indica que corresponde a la Comisión presentar las propuestas legislativas pertinentes para modificar los actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar una protección uniforme y coherente de las personas en este ámbito. Además, se hace una mención específica a las normas relativas a la protección de datos personales tratados por parte de las instituciones, órganos y organismos de la Unión.

De hecho, el 10 de enero de 2017, se publicó una Propuesta de reglamento del Parlamento Europeo y del Consejo con esta finalidad. Actualmente, se encuentra en pleno proceso de debate. El propio Supervisor Europeo de Protección de Datos ya ha emitido su informe al respecto mediante la Opinión 5/2017, relativa a la modernización de las reglas sobre protección de datos para las instituciones europeas.

Prestadores de servicios de intermediación

El artículo 2.4 del RGPD señala que el 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 de intermediación establecidas en sus artículos 12 a 15.

En el considerando 14 de la Directiva 2000/31/CE se indica claramente que:

> «La aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet».

El objeto de esta directiva es, además, contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

La mencionada directiva fue transpuesta al ordenamiento español mediante la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Tratamientos excluidos en el APLOPD

En el APLOPD, además de las exclusiones anteriormente indicadas, se añaden dos supuestos de tratamiento de datos que también quedarían excluidos del ámbito de aplicación de la normativa de protección de datos: los tratamientos de datos de personas fallecidas y los tratamientos sometidos a la normativa de materias clasificadas.

1) Tratamiento de datos de personas fallecidas

En el artículo 2.2.d) del APLOPD se indica, expresamente, que a los tratamientos de datos de personas fallecidas no les será de aplicación la ley de protección de datos. Sin embargo, en el artículo 3 del mismo anteproyecto de ley se regula la posibilidad de que determinadas personas ejerzan los derechos de acceso, rectificación o supresión de la persona fallecida. En concreto, establece que:

> «1. Los herederos de una persona fallecida que acrediten debidamente tal condición podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella, y, en su caso, su rectificación o supresión.
>
> Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.
>
> 2. El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese conferido un mandato expreso para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.
>
> Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.
>
> 3. En caso de fallecimiento de menores o personas con discapacidad para las que se hubiesen establecido medidas de apoyo, estas facultades podrán ejercerse, en el marco de sus competencias, por el Ministerio Fiscal».

En Cataluña, además, en relación a los prestadores de servicios digitales, debemos tener en cuenta la Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código civil de Cataluña, que regula las voluntades digitales, a través de las cuales una persona

puede disponer que, después de su muerte, el heredero o el albacea universal o la persona designada para ejecutarlas, actúe ante los prestadores de servicios digitales con quienes el causante tenga cuentas activas para la realización de una serie de acciones entre las que encontramos: comunicar a los prestadores de servicios digitales su defunción, solicitar a los prestadores de servicios digitales que se cancelen sus cuentas activas, solicitar a los prestadores de servicios digitales que ejecuten las cláusulas contractuales o que se activenlas políticas establecidas para los casos de defunción de los titulares de cuentas activas, y, si procede, que le entreguen una copia de los archivos digitales que estén en sus servidores.

2) Tratamiento sometido a la normativa de materias clasificadas

En el artículo 2.2.e) del APLOPD se establece que la ley no será de aplicación a los tratamientos sometidos a la normativa sobre protección de materias clasificadas. Exclusión que ya existe actualmente en el artículo 2.2.b) de la Ley orgánica 15/1999 en términos muy similares:

> «El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: [...] b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas».

Así, debemos remitirnos a la Ley 9/1968, de 5 de abril, sobre secretos oficiales, y a la Ley 48/1978, de 7 de octubre, por la que se modificó esta norma.

Actualmente, está en tramitación una Proposición de Ley de reforma de la Ley 9/1968, en el Congreso.

3) Otros ámbitos

En el apartado 3 del artículo 2 del APLOPD, se indica que los tratamientos incluidos en el ámbito de aplicación de la ley, a los que no sea directamente aplicable el RGPD, se regirán por lo dispuesto en su legislación específica, si la hubiere, y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica.

Se hace una mención específica al tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, que se regirán por lo dispuesto en el RGPD y por la Ley orgánica de protección de datos, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

2.2. Ámbito territorial de aplicación

Determinar cuándo es o no aplicable el RGPD va a ser imprescindible en un contexto de globalización de los tratamientos y auge de tecnologías como el *big data*, la internet de las cosas o el *cloud computing*. Solo a partir de una con-

creción clara de cuándo se aplica esta norma se lograrán los objetivos de garantizar la seguridad jurídica a los responsables del tratamiento y de dotar de un marco jurídico claro a las personas.

Y, para analizar el ámbito territorial, la regulación del artículo 3 del RGPD nos exige diferenciar entre los tratamientos de datos realizados en el seno de la Unión Europea y aquellos que, pese a realizarse fuera del territorio de la Unión, inciden en las personas que residen en ella.

2.2.1. Aplicación en el territorio de la Unión Europea

En el primer caso, el artículo 3.1 del RGPD establece que las normas de protección de datos personales se aplicarán a aquellas entidades que traten datos personales (sea el responsable del tratamiento, sea el encargado del tratamiento) y tengan un establecimiento en la Unión, con independencia de que el tratamiento se realice en la Unión o no.

> «**Artículo 3.1.**
>
> El presente Reglamento se aplica al tratamiento de datos 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».

Por tanto, va a ser el concepto de la ubicación de un establecimiento en el territorio de la Unión el que delimite, en primer lugar, la aplicabilidad del Reglamento. Para determinar cuándo nos encontramos ante un «establecimiento» a efectos del RGPD, nos ayuda el considerando 22 del RGPD, en el que se indica que un establecimiento «implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables», con independencia de cuál sea la forma jurídica que revistan tales modalidades (sucursal, filial, etc.).

Cuestión diferente, que se deja aquí solo señalada, es la noción de establecimiento principal, definida en el artículo 4. 16) del RGPD, que servirá a los efectos de determinar la autoridad de control competente en el caso de tratamientos transfronterizos de datos. No olvidemos que en la búsqueda de la seguridad jurídica y de un marco coherente de protección de datos, el Reglamento, norma de aplicación directa en el conjunto de la Unión, ha regulado el denominado mecanismo de *one-stop-shop* para facilitar la aplicación de la normativa de protección de datos y el ejercicio de los derechos de los interesados, así como mejorar el control por parte de las autoridades de protección de datos.

«**Art. 4. 16)**

"establecimiento principal": a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento».

2.2.2. Asunto Google Spain

Merece una mención especial, en este contexto, el asunto Google Spain[6], ya que, pese a referirse al ámbito de aplicación de la Directiva 95/46/CE y centrar su interpretación en la noción de establecimiento, sirve como claro ejemplo de la voluntad de proteger los derechos de las personas en lo que afecta al tratamiento de sus datos personales con independencia del lugar en el que se esté ejecutando el tratamiento efectivo de estos.

(6)Sentencia del Tribunal de Justicia de la Unión Europea. Asunto C-131/12 (Google Spain, S. L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González) de 13 de mayo de 2014.

Pese a que esta sentencia del Tribunal de Justicia de la Unión Europea suele ser más conocida por el reconocimiento de la obligación del gestor de un motor de búsqueda de eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web cuando se den determinadas circunstancias, también es significativa en relación con la interpretación del ámbito territorial de las normas de protección de datos.

Sobre la primera cuestión prejudicial, letras a) a d), relativas al ámbito de aplicación territorial de la Directiva 95/46/CE, el Tribunal recuerda que el objetivo de la Directiva es garantizar una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas y que el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se eludiera esta protección. Para ello, estableció un ámbito de aplicación territorial particularmente extenso. A partir de esta afirmación, el Tribunal llega a la conclusión de que:

«[...] el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa "en el marco de las actividades" de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor. [...] las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, 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. [...] la propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos. Pues bien, toda vez que dicha presentación de resultados está acompañada, en la misma página, de la presentación de publicidad vinculada a los términos de búsqueda, es obligado declarar que el tratamiento de datos personales controvertido se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro, en el caso de autos el territorio español».

Epígrafes 55 a 57 de la sentencia del Tribunal de Justicia de la Unión Europea. Asunto C-131/12.

Esta interpretación extensiva del concepto de establecimiento se ha visto reiterada con posterioridad en el asunto Weltimmo s. r. o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság[7]. En este caso, las cuestiones prejudiciales se derivan de un litigio entre la autoridad húngara de protección de datos y una empresa que gestiona una página web de intermediación inmobiliaria registrada en Eslovaquia en la que se anuncian inmuebles ubicados en Hungría. En esta sentencia se recuerda que la noción de establecimiento es flexible y que no tiene un sentido puramente formal, y que el concepto de establecimiento en el sentido de la Directiva 95/46/CE se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable (en el caso analizado, la actividad ejercida por Weltimmo consiste en la gestión de uno o varios sitios de internet de anuncios de inmuebles situados en Hungría, que están redactados en húngaro y que pasan a ser de pago transcurrido el primer mes).

(7)Sentencia TJUE. Asunto C-230/14 (Weltimmo s. r. o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság), de 1 de octubre de 2015.

Cabe resaltar la apreciación hecha por el Tribunal en el epígrafe 34 de esta sentencia, relativa a la necesidad de tener en cuenta el modelo de negocio en cuanto a ser una empresa que opera exclusivamente a través de internet, por lo que no requiere una instalación física permanente.

2.2.3. Aplicación fuera de la Unión Europea

Derivando directamente de lo anteriormente apuntado y atendiendo a la globalización de los tratamientos de datos personales, se ha hecho necesario establecer un régimen territorial extensivo de garantía del derecho a la protección de datos.

Así, el artículo 3.2 del RGPD establece que sus normas serán aplicables 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:

- La oferta de bienes o servicios a dichos interesados en la Unión, tanto si son remunerados como si no.
- El control de su comportamiento, en la medida en que este tenga lugar en la Unión.

El Reglamento busca garantizar plena y eficazmente los derechos de las personas que residan en la Unión y para ello extiende su aplicación a los dos supuestos indicados.

Oferta de bienes y servicios

En primer lugar, se refiere a los responsables y encargados que, pese a no estar establecidos en la Unión, traten datos en el contexto de la oferta de bienes y servicios independientemente de que medie pago.

En el considerando 23 del Reglamento se indica que para determinar si estamos ante una oferta de bienes o servicios a interesados que residan en la Unión, debe valorarse 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.

Hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados, o la mención de clientes o usuarios que residen en la Unión, que pueden dar indicios para determinar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión. Aunque también se señala que la mera posibilidad de acceder al 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 basta para determinar dicha intención.

Estas consideraciones se recogían ya en la sentencia del Tribunal de Justicia (Gran Sala) de 7 de diciembre de 2010, Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG (C-585/08) y Hotel Alpenhof GesmbH contra Oliver Heller (C-144/09), que no siendo relativa al tratamiento de datos personales sí ofrece una serie de elementos útiles para determinar si nos encontramos ante una oferta de bienes y servicios dirigida a interesados en la Unión. En concreto, la sentencia indica que, en primer lugar, debe comprobarse si antes de la celebración del contrato con el consumidor de las citadas páginas web y de la actividad global del vendedor, se desprendía que este último tenía intención de comerciar con consumidores domiciliados en otro u otros Estados miembros, entre ellos el del domicilio del consumidor, en el sentido de que estaba dispuesto a celebrar un contrato con ellos.

Y añade una lista de elementos que ofrecen indicios para determinar el hecho analizado:

- El carácter internacional de la actividad.
- La descripción de itinerarios desde otros Estados miembros al lugar en el que está establecido el vendedor.
- La utilización de una lengua o de una divisa distintas de la lengua o la divisa habitualmente empleadas en el Estado miembro en el que está establecido el vendedor, con la posibilidad de reservar y de confirmar la reserva en esa otra lengua.
- La mención de números de teléfono con indicación de un prefijo internacional.
- Los gastos en un servicio de remisión a páginas web en internet con el fin de facilitar el acceso al sitio del vendedor o al de su intermediario a consumidores domiciliados en otros Estados miembros.
- La utilización de un nombre de dominio de primer nivel distinto al del Estado miembro en el que está establecido el vendedor.
- La mención de una clientela internacional formada por clientes domiciliados en diferentes Estados miembros.

Vemos, por tanto, que el análisis del caso concreto será muy importante para delimitar la aplicabilidad del RGPD. En este sentido, la aplicación de criterios de responsabilidad proactiva y de protección de datos en el diseño por parte del responsable en el momento de definir la oferta será muy importante para garantizar una protección eficaz de los derechos de los interesados.

Control del comportamiento

En segundo lugar, se refiere a tratamientos destinados al control del comportamiento de las personas, en la medida en que este comportamiento tenga lugar en el territorio de la Unión.

En el considerando 24 se señala que para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas son objeto de un seguimiento en internet. En este caso, se incluye 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.

Será necesario que se determine con claridad cuándo nos vamos a encontrar con situaciones de control del comportamiento y recordar, en todo caso, que deberá tenerse siempre en cuenta que el objetivo del RGPD es garantizar el derecho de las personas a no ver limitados sus derechos y libertades, aspecto esencial en el caso de la toma de decisiones basadas en el análisis del comportamientos.

Un ejemplo de esas situaciones lo encontramos en la publicidad comportamental, definida por el Grupo del Artículo 29[8] como aquella publicidad que «implica la identificación de los usuarios que navegan por internet y la crea-

(8)Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010.

ción gradual de perfiles que después sirven para enviarles publicidad que corresponde a sus intereses». Pero las tecnologías emergentes nos regalan numerosos ejemplos de este tipo de situaciones, ya que el análisis de datos masivos (*big data* unido a inteligencia artificial y *machine learning*) tiene como objetivo básico encontrar correlaciones entre datos para poder, a partir de ellas, adoptar decisiones que, en muchos casos, afectarán significativamente a las personas en ámbitos muy diversos: de salud, educativo, financiero, laboral, por solo mencionar algunos.

El responsable o el encargado del tratamiento no establecido en la Unión Europea que esté tratando datos personales de personas residentes en la Unión y cuyas actividades de tratamiento se refieran a la oferta de bienes o servicios a dichos interesados en la Unión, o tengan que ver con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante (art. 27 del RGPD).

No será de aplicación la obligación de nombrar a un representante cuando el tratamiento sea ocasional, no se traten categorías especiales de datos a gran escala o datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, el contexto, el alcance y los objetivos del tratamiento [art. 27.2 a) del RGPD].

2.2.4. Incidencia del derecho internacional público

En el artículo 3.3 del RGPD se indica que «se aplica 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».

Este apartado se refiere a aquellas situaciones en las que, a partir de la regulación hecha por el derecho internacional público, se generan situaciones en las que el derecho del Estado miembro se aplica fuera de sus fronteras. Por ejemplo, en el caso de los tratamientos de datos realizados por embajadas o consulados, buques o aeronaves.

3. Principios de protección de datos: artículo 5 RGPD

Mònica Vilasau

El artículo 5 RGPD, que da inicio al capítulo II de dicho texto legal, bajo la rúbrica «Principios relativos al tratamiento», recoge cuáles son los principios de protección de datos, atribuyendo un nombre a cada uno de ellos. Con ello se facilita su identificación puesto que no existía antes unanimidad en la doctrina a la hora de enunciarlos.

De entrada, conviene señalar que no existen grandes cambios entre los principios recogidos en el RGPD y los reconocidos en la DPD y en la propia LOPD.

> Paul De Hert y Vagelis Papakonstantinou ponen de relieve la línea continuista del RGPD en cuanto a los principios, y señalan como únicos cambios la introducción de los principios de transparencia y de responsabilidad. También señalan el otorgamiento de un estatus especial para la finalidad de investigación, que estaría ligado al principio de limitación de la finalidad. Véase:
>
> **P. De Hert; V. Papakonstantinou** (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 179-194).
>
> Otros autores señalan que el RGPD no aporta grandes novedades en cuanto a los principios. Véase:
>
> **J. Puyol Montero** (2016). «Los Principios del derecho a la protección de datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 135-150). Madrid: Ed. Reus.

En definitiva, como señalan De Hert y Papakonstantinou:

> «[...] the basic principles for the lawful processing of personal data as were known for the past twenty years remain more or less the same, having demonstrated the necessary resilience and flexibility in order to survive an increasingly complex data processing environment».
>
> P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, pág. 186).

Constituye una novedad la introducción del principio de responsabilidad proactiva (art. 5.2 RGPD). Asimismo, también cabe destacar la nueva orientación que se ha dado a la seguridad de la información, adoptando un enfoque de responsabilidad por riesgo, que bien puede configurarse como un principio transversal a todo tratamiento de la información.

El artículo 5 RGPD lleva por rúbrica (las cursivas son nuestras) «Principios relativos al *tratamiento*», a diferencia de la Directiva, cuya sección I (dentro del capítulo II, dedicado a «Condiciones generales para la licitud del tratamiento de datos personales») se dedicaba a «Principios relativos a la *calidad* de los datos», que se desarrollaban en el artículo 6 DPD. La Directiva reconducía

todos los principios de protección de datos al principio de calidad, mientras que el RGPD separa y trata de manera independiente cada uno de los distintos principios.

Los principios recogidos en el artículo 5 RGPD constituyen auténticos principios que afectan no solo al responsable del tratamiento (RT), sino a todos aquellos que intervienen en él. Se trata, además, de una pauta normativa e interpretativa para todas las instituciones jurídicas donde se lleve a cabo un tratamiento de datos.

A continuación se analizan estos principios recogidos en el artículo 5 RGPD.

Referencia bibliográfica

J. Puyol Montero (2016). «Los Principios del derecho a la protección de datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 135-150). Madrid: Ed. Reus.

3.1. Principio de «licitud, lealtad y transparencia»

Según dispone el artículo 5.1.a) RGPD, los datos personales serán «a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia")».

Tal y como se determina en el considerando 39:

> «Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro [...]».

Licitud, lealtad y transparencia están muy interconectados, especialmente los dos últimos. Debe informarse especialmente acerca de la identidad del responsable del tratamiento y de los fines de este, en definitiva, qué se hará con los datos. Además, el principio de transparencia está ligado al ejercicio de todos los derechos.

La exigencia de licitud, lealtad y transparencia no representa una gran innovación ni separarse de las previsiones de la DPD ni de la propia LOPD. De hecho, el artículo 4 LOPD, al recoger el que se conocía como principio de calidad de los datos, prohibía la recogida de los datos mediante medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD).

El principio de transparencia tampoco es nuevo y también se halla recogido en la LOPD. Sin embargo, en esta última no se formula propiamente como un principio sino como una obligación del responsable del tratamiento (art. 5 LOPD). En el texto del RGPD se trata la transparencia como un principio y más adelante, en su articulado, como un derecho. Es preciso recordar, además, que según el TC la transparencia representa un presupuesto del ejercicio de los otros derechos.

Deber de informar

Más concretamente, en cuanto al contenido del deber de informar, véase el considerando 60 RGPD (las cursivas son nuestras):

«Los principios de tratamiento *leal y transparente* exigen que se *informe al interesado* de la *existencia de la operación de tratamiento y sus fines*. 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. Si los datos personales se *obtienen de los interesados*, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha *información puede transmitirse en combinación con unos iconos normalizados* que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente».

El principio de licitud se encuentra desarrollado en el artículo 6 RGPD. En cuanto a la licitud, el considerando 40 del RGPD dispone que:

«Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato».

El artículo 6 RGPD, al desarrollar qué se entiende por *licitud*, regula los supuestos que habilitan, que permiten, el tratamiento de datos. El tratamiento de datos personales, en el marco de la UE, y a diferencia de otros ordenamientos jurídicos como es el caso del de Estados Unidos, no es un *free lunch* que permita tratar los datos sin más. Para hacerlo, es preciso que se cumplan unas bases legales o supuestos de habilitación.

En cuanto a los supuestos de habilitación, el RGPD adopta una sistemática muy parecida a la DPD y expone cuáles son los supuestos habilitadores. La legislación española recogió el principio de licitud bajo la rúbrica «Principio del consentimiento» en el artículo 6 LOPD. Sin embargo, en este precepto además del consentimiento se regulan los otros supuestos que habilitan el tratamiento de los datos de carácter personal.

Supuestos de habilitación

Los artículos 11 y 21 LOPD contemplan supuestos concretos de habilitación. El artículo 11 LOPD respecto de la cesión de datos y el artículo 21 LOPD en relación a la comunicación de datos entre administraciones. En cambio, el RGPD no proporciona una regulación específica de la comunicación de datos y tampoco incluye una definición de dicho término. La DPD tampoco define qué se entiende por *comunicación*, lo que sí hace en cambio el artículo 3.i) LOPD. Por el contrario, el RGPD sí que incluye dentro de la relación de definiciones la relativa a *destinatario de una comunicación* (art. 4.9 RGPD) y debe subrayarse que se entiende por *destinatario* tanto la persona física como un servicio.

En cuanto a la licitud de los datos, tampoco existen novedades relevantes y en todo caso el artículo 6 RGPD será analizado con más detenimiento más adelante.

3.2. Principio de «limitación de la finalidad»

El artículo 5.1 RGPD dispone que los datos personales serán «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")».

En cuanto a la limitación de la finalidad, es importante tener en cuenta lo que dispone el considerando 50:

«El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles».

El artículo 89 RGPD, cuya rúbrica es «Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos», dispone que:

«1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos 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».

Este precepto es muy similar al artículo 6.1.b) DPD, que establece que los Estados miembros dispondrán que los datos personales sean «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».

En definitiva, la única diferencia relevante entre el RGPD y la DPD es que el primero añade que no será incompatible el tratamiento ulterior de los datos personales con «fines de archivo en interés público». Este último supuesto no se contempla ni por el artículo 4.2 LOPD ni por el artículo 6.1.b DPD. La cuestión es determinar qué debe entenderse por «archivo en interés público». ¿Se trata solo de un archivo público? O ¿también puede comprender un archivo privado pero de interés público?

Parece claro que quedan comprendidos los archivos que tienen cabida dentro de la Ley de Patrimonio Nacional y dentro de las correspondientes leyes de archivos de las comunidades autónomas. Sin embargo, parece que también deberían incluirse aquellos archivos privados de interés público.

Archivos privados de interés público

En este sentido, se pronuncia S. Farré en su intervención realizada en el Ciclo de conferencias sobre el nuevo RGPD. Concretamente, se trata de la Jornada que tuvo lugar el día 27 de octubre de 2016, bajo el título: «El nou Reglament general de protecció de dades: revisió dels principis en un entorn sense fronteres». Véase: http://apdcat.gencat.cat/ca/actualitat/noticies/noticia/Jornada-El-nou-Reglament-general-de-proteccio-de-dades-revisio-dels-principis-en-un-entorn-sense-fronteres.

El precepto en cuestión se remite al artículo 89 RGPD («Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos»), al regular el uso de los datos. Se dice que será preciso la adopción de medidas adecuadas.

Es necesario subrayar que el principio de limitación de la finalidad del artículo 5.1.b) RGPD queda de algún modo relativizado en el artículo 6.4 del mismo texto. Este último precepto admite, en determinados supuestos, destinar los datos a una finalidad distinta de aquella inicialmente prevista. En este caso, será el responsable del tratamiento quien deberá valorar si el uso de los datos para otra finalidad es compatible o no.

Ved también

Este supuesto (art. 6.4 RGPD) será analizado con más detalle en el apartado «Bases legales que permiten el tratamiento de datos de carácter personal: artículo 6 RGPD».

¿Cómo valorará el RT si el cambio de finalidad es posible o no? El parámetro y criterio lo proporciona el artículo 6.4 RGPD. Sin duda, ello supone abrir la puerta a un terreno que generará dudas tanto al RT como a las AAPD.

En cuanto a la «relajación del principio de finalidad», De Hert y Papakonstantinou señalan que:

«The fact remains, however, that further processing is indeed permitted under the Regulation, and it is up to the controller, according to the principle of accountability, to make the necessary evaluations as to whether the new, further processing, purposes are compatible with, and therefore permitted, the initials or not».

P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 179-194).

En cuanto al supuesto de que se produzca un cambio de finalidad, debe tenerse también en cuenta el artículo 23.2 RGPD (relativo a las limitaciones).

3.3. Principio de «minimización de los datos»

Dispone el artículo 5.1. RGPD que los datos personales serán «c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos")».

Ello comporta que, al llevar a cabo un tratamiento, deba en primer lugar valorarse si efectivamente es preciso tratar datos personales. En caso de que deban tratarse, dicho tratamiento debe ser aquel imprescindible para la finalidad que se quiere alcanzar.

El principio de minimización tampoco supone en rigor un nuevo principio. Ya la LOPD establece que los datos podrán ser tratados cuando sean adecuados, pertinentes y no excesivos en relación con la finalidad (art. 4 LOPD). Esto es, el tratamiento deberá ser proporcional a la finalidad. El artículo 6.2 c) DPD señala: «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente».

Respecto al principio de minimización, es importante tener en cuenta el concepto de seudonimización. Según se determina en el artículo 4.5) RGPD, se entiende por *seudonimización*:

> «[...] 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 destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable».

La seudonimización, un nuevo concepto introducido en el RGPD, constituye un mecanismo que permite tratar datos que se incluyen dentro de la categoría de datos de carácter personal (por lo que son efectivamente datos de carácter personal). Sin embargo, al atribuirles un código, ello permite que los terceros no tengan acceso directo a los datos identificativos y de este modo se pueda minimizar el riesgo de su tratamiento. Por lo tanto, el hecho de recurrir a esta técnica puede potenciar y facilitar que solo se traten aquellos datos necesarios.

Asimismo, el principio de minimización debe relacionarse con el de conservación de los datos. De modo que se reconoce una limitación del plazo de conservación de los datos.

Lógicamente, también existen excepciones a esta necesidad de establecer un límite a la conservación de los datos, como el supuesto anteriormente indicado de conservación para una finalidad de archivo en interés público.

En relación con el plazo de conservación de los datos, debe tenerse en cuenta la exigencia del RGPD en relación al contenido de las cláusulas informativas. Debe informarse del plazo durante el que se conservarán los datos. Si no es posible fijar un plazo, sí al menos establecer los criterios que permitirán determinar el plazo de conservación. No obstante, en muchas ocasiones no será fácil dar cumplimiento a esta exigencia, en la medida en que el propio RT puede desconocerlo al iniciar el tratamiento –véanse los artículos 13.2.a) y 14.2.a) RGPD.

Nota

En cuanto a la conservación de los datos, la Directiva 2006/24, de 15 de marzo de 2006, reguló expresamente 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. Esta Directiva, declarada inválida en el caso Digital Rights Ireland, STJUE de 8 de abril de 2014 ([Gran Sala], asuntos acumulados C-293/12 y C-594/12], fue traspuesta al ordenamiento jurídico español mediante la Ley 25/2007, de 18 de octubre. Esta norma no ha sido derogada ni anulada.

3.4. Principio de «exactitud»

Determina el artículo 5.1 que los datos personales serán «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")».

Los datos deben ser exactos y estar actualizados. De otro modo, deben rectificarse o suprimirse. Ello también está relacionado con el deber del RT de comunicar a los destinatarios de los datos que estos han sido rectificados/eliminados. Así lo establece el artículo 19 RGPD en relación con el ejercicio del derecho de supresión (regulado en el art. 17 RGPD).

Derecho de supresión

El artículo 17 RGPD lleva por rúbrica «Derecho de supresión ("el derecho al olvido")». La regulación del derecho al olvido en la versión final del RGPD quedó un tanto diluida respecto de la propuesta de la Comisión, y finalmente se trata de supuestos de supresión de los datos, como efectivamente recoge la rúbrica del artículo 17 RGPD.

En relación con el principio de exactitud, la corrección y actualización de oficio de los datos puede plantear en algunos casos problemas con la constatación y acreditación del consentimiento del titular de los datos.

Referencia bibliográfica

J. Puyol Montero (2016). «Los Principios del derecho a la protección de datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 135-150). Madrid: Ed. Reus.

3.5. Principio de «limitación del plazo de conservación»

Dispone el artículo 5.1 RGPD que los datos personales serán «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 periodos 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")».

Debe tenerse en cuenta lo que se ha dicho respecto al principio de minimización de los datos, al hacerse referencia al plazo de conservación de los datos. Concretamente, en las cláusulas informativas deberá informarse del plazo en el que se piensa conservar los datos y, de no ser posible fijar un plazo, al menos establecer los criterios que permitirán determinar dicho plazo [arts. 13.2.a) y 14.2.a) RGPD].

Nota

En cuanto a la conservación y retención de los datos, véase la nota sobre la Directiva 2006/24 en el apartado «Principio de "minimización de los datos"».

3.6. Principio de «integridad y confidencialidad»

Determina el artículo 5.1 RGPD que los datos personales serán «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")».

Otra de las novedades que introduce el RGPD es el enfoque del riesgo. En consecuencia, las medidas que se adopten para hacer frente a los posibles riesgos deberán tener en cuenta la naturaleza, el contexto y las finalidades del tratamiento, así como el riesgo que dicho tratamiento pueda comportar para los derechos y las libertades de las personas.

El principio de integridad y confidencialidad supone una concreción de los artículos 9 (principio de seguridad) y 10 (deber de confidencialidad) de la LOPD. Si bien el RGPD utiliza los términos de «integridad y seguridad», se trata del principio de seguridad revisado.

En definitiva, debe garantizarse mediante medidas técnicas u organizativas una seguridad adecuada contra el tratamiento no autorizado o ilícito, la pérdida, la destrucción o el daño accidental.

El contenido es casi el mismo que el del artículo 9 LOPD. Se trata, en definitiva, de garantizar una seguridad adecuada respecto de la pérdida de información o de un daño en la información. Lo que es más novedoso no son los deberes de seguridad, sino los instrumentos para hacerla efectiva. Se trata principalmente de tres:

- Evaluación de los riesgos que deben afrontarse al iniciar un tratamiento.
- Implementación de medidas técnicas y organizativas adecuadas.
- Notificación de las violaciones de seguridad.

La implementación de las medidas técnicas y organizativas, o incluso de las medidas de seguridad, es responsabilidad del RT, que deberá adoptar las que sean más idóneas y necesarias una vez realizada una evaluación de los riesgos a que está sujeto el tratamiento de la información. En particular, para ello se tendrá en cuenta la tipología de los datos, las finalidades y otras circunstancias que rodean el tratamiento.

3.7. Principio de «responsabilidad proactiva»

El artículo 5.2. RGPD dispone que «El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (“responsabilidad proactiva”)».

El artículo 6.2 DPD ya dispone que «Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1».

Por lo tanto, la novedad que introduce el RGPD es la parte final del artículo 5.2, esto es, «capaz de demostrarlo». Este principio es el que se conoce como *accountability* en el mundo anglosajón y que puede traducirse como ‘responsabilidad proactiva’.

Sobre la base de esta responsabilidad proactiva, las organizaciones deben ser conscientes de qué información tratan y con qué finalidad llevan a cabo el tratamiento, y tienen que planificar y diseñar cómo cumplirán las normas contenidas en el RGPD. Además, deberán poder acreditar, cuando se les exija, que cumplen adecuadamente con la normativa.

Se trata de una responsabilidad demostrable. El enfoque de la LOPD (y de la DPD) puede calificarse como de reactivo. De modo que si sucede algo, el RT debe responder.

La aproximación del RGPD añade a esta aproximación reactiva una proactiva. Establece sobre el RT la carga de adoptar determinadas medidas y estar en condiciones de poderlo demostrar. Se trata, en definitiva, de rendir cuentas de cómo se efectúa el tratamiento. Para ello, puede dotarse de las herramientas que están contempladas en el capítulo IV RGPD: la adopción de una política de protección de datos, el registro de operaciones de tratamiento, la protección de datos desde el diseño y la protección de datos por defecto, el establecimiento y reconocimiento de códigos de conducta, certificaciones y sellos, así como la evaluación del impacto sobre la protección de datos. También se incluyen dentro de estas medidas preventivas la necesidad de formalizar una consulta previa, los criterios y la diligencia al designar un encargado del tratamiento (ET) y un delegado de protección de datos (DPD), y, singularmente, la adopción de medidas de seguridad. Asimismo, dentro de este concepto de seguridad amplio, se incluye el deber de notificar las violaciones de seguridad. Otro aspecto que supone acreditar que se adopta una postura diligente es que dichas medidas deben revisarse y actualizarse periódicamente.

En definitiva, se trata de una batería de instrumentos para hacer efectiva la responsabilidad. Esta responsabilidad requiere una actitud consciente, diligente y proactiva por parte del RT. Si bien se trata de un principio de protección de datos, las obligaciones recogidas en el capítulo IV constituyen auténticas obligaciones que deben ser aplicadas a lo largo del tratamiento.

Finalmente, y como conclusión una vez expuestos cuáles son los principios de protección de datos, debe subrayarse que algunos de ellos difícilmente serán aplicables a nuevas realidades, concretamente a fenómenos como el *big data*. En el caso del tratamiento y análisis masivo de datos, se ponen en entredicho precisamente algunos de los principios que constituyen el núcleo de la normativa de protección de datos y del tratamiento de la información personal que han sido expuestos.

Especialmente se ponen en cuestión principios como el de «licitud, lealtad y transparencia» y, más en concreto, este último, en la medida en que no se podrá informar (por desconocimiento en muchas ocasiones), por ejemplo, ni de la finalidad del tratamiento ni del plazo durante el cual se conservarán los datos.

Otro principio que queda claramente amenazado por la propia naturaleza del tratamiento masivo de datos es el principio de «limitación de la finalidad», y ello porque en el momento de recopilarse los datos, la filosofía del *big data* es la de recabar cuantos más datos mejor, porque no se sabe qué correlaciones se podrán descubrir dentro del conjunto de información recabada. Por ello se hace difícil, si no imposible, determinar de entrada la finalidad del tratamiento. En estrecha relación con esto, el principio de «minimización de los datos» también resulta incluso antagónico con la propia naturaleza del *big data* porque se trata, una vez más, de recoger cuantos más datos mejor.

Por último, en cuanto a la «limitación del plazo de conservación», si ya en muchos de los tratamientos de datos puede que se desconozca durante cuánto tiempo se conservarán los datos, ello es aún más acentuado en el caso del *big data*. Si no se sabe muy bien a qué finalidad (finalidades) se destinarán los datos, aún será más difícil determinar durante cuánto tiempo se conservarán.

Ved también

Estos aspectos serán analizados con detenimiento en otra de las asignaturas de este posgrado, concretamente en la relativa a «Entornos digitales y nuevos retos para la protección de datos».

4. Bases legales que permiten el tratamiento de datos de carácter personal: artículo 6 RGPD

Mònica Vilasau

El artículo 5.1.a) RGPD determina que el tratamiento debe ser lícito, requisito que viene desarrollado en el artículo 6 del RGPD. En este precepto se recogen los supuestos que permiten (habilitan) un tratamiento de datos, de tal manera que si no existe alguna de estas habilitaciones, el tratamiento no sería lícito y no podría llevarse a cabo. Este es el esquema que ya se estableció en el artículo 7.1 DPD, que determinaba que (las cursivas son nuestras): «los Estados miembros dispondrán que el tratamiento de datos personales *solo* pueda efectuarse *si* [...]».

Por lo tanto, la posibilidad de llevar a cabo un tratamiento de datos es vista como algo residual, si bien son tantas las excepciones que en la práctica es difícil que un supuesto de tratamiento de datos no halle cabida dentro de alguna de las excepciones que permite el tratamiento.

El RGPD sigue el mismo patrón que la DPD, de modo que según dispone el artículo 6.1 RGPD (las cursivas son nuestras): «El tratamiento *solo será lícito si* se cumple al menos una de las siguientes condiciones [...]».

Sí se produce un cambio entre la DPD y el RGPD respecto a la terminología utilizada, de modo que la DPD, en su sección II, dentro del capítulo II, dedicada a este aspecto, lleva por rúbrica «Principios relativos a la legitimación del tratamiento de datos», mientras que en el RGPD el artículo 6 lleva por rúbrica «Licitud del tratamiento».

Concretamente, el artículo 6 RGPD dispone que:

> «1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
>
> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
>
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
>
> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

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

En cuanto al artículo 6 RGPD, lo más importante es dejar claro que sin la concurrencia de uno de los supuestos contemplados en el precepto no es posible llevar a cabo un tratamiento[9]. Si bien es cierto, como ya se ha subrayado, que el abanico de supuestos es amplio y quedarán pocos casos fuera de una habilitación legal, debe subrayarse la necesidad de que exista una base legal.

(9)Así lo subrayan, entre otros autores: Boulanger, Poullet *et al.* («La protection des données à caractère personnel en droit communautaire: deuxième partie», 1997); Heredero Higueras (*La directiva comunitaria de protección de los datos de carácter personal*, 1997, págs. 110-111), y Lynskey (*The foundations of EU data protection law*, 2015, págs. 30-35).

Asimismo, el hecho de que concurra una base legal *ex* artículo 6 RGPD no es suficiente por sí mismo para poder tratar los datos, de manera que también deben cumplirse necesariamente los principios de protección de datos *ex* artículo 5 RGPD.

La vinculación entre los principios de protección de datos y los mecanismos de legitimación (supuestos que permiten tratar los datos) se constata en la medida en que el artículo 5 RGPD se remite al artículo 6 RGPD. Efectivamente, el artículo 5.1.a) RGPD, en la medida en que establece que el tratamiento debe ser lícito, se remite al artículo 6 RGPD, cuya rúbrica precisamente es la «Licitud del tratamiento».

Esta conexión entre principios y bases legales ya fue puesta de relieve por Poullet y otros autores en uno de los primeros comentarios que se llevaron a cabo al texto de la DPD en el año 1997. Por lo tanto, para que se pueda llevar a cabo un tratamiento, ello comporta que deben cumplirse cumulativamente los artículos 5 y 6 RGPD. De Hert y Papakonstantinou ponen de relieve esta conexión, si bien también señalan que hubiera sido deseable que en el texto del RGPD fuera más evidente.

Referencias bibliográficas

M.-H. Boulanger; Y. Poullet y otros (1997). «La protection des données à caractère personnel en droit communautaire: deuxième partie». *Journal des Tribunaux - Droit Européen* (núm. 41, pág. 148).

En el mismo sentido se pronuncian, entre otros:

M. Heredero Higueras (1997). *La directiva comunitaria de protección de los datos de carácter personal*. Bilbao: Aranzadi, Elcano (págs. 109-110).

R. Gellert; S. Gutwirth (2013).«The legal construction of privacy and data protection». *Computer Law & Security Review* (vol. 29, pág. 527).

Véase tambié el Dictamen 15/2011 sobre la definición del consentimiento del Grupo de Trabajo del Artículo 29, adoptado en julio de 2011 (pág. 7).

De Hert y Papakonstantinou señalan concretamente que en la DPD la conexión entre los artículos 6 y 7 no era muy clara, si bien según ellos era indiscutible (pág. 185). Hubiera sido deseable que el RGPD estableciera la conexión de forma más clara que la DPD, si bien tampoco es que sea muy evidente, pero según los autores citados esta conexión se deriva

del hecho de que el artículo 5 RGPD hace referencia a la licitud del tratamiento (art. 5.1.a), y el artículo 6 RGPD lleva precisamente por rúbrica: «Licitud del tratamiento» (pág. 187).

P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 179-194).

Otra característica del elenco de supuestos que recoge el artículo 6.1 RGPD es que se trata de un número cerrado. Así lo subrayó el TJUE en la sentencia de 24 de noviembre 2011, en el caso ASNEF[10]. Dicho tribunal puso de relieve que las bases legales constituyen un número cerrado, de modo que son las que son, y no constituyen un supuesto ejemplificativo al que puedan añadirse otras categorías (véase STJUE, de 24 de noviembre de 2011, §§ 30 y 31.).

(10)Se trata de la STJUE, de 24 de noviembre de 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD) *vs.* Administración del Estado, asuntos acumulados C-468/10 y C-469/10. El TS español planteó cuestión ante el Tribunal de Luxemburgo como consecuencia de los recursos contencioso administrativos que se plantearon contra el Reglamento que desarrolló la LOPD. El TS, en las sentencias que dictó el 15 de julio de 2010, anuló algunos preceptos de dicho Reglamento y respecto de otros preceptos planteó cuestión ante el TJUE en relación con la interpretación del art. 7 DPD.

Además, siguiendo en esta misma línea, el TJUE afirmó que en la implementación de la DPD, los Estados no podían añadir más requisitos a los que ya constan en el texto del articulado. Un ejemplo en el que no se cumplió esta exigencia fue en el caso de la legislación española, respecto del interés legítimo. La LOPD no contemplaba este supuesto como un mecanismo que por sí solo habilitara el tratamiento de datos, sino que exigía además que los datos estuvieran contenidos en fuentes accesibles al público. El TJUE declaró (véase STJUE, de 24 de noviembre de 2011, §§ 32, 35 y 36) que no era posible añadir más exigencias a las establecidas en el artículo 7 DPD y, por lo tanto, el interés legítimo era un mecanismo suficiente y su aplicación no podía quedar supeditada al hecho de que los datos además constaran en una fuente accesible al público. En definitiva, no pueden añadirse otros requisitos a los que se establecían en el artículo 7 DPD, afirmación que resulta plenamente trasladable al artículo 6 RGPD en la medida en que tiene una redacción prácticamente idéntica a la de la DPD.

En cuanto a los supuestos particulares habilitadores del tratamiento, a continuación se hará alguna precisión respecto de alguno de ellos, si bien el supuesto del consentimiento se analizará con más detalle en el apartado siguiente.

4.1. Análisis de las bases legales en particular

«1. 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; [este supuesto se analiza con más detalle en el apartado «En particular: el consentimiento» de este módulo].

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».

Al respecto, hay que tener en cuenta el considerando 44, que dispone que: «El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato».

Referencia bibliográfica

Acerca de las distintas bases legales, especialmente respecto a la legislación española, pueda consultarse:

M. Vilasau (2008).«¿Cómo llegar al consumidor? Entre la protección de datos y la legislación sobre la sociedad de la información». *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 18, págs. 83-101).

Esta base legal está vinculada al principio de minimización de los datos (art. 5.1.c RGPD), de forma que se recaban aquellos datos necesarios para el cumplimiento del contrato o para su perfección. Asimismo, también debe ponerse en relación con la previsión del artículo 7.4 RGPD, que se analizará al tratar del consentimiento del sujeto afectado.

> «c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento».

Al respecto, véanse los considerandos 41 y 45; este último dispone que:

> «Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinarse en virtud del Derecho de la Unión o de los Estados miembros [...]».

> «d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física».

De entrada, cabe señalar un pequeño cambio que se introduce en el RGPD y que supone una diferencia respecto de la DPD (art. 7.d. DPD): se contempla no solo el interés vital del interesado, sino también el de otra persona física. Sin embargo, como señalan De Hert y Papakonstantinou, se trata de una modificación de segundo nivel.

Referencia bibliográfica

P. De Hert; V. Papakonstantinou (2016).«The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 186).

Según se dispone en el considerando 46 RGPD, el recurso a esta base legal debe ser residual, de modo que los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Otra base jurídica distinta podría ser, como pone de relieve este mismo considerando, motivos relevantes de interés público. Piénsese, por ejemplo, en el control de una epidemia; en este caso, el tratamiento de los datos personales podría hallar su fundamento tanto en el interés público como en el interés vital del interesado y, según se ha dicho, el considerando 46 indica que es preferible que el recurso al interés vital sea subsidiario.

> «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».

En cuanto a esta base legal, deben tenerse en cuenta los artículos 6.2 y 6.3 RGPD. Si bien, como señalan De Hert y Papakonstantinou, el primero de ellos resulta redundante al existir la previsión del art. 6.3 RGPD.

«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».

Respecto a la interpretación de este precepto, los considerandos del RGPD establecen una serie de pautas que facilitan su interpretación.

Nota

Al respecto, véase el Dictamen 06/2014 del Grupo del Artículo 29, sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del art. 7 de la Directiva 95/46/CE, WP 217, adoptado el 9 de abril de 2014: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

1) En cuanto a la determinación de qué intereses deben prevalecer, deben tenerse en cuenta, entre otros aspectos, las expectativas razonables de los interesados, basadas en su relación con el responsable. En consecuencia, prevalecerán los intereses del afectado cuando se proceda al tratamiento de datos en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior (considerando 47).

2) Supuestos en los que puede darse dicho interés legítimo:

- «cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable» (considerando 47).

- «El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento» (considerando 47).

- «El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo» (considerando 47).

- «La transmisión de datos personales entre responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central, para fines administrativos internos» (considerando 48).

- «El tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información» (considerando 49).

3) La existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. Debe recordarse que esta base jurídica no resulta aplicable al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones.

En los supuestos en los que el afectado sea un niño, la ponderación entre los intereses existentes se decanta aún más a favor del afectado, de modo que deberá argumentarse aún con más fuerza la prevalencia del interés del RT respecto de los intereses legítimos del menor.

Asimismo, también debe tenerse en cuenta el considerando 48, que determina que:

> «Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados».

El interés legítimo, en cuanto base legal, fue especialmente analizado por el TJUE en el caso de ASNEF y también en el caso Google (derecho al olvido). En el primero de estos casos, el TJUE abordó si la legislación española había implementado correctamente el artículo 7.f) DPD, concretamente la referencia al interés legítimo. El TJUE contestó negativamente la pregunta planteada y señaló que no se pueden añadir más requisitos a la existencia del interés legítimo (como había hecho el legislador español, tanto en la LOPD como en el RLOPD).

Nota

STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S. L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12).

En el caso de Google Spain, el TJUE estudió cuál era el fundamento legal para tratar los datos personales por parte del buscador y, si bien consideró que sí existía un interés legítimo en dicho buscador, la STJUE dictaminó que en este caso debía prevalecer el derecho del afectado.

Nota

En cuanto al interés legítimo, véase STJUE Google Spain, §§ 71, 73, 74, 86 y 95. En cuanto a la ponderación en el caso concreto entre los intereses legítimos implicados, véase §§ 81, 97 y 98. Al respecto también puede consultarse:

M. Vilasau (2014). «El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido». *IDP. Revista de Internet, Derecho y Política* (núm. 18, págs. 16-32).

En cuanto al interés legítimo, la conclusión es que la redacción adoptada por el RGPD no aporta nada especialmente nuevo respecto a la redacción del artículo 7.(f) DPD. La única novedad es la referencia al supuesto en el que el interesado sea un niño. En tal caso, la ponderación entre los intereses en juego que comporta recurrir al interés legítimo debe tener especialmente en cuenta el hecho de que el afectado sea un niño. Se supone que en este caso será más difícil que prevalezcan los intereses del responsable del tratamiento.

Además de la enumeración de los supuestos que habilitan el tratamiento de datos, el artículo 6 RGPD realiza una serie de precisiones.

En el caso del artículo 6.2 RGPD, se dispone que:

> «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».

Si bien este precepto puede parecer que otorga un nivel de autonomía a los Estados en la medida en la que pueden mantener o introducir especificaciones respecto a las bases legales que habilitan el tratamiento de datos y adaptar la aplicación de las reglas reconocidas en el artículo 6.1, se trata, como señalan De Hert y Papakonstantinou, de un artículo superfluo, en tanto que el artículo 6.3 viene a disponer una previsión parecida.

Por otro lado, el artículo 6.3 RGPD dispone que:

> «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».

Una novedad que introduce el artículo 6.4 RGPD es la posibilidad de tratar los datos para otro fin distinto de aquel inicialmente previsto. Recuérdese que el artículo 5.1.b) RGPD dispone que los datos personales serán «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; [...]».

Sin embargo, el principio de limitación de la finalidad que se enuncia en este precepto quedaría de alguna forma un tanto diluido con la previsión del artículo 6.4 RGPD. Este último precepto permite que los datos sean tratados para otro fin distinto de aquel para el que se recogieron si se dan determinadas circunstancias:

Referencia bibliográfica

P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 179-194).

> «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».

El presupuesto para la aplicación de este precepto es que el nuevo tratamiento no esté basado en el consentimiento del interesado ni en el derecho de la Unión o de los Estados miembros.

> De algún modo se entiende que si hay consentimiento, no hace falta mayor justificación porque el consentimiento es el que da cobertura al tratamiento y si es una norma, esta es la que proporciona también cobertura, por lo que no es preciso ninguna otra causa de justificación.

En estos casos se atribuye al RT la facultad (podría decirse que la responsabilidad) de valorar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, y para ello debe tener en cuenta los elementos indicados en el artículo 6.4 RGPD. Debe señalarse que en la medida en que dicho precepto señala que el RT «tendrá en cuenta entre otras», se da a entender que la relación de elementos que se deben considerar no es cerrada, sino que es ejemplificativa, y que en definitiva se trata de una valoración subjetiva del RT. Por lo tanto, constituye una responsabilidad del RT llevar a cabo esta valoración. Ello supone abrir la puerta a un terreno que, sin duda alguna, generará incertidumbre al RT y también a las propias AAPD.

En aquellos casos en los que se traten datos para otra finalidad distinta de la inicialmente prevista, esto es, que se produzca un cambio de finalidad, también deberá tenerse en cuenta el artículo 23.2 RGPD (relativo a las limitaciones).

De Hert y Papakonstantinou señalan que esta mitigación del principio de finalidad resulta en parte realista, en la época del *big data*, la computación ubicua y la internet de las cosas. También afirman que el Parlamento Europeo estaba en contra de esta posibilidad y que hubiera preferido que se suprimiera este supuesto.

En definitiva, como señalan estos mismos autores:

«The fact remains, however, that further processing is indeed permitted under the Regulation, and it is up to the controller, according to the principle of accountability, to make the necessary evaluations as to whether the new, further processing, purposes are compatible with, and therefore permitted, the initials or not».

P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, pág. 186).

5. En particular: el consentimiento

Mònica Vilasau

Según dispone el artículo 6.1.a) RGPD, el consentimiento constituye una de las condiciones de licitud del tratamiento. Es decir, es una de las bases legales que permite el tratamiento de datos.

Gran parte de los tratamientos de datos se basan en el consentimiento del sujeto afectado y una de las formas que tienen los sujetos de ser conscientes de que un responsable está tratando sus datos es que este último se lo solicite.

5.1. Características del consentimiento

El artículo 4.11 RGPD proporciona una definición del término *consentimiento* según la cual se trata de:

> «[...] 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».

Nota

En términos prácticamente idénticos se pronuncia el art. 7.1 del Anteproyecto de Ley Orgánica de protección de datos de carácter personal (APLOPD).

En el considerando 32 se precisa lo siguiente:

> «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».

El requisito del **consentimiento libre** constituye la esencia misma del consentimiento, como exteriorización de la voluntad interna de un sujeto. Sin embargo, muy a menudo en las relaciones en las que se tratan dados de carácter personal se produce una situación de asimetría entre los sujetos que participan en dicha relación que dificulta que el consentimiento sea verdaderamente libre. Por ejemplo, si se desea comprar un billete de avión y se tienen que proporcionar determinados datos para poder adquirir el billete, ¿se puede decir que se trata de un consentimiento libre? O bien si alguien quiere participar en una determinada red social porque forman parte de esta todos sus amigos y se

le pide determinada información personal, de modo que si no se proporciona no se puede acceder a ella, ¿puede afirmarse que se presta el consentimiento de forma libre?

Referencias bibliográficas

En cuanto a la necesidad de un consentimiento libre, puede consultarse:

B. Van Alsenoy; E. Kosta; J. Dumortier (2013). «Privacy notices versus informational self-determination: Minding the gap». *International Review of Law, Computers & Technology*.

M. Arenas Ramiro (2013). «La validez del consentimiento en las redes sociales *on line*». En: Rallo Lombarte, A; Martínez Martínez, R. (coords.). *Derecho y Redes sociales* (2.ª ed.). Cizur Menor: Civitas-Thomson (pags. 159-201).

D. Le Métayer; S. Monteleone (2009). «Automated consent through privacy agents: Legal requirements and technical architecture». *Computer Law & Security Review* (vol. 25, núm. 2, págs. 136-144). http://dx.doi.org/10.1016/j.clsr.2009.02.010

A. Mantelero (2014). «The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics», *Computer Law & Security Review* (vol. 30, págs. 643 -660).

G. Zanfir (2013). «Forgetting About Consent: Why the Focus Should Be on "Suitable Safeguards"». *Data Protection Law*. http://ssrn.com/abstract=2261973

Para resolver estos interrogantes, debe subrayarse que no son lo mismo los casos en los que se proporcionan datos porque es preciso para celebrar un contrato (por ejemplo, compra de un billete), de aquellos otros en los que se trata de un servicio que *per se* no requiere necesariamente todo el conjunto de datos solicitados. El RGPD trata de dar respuesta a alguna de estas cuestiones.

Concretamente, en la Propuesta de RGPD presentada por la Comisión el 25 de enero de 2012 se establecía una disposición, distinta del texto final actual, que pretendía garantizar que se tratara de un consentimiento libre. Así, en el artículo 7.4 se disponía que: «El consentimiento no constituirá una base jurídica válida para el tratamiento cuando exista un desequilibro claro entre la posición del interesado y el responsable del tratamiento». Sin embargo, esta disposición fue eliminada y no se consolidó en el texto definitivo aprobado. De todos modos, sí que se trasladó a los considerandos, aunque obviamente no tiene el mismo potencial que de haber permanecido en el articulado del RGPD.

Concretamente, se trasladó al considerando 43, que dispone que:

> «Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento».

Otras de las cuestiones planteadas en este considerando se tratan de resolver en el artículo 7 RGPD, que hace referencia a las condiciones del consentimiento y que será abordado en el apartado «Condiciones para el otorgamiento del consentimiento».

En cuanto al requisito de que se trate de un **consentimiento específico**, este es un aspecto intrínsecamente relacionado con los principios de protección de datos, concretamente con los principios de limitación de la finalidad (art. 5.1.b. RGPD) y también en cierta medida con el principio de minimización de los datos (art. 5.1.c. RGPD). Es obvio que si la finalidad tiene que estar limitada, los datos que hay que recabar son los relacionados con dicha finalidad y, por lo tanto, no puede hacerse una solicitud genérica de datos, sino acotada a una finalidad concreta.

Por lo que respecta al requisito del **consentimiento informado**, debe proporcionarse la información precisa para que el afectado pueda decidir en consecuencia si consiente el tratamiento. Este requisito está relacionado con el principio de transparencia (art. 5.1.a. RGPD).

La exigencia de información conlleva dos aspectos. Uno formal, esto es, la forma como debe proporcionarse la información; y otro de contenido, en cuanto al alcance y objeto de la información:

- En cuanto a la forma de la información, como señala el considerando 42, «[...] De acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas». A ello se dedica además el artículo 12 RGPD.

- En cuanto al aspecto de contenido, según dispone también el considerando 42, «[...] Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. [....]».

Nota

Véase al respecto el art. 21 del APLOPD, cuya rúbrica es: «Transparencia e información».

Además, a lo largo del articulado del RGPD se dedican preceptos concretos a detallar cómo debe ser esta información, en función de si los datos se obtienen o no del afectado. Véanse concretamente los artículos 13 y 14 RGPD.

En cuanto al requisito de que sea un **consentimiento inequívoco** , es preciso subrayar que las Propuestas de la Comisión (enero de 2012) y del Parlamento (texto de abril 2014) establecían en lugar del término *inequívoco*, que el consentimiento debía ser *explícito*. Sin embargo, esta exigencia no se mantuvo en la redacción final, que retornó al requisito establecido en la Directiva acerca de la necesidad de un consentimiento **inequívoco** (art. 7.a DPD).

No obstante, el hecho de proporcionar el consentimiento se ha convertido en muchas ocasiones en algo automático. Ello comporta que ya se trate de un consentimiento explícito ya de uno inequívoco, no se garantiza en muchos casos la plena conciencia y voluntad del afectado por el tratamiento, de ahí que deba adoptarse con cautela el recurso generalizado a la obtención del consentimiento.

Voluntad del afectado

Piénsese en las numerosas ocasiones en las que bien para instalar una aplicación en el móvil, bien para consultar una información o acceder a un servicio, se pide el consentimiento al afectado. Este consentimiento se da de manera mecánica, sin leer toda la información proporcionada, y con la única finalidad de obtener cuanto antes el servicio o el bien deseado.

La fórmula adoptada por el artículo 4.11 RGPD rechaza el silencio como mecanismo de obtención del consentimiento del sujeto afectado. Este puede manifestarse mediante una declaración o mediante «una clara acción afirmativa». En consecuencia, el mero silencio no puede considerarse una forma de prestar el consentimiento y por lo tanto no habilitaría para tratar los datos personales.

Al respecto, debe tenerse en cuenta el considerando 32 del RGPD, que dispone 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».

Por ejemplo, el afectado recibe una comunicación en la que se le invita a suscribirse gratuitamente a una publicación y se le indica que si no contesta en un determinado plazo se entenderá que consiente el tratamiento de determinados datos. Sobre la base del artículo 4.11 RGPD, esta cláusula, junto con la falta de respuesta por parte del afectado, no tendría ninguna validez como consentimiento. Por lo tanto, en caso de que una persona no manifieste nada ante la solicitud de tratar los datos que le conciernen, ello no comportará en ningún caso que consienta el tratamiento.

Por el contrario, el artículo 14 del Reglamento que desarrolla la LOPD (RLOPD) atribuyó precisamente unas consecuencias positivas al silencio si se cumplían determinados requisitos. Por lo tanto, cuando resulte plenamente aplicable el RGPD, este precepto del RLOPD no podrá utilizarse en la medida en que es contrario al texto de la norma de la UE.

Nota

El art. 7.1 APLOPD, que prácticamente reproduce el art. 4.8 RGPD, establece que se entiende por consentimiento del afectado toda manifestación de voluntad «[...], ya sea mediante una declaración o una clara acción afirmativa [...]». En definitiva, siguiendo el texto de la UE, el APLOPD establece que no cabe inferir un consentimiento del silencio del sujeto afectado.

5.2. Condiciones para el otorgamiento del consentimiento

El artículo 7 RGPD lleva por rúbrica «Condiciones para el consentimiento». En dicho precepto, se regulan distintas previsiones relativas al consentimiento.

Artículo 7.1 RGPD:

> «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».

En definitiva, corresponde al RT acreditar la existencia del consentimiento del afectado. Así lo dispone el considerando 42 RGPD, que determina que:

> «Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento [...]».

Artículo 7.2 RGPD:

> «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».

Así lo dispone también el considerando 42, que establece que:

> «[...] En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo (1), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. [...]».

Por otro lado, el considerando 43 dispone que:

> «[...] Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento».

El punto de partida de este precepto lo constituye aquel supuesto en el que en el marco de una declaración escrita o de un negocio jurídico se abordan distintos aspectos de forma indistinta. El artículo determina la necesidad de identificar y separar claramente, entre las distintas disposiciones, aquella relativa al tratamiento de los datos personales. Se plantea la necesidad de prestar el consentimiento por separado, de modo que si se solicita el consentimiento para distintos asuntos, se distinga claramente cada uno de ellos (art. 7.2 RGPD). La finalidad de este precepto es que el sujeto pueda conocer claramente qué se está solicitando y pueda, por ejemplo, consentir una cláusula y rechazar otra.

Nota

Téngase en cuenta que el art. 6.1 RGPD indica que el consentimiento debe proporcionarse para uno o varios fines específicos. En consecuencia, no sería válido un consentimiento para un conjunto de finalidades, sin especificar el alcance del consentimiento. En este sentido, véase el considerando 32 *infine* del RGPD.

También cabe destacar que el art. 7.2. APLOPD dispone que: «Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste claramente dicho consentimiento para cada una de ellas».

Por ejemplo, se contrata un servicio de telefonía y en el contrato deben distinguirse las cláusulas que afectan a la prestación del servicio (por ejemplo, las tarifas) de aquellas que hacen referencia al tratamiento de los datos personales (qué datos son necesarios, plazo de conservación, etc.). Muy a menudo la información se proporciona de manera entremezclada y el afectado no sabe bien a qué consiente.

Artículo 7.3 RGPD

> «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».

El término *retirar el consentimiento* se refiere a lo que se conoce habitualmente en la teoría del negocio jurídico como «revocación del consentimiento».

El afectado debe ser debidamente informado de esta facultad, tal y como se establece en los artículos 13.2.c) y 14. 2.d) RGPD.

Todas aquellas operaciones que el RT haya efectuado previamente a la revocación serán perfectamente válidas.

El artículo 6.3 LOPD también establece la facultad de revocar el consentimiento cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Artículo 7.4 RGPD

> «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».

Así también se recoge en el considerando 42 RGPD, que dispone que:

> «[...]. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno».

Esta medida pretende garantizar que el consentimiento sea libre y recoge lo que se conoce en la normativa de defensa de los consumidores y usuarios como «prohibición de vinculación».

Por ejemplo, si se contrata un servicio de suministro de gas o de electricidad, la prestación de este no puede supeditarse al hecho de que el afectado preste su consentimiento para el tratamiento de datos relativos a sus preferencias o hábitos de alimentación porque estos datos no son necesarios para prestar el servicio contratado.

Por lo tanto, si el RT quiere pedir datos que no son necesarios para un determinado contrato, podrá hacerlo siempre y cuando:

- En el contrato que suscriba con el afectado se distinga convenientemente aquellas cláusulas relativas al tratamiento de datos del resto de las cláusulas, tal y como exige el artículo 7.3 RGPD.
- En el contrato que suscriba se distinga convenientemente aquellos datos que son precisos para la prestación del contrato/servicio y los que no los son.
- No se vincule la prestación del servicio o contratación de un bien al tratamiento de datos que no sean necesarios para el cumplimiento del contrato celebrado, según exige el artículo 7.4 RGPD.

El art. 7.3 APLOPD dispone que:

«Cuando en el marco de un proceso de negociación o formalización de un contrato se solicite el consentimiento del afectado para llevar a cabo un tratamiento cuya finalidad no guarde relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá garantizarse que el afectado pueda manifestar específicamente su voluntad en relación con este tratamiento poniendo a su disposición un procedimiento sencillo, claro y comprensible.

Este procedimiento podrá consistir, en particular, en la inclusión de una casilla específica en el contrato, siempre y cuando la misma no se encuentre previamente marcada».

Si bien este precepto trata de alguna forma de incorporar la prohibición de vinculación (del art. 7.4 RGPD) al ordenamiento jurídico español, parece que no lo logra plenamente.

De hecho, el art. 7.3 APLOPD está mezclando dos aspectos distintos regulados en el art. 7 RGPD. Concretamente, está intentando reunir en un mismo precepto las previsiones de los arts. 7.2 y 7.4 RGPD. Sin embargo, consideramos que no lo consigue plenamente y debería introducirse de forma clara en el art. 7.3 APLOPD que no puede supeditarse la ejecución de un contrato o la prestación de un servicio a que el afectado consienta el tratamiento de datos personales que no sean necesarios para la prestación de dicho servicio o la ejecución de dicho contrato.

5.3. El consentimiento de los menores

El RGPD hace unas referencias específicas al tratamiento de datos de los menores. En la versión del RGPD de 2012 se incluía una definición de qué se consideraba *niño*. El artículo 4 RGPD no define qué se entiende por *menor*.

El RGPD contiene algunas disposiciones acerca del tratamiento de los datos de carácter personal de los menores, una específica en el artículo 8 y otra en el artículo 6.1.f) al hacer referencia al interés legítimo. También existe otra referencia a la información que debe proporcionarse a los niños en el considerando 58.

El artículo 8 RGPD dispone que:

> «1. 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.
>
> 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
>
> 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño».

En consecuencia, sobre la base del RGPD, el menor podría otorgar su consentimiento si es mayor de 16 años. Por debajo de esta edad sería necesario el consentimiento (o la autorización) de sus padres o tutores. Sin embargo, los Estados miembros pueden establecer una edad inferior siempre que no esté por debajo de los 13 años.

El artículo 8.1 RGPD es bastante similar al artículo 13.1 RLOPD. Este último dispone que:

> «Podrá procederse al tratamiento de los datos de los mayores de 14 años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de 14 años se requerirá el consentimiento de los padres o tutores».

Sin embargo, pese a las similitudes entre el texto RLOPD y RGPD se constatan las siguientes diferencias:

- El ámbito de aplicación del RLOPD es más amplio que el del RGPD. El primero hace referencia sin más a «el tratamiento de los datos de los mayores de 14 años», mientras que el RGPD contempla «la oferta directa a niños de servicios de la sociedad de la información». Por lo tanto, el RLOPD incluye el tratamiento de datos incluso por medios no automáticos, por ejemplo en papel (piénsese en las fichas médicas no informatizadas), así como los tratamientos automatizados que no estén circunscritos a la oferta directa de servicios de la sociedad de la información.

- En cuanto a la edad, el límite se establece en el RLOPD a los 14 años, mientras que en el RGPD es a los 16; sin embargo, en este último texto puede rebajarse hasta los 13, lo que no contempla el RLOPD.

En definitiva, en el marco de aplicación de la LOPD y RLOPD pueden tratarse los datos de los mayores de 14 años con su consentimiento. Cuando resulte aplicable plenamente el RGPD en el ordenamiento jurídico español, cabe afirmar que también podrán seguir tratándose los datos de los mayores de 14 años puesto que ya existe la norma que así lo dispone y a la que habilita el artículo 8.1. *infine* RGPD. Sin embargo, la aplicación del artículo 13 RLOPD en cuanto a la edad de los menores podría plantear alguna duda, en la medida en que el artículo 8 RGPD hace una llamada a la Ley para determinar, en el ordenamiento interno de cada Estado, el límite de edad a partir del que se puede consentir, y teniendo en cuenta que el RLOPD es una norma reglamentaria. Sin embargo, puesto que el APLOPD aborda esta cuestión, ya existiría la cobertura legal necesaria. Concretamente, el artículo 8.1 APLOPD resuelve expresamente este aspecto y establece que el tratamiento de datos de un menor podrá fundarse en su consentimiento cuando sea mayor de trece años, con lo que se amplía la edad respecto de las posibilidades permitidas por el RGPD.

Debe destacarse que el RGPD no hace referencia en ningún caso al supuesto de los incapacitados. Se puede entender que la sentencia de incapacitación determinará tales extremos, pero ¿y si no dice nada al respecto? Piénsese en todos los datos de salud de los incapacitados, ¿quién debe autorizar el tratamiento de estos datos? En defecto de una norma al respecto, y si la sentencia nada determina, debería otorgarse al incapacitado la facultad de poder consentir, a partir del principio de que la limitación de la capacidad debe interpretarse siempre en el sentido menos restrictivo posible.

Según dispone el artículo 8.2. RGPD:

> «El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible».

Este precepto es muy similar al artículo 13.4 RLOPD. Lógicamente, se atribuye al RT un deber de poner unos medios razonables, pero no se establece una obligación de resultado.

Referencia bibliográficas

En cuanto al uso que hacen los menores de Internet y de las redes sociales puede consultarse:

S. Livingstone (2015). «Children's digital rights». *InterMEDIA*, 42 (4/5) (págs. 20-24).

S. Livingstone; M. Bulger (2014). «A global research agenda for children's rights in the digital age». *Journal of Children and Media*. DOI: 10.1080/17482798.2014.961496.

A. Marwick; D. Boyd (2014). «Networked privacy: How teenagers negotiate context in social media». *New Media & Society* (vol. 16, núm. 7, págs. 1051-1067).

5.4. El tratamiento de categorías especiales de datos (datos sensibles)

El término *dato personal*, analizado previamente, hace referencia a un abanico muy amplio de información relativa a un sujeto. En este apartado se trata de analizar una categoría de datos personales. Gran parte de los textos legales que regulan el tratamiento de datos personales otorgan una mayor protección a determinados datos (categorías especiales), que se conocen como **datos sensibles**.

Determinar qué datos deben considerarse sensibles puede hacerse de dos modos. Una primera opción es identificar una serie de datos que por su naturaleza deben gozar de mayor protección. Por ejemplo, los datos relativos a la raza o a la ideología se considerarían más sensibles porque en función de ellos se podría clasificar a las personas y dar lugar a discriminación. La otra opción es considerar que aquello determinante no es el tipo de dato en sí mismo, sino el tratamiento que se haga de él. En este sentido, una fotografía de un sujeto puede revelar su raza, pero en función del tratamiento ello puede entrañar cierta peligrosidad o no. Por ejemplo, si se trata de una foto para un carné que permita acceder a una biblioteca, ello considerado en sí mismo no generaría discriminación. Por el contrario, si se trata de llevar a cabo un listado de modo que en función de la raza el sujeto sea más susceptible de ser investigado o vigilado, ello sí que sería constitutivo de discriminación.

La DPD siguió el criterio más tradicional de contemplar un listado de datos que son considerados sensibles y el RGPD ha seguido el mismo patrón. Sin embargo, algunos autores han señalado que el hecho de que el artículo 8.1. DPD estableciera que «Los Estados miembros prohibirán el tratamiento de datos personales que revelen [...]»podría dar a entender que la información sensible tendría una dimensión más dinámica, de manera que aquello relevante sería el tratamiento que se hiciera del dato. El RGPD, como decíamos, ha optado por la misma solución que la DPD y establece que: «Quedan prohibidos el tratamiento de datos personales que revelen el [...]». De adoptarse esta visión más dinámica, un dato como por ejemplo la alimentación de un sujeto podría considerarse como un dato sensible, en la medida en que podría revelar la ideología de una persona. Piénsese por ejemplo en un hospital, en donde se le pide al paciente que indique cuáles son sus preferencias de un menú. En caso de marcar determinadas opciones, ello podría revelar información relativa a creencias religiosas. Si se optara por una dimensión más dinámica del término *dato sensible*, ello en según qué casos podría determinar que un dato inocuo como una opción alimentaria pudiera considerarse como sensible.

Sin embargo, como señalan De Hert y Papakonstantinou, si bien el término *revelar* podría denotar una interpretación dinámica de qué se entiende por información sensible, no ha sido así en la interpretación de la DPD. Los datos se distinguían entre sensibles y no sensibles en función de su naturaleza y no de su uso potencial. Y según estos autores este problema continuará igual en el marco del nuevo RGPD.

Referencia bibliográfica

P. De Hert; V. Papakonstantinou (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 183).

En esta línea, el RGPD, siguiendo la DPD, no trata todos los datos de la misma forma, sino que establece una distinción entre ellos.

El artículo 9 RGPD lleva por rúbrica «Tratamiento de categorías especiales de datos personales». Por lo tanto, lo que hace especial un tratamiento es el tipo de datos a los que hace referencia, y no las circunstancias de dicho tratamiento. A menudo, en lugar del término *categorías especiales de datos*, se utiliza el de *datos sensibles*.

5.4.1. Datos que tienen la categoría de especiales (artículo 9 RGPD)

Se trata de los datos personales que revelen «el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física» (art. 9.1 RGPD).

El artículo 9 RGPD sigue un patrón similar al artículo 8 DPD, si bien entre ambos preceptos existen algunas diferencias. En el RGPD se incluyen nuevas categorías de datos respecto a las contempladas en la DPD. Este es el caso de los datos genéticos y biométricos. Antes de la aprobación del RGPD se defendía por algunos autores que los datos genéticos podían considerarse incluidos dentro de los datos de salud. Sin embargo, debe admitirse que no todos los datos genéticos están relacionados con la salud. Por lo tanto, el hecho de incluir expresamente el dato genético implica que se hayan disipado las dudas acerca de que quedan protegidos de manera especial este tipo de datos.

Definiciones

Véase la definición de estos tipos datos en el artículo 4 RGPD; concretamente, el artículo 4.13 RGPD en cuanto a los datos genéticos y el artículo 4.14 RGPD por lo que respecta a los datos biométricos.

Por lo que se refiere a otros tipos de datos sensibles, el RGPD proporciona alguna variación en cuanto a la redacción y a los términos utilizados. Concretamente, en cuanto a los datos relativos a la sexualidad; así, el RGPD habla de datos relativos a la «vida sexual» o la «orientación sexual» de una persona física, mientras que la DPD hace referencia a «datos relativos a la sexualidad», por lo que los términos del RGPD son más amplios que los de la DPD.

Otra categoría que cabe tener en cuenta es la relativa a los datos referentes a condenas e infracciones penales. La Propuesta de la Comisión de enero de 2012 incluyó dentro de la relación de datos sensibles aquellos relativos a «condenas penales o medidas de seguridad afines» y en el artículo 9.2.j) de dicha Propuesta se determinaban las excepciones en las que estos datos podían tratarse.

Cita

«**Artículo 9.1.COM 2012**
Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, *las condenas penales o medidas de seguridad afines*».

Sin embargo, en el texto finalmente aprobado se reubicaron este tipo de datos; se excluyeron del artículo 9 RGPD y se destinó un artículo específico, el 10 RGPD, a su regulación. Este precepto dispone que:

> «El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, solo 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».

Cita

«**Artículo 9.2.j) COM 2012**
El tratamiento de datos relativos a condenas penales o medidas de seguridad afines se lleva a cabo bajo la supervisión de poderes públicos o si el tratamiento es necesario para cumplir una obligación jurídica o reglamentaria a la que esté sujeto el interesado o para desarrollar una tarea llevada a cabo por motivos importantes de interés público y siempre que lo autorice el Derecho de la Unión o la legislación de los Estados miembros que establezca las garantías apropiadas. Solo se llevará un registro completo de condenas penales bajo el control de los poderes públicos».

La DPD había adoptado una solución a medio camino entre las dos opciones planteadas. Los había incluido en el artículo dedicado a regular las categorías especiales de tratamiento pero no los hacía constar en la relación de datos sensibles que se recogía en el artículo 8.1 DPD. En cambio, dedicaba el artículo 8.5 DPD a regular cómo podían ser tratados. El RGPD, como acabamos de decir, los saca del precepto que dedica a regular las categorías especiales de datos personales y les dedica un precepto específico.

La solución que proporciona el RGPD respecto a las condenas e infracciones penales y a las medidas de seguridad tiene una diferencia sutil respecto de la DPD. Nótese que en el artículo 10 RGPD se hace mención solo a un supuesto cuyo tratamiento está sometido a las autoridades, aquel que pueda tener lugar mediante el consentimiento del sujeto afectado. En cambio, la DPD hacía una declaración general de sujeción al control de las autoridades públicas. Por lo tanto, podría sostenerse que actualmente se otorga menos protección

En cuanto al tratamiento de datos relativo a sanciones administrativas o procesos civiles, el texto de la DPD establece que «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» (art. 8.5.2 DPD). Por el contrario, el RGPD nada dice al respecto.

5.4.2. Condiciones para tratar los datos especiales (sensibles)

Las condiciones para tratar los datos sensibles no difieren mucho entre la DPD y el RGPD.

De la misma forma que se contempla en el artículo 8 DPD, el artículo 9 RGPD parte de un principio prohibitivo del tratamiento de los datos sensibles. El artículo 9.1 RGPD determina que «quedan prohibidos el tratamiento de datos personales que revelen [...]». Sin embargo, tras establecer esta prohibición tan

radical, se establece que «el apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: [...]» (art. 9.2 RGPD), con lo que se puede levantar la prohibición en los supuestos que a continuación se enumeran.

En definitiva, del mismo modo que se establece en el artículo 8 DPD, el artículo 9 RGPD determina una regla general de prohibición y a continuación una relación de excepciones a dicha prohibición.

«**Artículo 9.2 RGPD**

El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito, 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 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,

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física,

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,

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,

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,

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».

Nótese, en cuanto al otorgamiento del consentimiento, que el artículo 9.2.a) RGPD establece la exigencia de consentimiento explícito. Se considera que con la exigencia de un **consentimiento explícito**, en lugar de un consentimiento inequívoco (tal y como establece el art. 4.11 RGPD como regla general), se

otorga una mayor protección al afectado en la medida en que no será tan automática la prestación del consentimiento. Esta misma solución también era la ofrecida por la DPD (art. 8.2.a DPD).

> En cuanto al tratamiento de los datos sensibles y respecto a la posibilidad de que el consentimiento explícito del afectado habilite el tratamiento de estos datos, la Propuesta de reforma de la LOPD adopta una solución muy restrictiva al respecto. El art. 10.1 APLOPD dispone que:
>
> «A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico».
>
> Si bien es preciso subrayar que se hace referencia no a todo tratamiento de datos sensibles, sino aquel cuya finalidad principal sea identificar los datos mencionados. (Al respecto compárese la redacción del art. 7 LOPD con el art. 10 APLOPD.)

En cuanto a las diferencias entre el contenido del artículo 8 DPD y el artículo 9 RGPD respecto al tratamiento de los denominados datos sensibles, pueden determinarse las siguientes:

1) La forma de hacer referencia a las excepciones a la regla general contenida en el primer párrafo de los respectivos artículos. Así, en la DPD se dispone que «no se aplicará cuando», mientras que el RGPD hace referencia a que «concurra una de las circunstancias siguientes». Por lo tanto, en el texto RGPD queda claro que solo con que concurra una de ellas es suficiente para su aplicación.

2) En cuanto a la posibilidad de establecer excepciones, el artículo 8.4 DPD determina que:

> «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».

Por lo tanto, ello comportaría añadir otras excepciones a las ya previstas.

Esta posibilidad también se contempla en el artículo 9.2.g) RGPD, si bien su redacción es un tanto diferente: dispone que la prohibición de no tratar los datos sensibles no será de aplicación cuando:

> «[...] 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».

Sin embargo, existen matices entre la redacción del artículo 8.4 DPD y la del artículo 9.2.g) RGPD, algunos de los cuales son relevantes. La DPD determina que son los Estados los que podrán establecer otras excepciones, con lo que se deduce que como mínimo deberá adoptarse una disposición o regulación en la que se ponderen los derechos en juego y especialmente la adopción de las garantías adecuadas. En cambio, sobre la base del texto del RGPD, parece ser que sin necesidad de adoptar esta disposición pueden establecerse excep-

(11)La DPD hace referencia a «por motivos de interés público importantes».

ciones si concurre una circunstancia concreta: que el tratamiento **sea necesario por razones de un interés público esencial**[11]. Pero no se determina ni quién debe llevar a cabo esta valoración, ni cómo debe adoptarse (mediante qué instrumento). Solo se determina qué elementos deberán tenerse en cuenta: 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.

Por lo tanto, el artículo 9.2.g) RGPD podría incluso interpretarse en el sentido de que es el RT quien podría adoptar la decisión de tratar los datos sobre la base de lo que él considerara un interés público esencial. Esta solución no parece la más adecuada. En cambio, en el texto de la DPD parece más claro que debe adoptarse una medida legislativa antes de poder introducir otra excepción.

Además, la redacción de la DPD establece una ulterior garantía, en la medida en que, según dispone en el artículo 8.6, «Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión». Esto es, una vez establecida la excepción, esta debe notificarse a la Comisión, con lo que parece existir un control suplementario.

3) En relación con los datos de salud, el RGPD establece más supuestos en los que los datos pueden tratarse prescindiendo del consentimiento explícito del afectado. Ello en parte es razonable, puesto que cada vez la casuística es mayor y deben contemplarse más escenarios de los que inicialmente la DPD previó. Otra cosa es que esto sea deseable, pero de alguna forma es una consecuencia lógica de la complejidad de los tratamientos sanitarios y de la necesidad de tener este tipo de información interconectada.

4) Otras diferencias son las siguientes:

Mientras que el artículo 8.e) DPD establece como excepción que el tratamiento «sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial», el artículo 9.f) RGPD dispone que será excepción si «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». Por lo tanto, la terminología que usa el RGPD, que habla de «reclamaciones», es más amplia que la de la DPD, que parece circunscribirse a un procedimiento judicial.

Cabe señalar también que los supuestos recogidos en los artículos 9.h) y 9.i) RGPD son más amplios que el equivalente del artículo 8.3 DPD. Por último, debe subrayarse que el artículo 9.2. j) sí que supone una diferencia respecto a la DPD.

6. Los mecanismos de *soft law*: los códigos de conducta y la certificación

Mònica Vilasau

Ya se ha señalado que uno de los principios sobre los que se basa el RGPD y que supone una novedad de la nueva regulación es el principio de responsabilidad proactiva. Ello está ligado a una serie de medidas que se pueden calificar como de *soft law* y que se concretan, entre otras, en la implementación de códigos de conducta y mecanismos de certificación.

Los códigos de conducta tienen como objetivo contribuir a una correcta aplicación del RGPD. Las certificaciones, los sellos y las marcas ayudan a demostrar que se está cumpliendo con las disposiciones del RGPD (se trata, en definitiva, de mecanismos de *compliance*, esto es, de acreditación del cumplimiento).

Las organizaciones independientes de certificación, las autoridades de protección de datos, el Comité Europeo de Protección de Datos y en su caso la Comisión certificarán a las empresas y llevarán a cabo un seguimiento del cumplimiento adecuado de la certificación. Este aspecto también constituye una novedad del RGPD respecto de la DPD.

6.1. Los códigos de conducta

Los códigos de conducta (CC) ya se mencionaban en la DPD, si bien no se les proporcionó demasiada atención. Durante el proceso de adopción del RGPD, se criticó el hecho de que la aplicación del texto podía comportar un coste elevado para las pymes. Uno de los mecanismos para tratar de dar respuesta a estas críticas fue la introducción de códigos de conducta, que ya habían sido recogidos en el art. 27 DPD, si bien, como decíamos, habían pasado un tanto desapercibidos.

Los códigos de conducta, según algunos autores, constituyen un ejemplo de autorregulación, pero otros autores, como por ejemplo Díaz-Romeral, consideran más apropiado hablar de corregulación en la medida en que, aparte de la iniciativa privada que los pone en marcha o que promueve su adopción, deben pasar una serie de controles en cuanto a su contenido y ser aprobados por alguna autoridad, ya sea una autoridad de control, el Comité o la propia Comisión.

Referencia bibliográfica

A. Díaz-Romeral (2016). «Los códigos de conducta en el Reglamento General de Protección de Datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Actualmente, con la excepción de algunos sectores específicos, existen pocos códigos de conducta. Sin embargo, su potencial para abordar el tratamiento de información personal se ha hecho patente, de modo que se les ha prestado mayor atención. Entre las novedades del RGPD destaca la incorporación

de la necesidad de monitorizar el cumplimiento de los códigos de conducta aprobados. Este seguimiento del cumplimiento de un CC será llevado a cabo por una organización que tenga un nivel apropiado de experiencia en el sector concreto del que se trata y resulte acreditada para desempeñar dicha función por la autoridad competente.

El artículo 40.1. RGPD dispone que:

> «Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas».

Siguiendo a Díaz-Romeral, en cuanto a las características de los códigos de conducta cabe destacar que:

- Se trata de un acuerdo de buenas prácticas.
- No es impuesto por disposiciones legales, ni a nivel nacional ni supranacional.
- Es aprobado por una autoridad pública de control competente.
- Define comportamientos y buenas prácticas
- El adherente a un CC se compromete a cumplir sus disposiciones, orientadas a la correcta aplicación del RGPD en sectores de tratamiento específicos.
- En cualquier caso queda sujeto a la supervisión por un organismo acreditado por la autoridad de control competente.

Referencia bibliográfica

A. Díaz-Romeral (2016). «Los códigos de conducta en el Reglamento General de Protección de Datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (pág. 390). Madrid: Ed. Reus.

6.1.1. Funciones de los códigos de conducta

Un CC desempeña dos funciones principales:

- Facilita la aplicación de las normas jurídicas.
- Constituye un indicio del cumplimiento de la normativa.

1) El código de conducta como facilitador del cumplimiento normativo

Los códigos de conducta, según dispone el artículo 40.1. RGPD, están destinados a contribuir a la correcta aplicación del Reglamento; esta finalidad se corrobora en el artículo 40.2 RGPD, que prevé que quienes están legitimados para elaborar los códigos de conducta lo harán con el objeto de especificar la aplicación del RGPD.

En consecuencia, la primera finalidad de un CC es la de concretar la aplicación del RGPD en un sector determinado.

La finalidad del CC es pues la de especificar, respecto a un determinado sector, cuáles son las obligaciones que corresponden al RT y al ET. Así lo concreta el considerando 98 del RGPD, que dispone que:

> «Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento».

2) El código de conducta como acreditador del cumplimiento del RGPD

La adhesión a un CC constituye un indicio del cumplimiento de las obligaciones que se recogen en él. Así lo pone de relieve el artículo 24 RGPD, que al regular la responsabilidad del responsable del tratamiento, señala que «La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento» (art. 24.3 RGPD).

Del mismo modo, al regularse el supuesto en el que un RT recurra a un ET y determinar que debe elegirse a alguien que ofrezca garantías suficientes (art. 28.1 RGPD), se dispone que «La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo» (art. 28.5 RGPD). En este sentido se pronuncia también el considerando 81.

En relación con la seguridad del tratamiento, el artículo 32.1. RGPD dispone que:

> «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: [...]».

Y concretamente el artículo 32.3 RGPD establece:

> «La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo».

En definitiva, la adhesión a un CC (si no es una adhesión meramente formal, de modo que este no sea observado), puede valorarse como un elemento de atenuación de la responsabilidad en caso de imponer una sanción. Ello es lógico; si un RT se ha adherido a un CC y lo ha cumplido, ello debe tenerse

en cuenta por la autoridad competente como un mecanismo favorable, en la medida en que el RT o ET se haya ajustado a dicho código. Así se dispone en el considerando 148.

6.1.2. Procedimiento de adopción de los códigos de conducta

En la medida en que se considera que la adopción de un CC es un instrumento beneficioso para la implementación del RGPD, determinados sujetos deben promover la adopción de estos (art. 40.1 RGPD). Para ello, deben tenerse en cuenta los elementos que se mencionan en el artículo 40.1 RGPD, y concretamente: «las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas». Asimismo, se faculta a las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento para elaborar y modificar códigos de conducta (art. 40.2 RGPD).

El artículo 40.2 RGPD hace una relación del posible contenido de los códigos de conducta, cuya finalidad es la de especificar la aplicación del RGPD.

En cuanto al procedimiento que hay que seguir, debe distinguirse entre aquellos códigos referidos a actividades de tratamiento en un solo Estado miembro, de aquellos otros que afecten a varios Estados.

En el primer caso, quienes proyecten elaborar un CC o modificar o ampliar uno existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas (art. 40.5 RGPD).

Si el proyecto de código o la modificación o ampliación es aprobado y el código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código (art. 40.6 RGPD).

En el segundo caso, si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente lo presentará antes de su aprobación o de la modificación o ampliación al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el Reglamento u ofrece garantías adecuadas (art. 40.7 RGPD).

Si el dictamen del Comité confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el Reglamento u ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión (art. 40.8 RGPD).

La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados tengan validez general dentro de la Unión (art. 40.9 RGPD).

La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el artículo 40.9 RGPD (art. 40.10 RGPD). El Comité, por su parte, archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado (art. 40.11 RGPD).

En definitiva, los CC tienen un procedimiento de elaboración participativo y multinivel, con una participación pública final que aporta una garantía porque lo aprueba solo si es conforme con el RGPD.

6.1.3. Supervisión de los códigos de conducta

Un elemento clave de los CC es la supervisión en su cumplimiento, lo que constituye un elemento básico para generar confianza, tanto respecto de los afectados por el tratamiento como de la sociedad en general, en dichos códigos.

La supervisión de los CC se deja a dos instancias: por un lado, a las autoridades competentes y, por el otro, a un órgano específico de supervisión. Así los dispone el artículo 41.1 RGPD, que determina que, sin perjuicio de las funciones de las autoridades de protección, «podrá supervisar el cumplimiento de un código de conducta [...] un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente».

El organismo *ex* artículo 41.1 RGPD podrá ser acreditado para supervisar si cumple una serie de requisitos, que se recogen en el art. 41.2 RGPD. Concretamente, se trata de que dicho organismo:

> «(a) haya demostrado su independencia y pericia en relación con el objeto del código;
>
> (b) haya establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
>
> (c) haya establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y
>
> (d) haya demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses».

El propio CC ha de contener los mecanismos que permitan a dicho organismo efectuar el control obligatorio del cumplimiento de sus disposiciones. Así lo dispone el artículo 40.4 RGPD, según el cual el código de conducta «contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apar-

tado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes [...]».

Se trata de un control obligatorio, que deberá efectuarse de forma diligente, y si no es así ello puede comportar la revocación de la acreditación (art. 41.5 RGPD). Dicho control puede consistir, por ejemplo, en la realización de auditorías. Asimismo, como aspecto fundamental en la labor de supervisión, el artículo 41.4 determina que el organismo de supervisión deberá adoptar las medidas adecuadas en caso de infracción del código, que pueden ser la suspensión/exclusión de este:

> «Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente».

La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia, el proyecto que fije los criterios de acreditación de un organismo supervisor (art. 41.3 RGPD).

Debe tenerse en cuenta que la posibilidad de supervisar la aplicación de un código de conducta por parte de un organismo externo, distinto de una autoridad de control, no resulta aplicable al tratamiento realizado por autoridades y organismos públicos (art. 41.6 RGPD).

En definitiva, los códigos de conducta están llamados a generar confianza y un elemento clave para alcanzarla es que exista una supervisión por un organismo experto, cualificado y acreditado. Asimismo, para que los códigos de conducta lleguen a implementarse en la práctica de la protección de datos, es preciso que se conozcan las ventajas que supone la adhesión a estos.

6.2. La certificación

El origen de las certificaciones se sitúa en Estados Unidos, donde se empezaron a implementar alrededor de la década de 1990. En Europa se adoptó la idea pero con una filosofía distinta. Así, mientras que en Estados Unidos el modelo es el de una autorregulación total, en el marco del RGPD se trata de un mecanismo establecido bajo el escrutinio directo/indirecto de la APD competente.

El texto originario de la Comisión concedía mucha más iniciativa a la APD, sobre la base del mecanismo de dictar actos delegados. Pero finalmente se ha optado por un modelo más concreto, de modo que una certificación puede ser emitida por un ente certificador (a partir de los criterios adoptados por la APD) o por la propia APD.

A estos efectos, el artículo 42.1 RGPD establece que:

> «Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas».

El artículo 42.2 RGPD señala que:

> «Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento en el marco de transferencias de datos personales a terceros países u organizaciones internacionales. Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados».

La certificación será voluntaria y estará disponible a través de un proceso transparente (art. 42.3 RGPD). En cualquier caso, la certificación no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes (art. 42.4 RGPD).

La certificación será expedida por los organismos de certificación *ex* art. 43, por la autoridad de control competente o por el Comité de conformidad con el artículo 63 (sobre la base de los mecanismos de coherencia). Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos (art. 42.5 RGPD).

Los responsables o encargados que sometan su tratamiento al mecanismo de certificación darán al organismo de certificación o, en su caso, a la autoridad de control competente toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación (art. 42.6 RGPD).

La certificación se expedirá a un responsable o encargado de tratamiento por un periodo máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación (art. 42.7 RGPD).

El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado (art. 42.8 RGPD).

Este sistema de certificación se basa en la existencia de unos organismos de certificación con un nivel adecuado de pericia, que expedirán y renovarán las certificaciones una vez informada la autoridad de control. En cualquier caso, debe garantizarse que dichos organismos de certificación estén acreditados por la autoridad o el organismo adecuado.

Esta acreditación puede ser efectuada por una autoridad de control o por un organismo nacional de acreditación (art. 43.1 RGPD). Para poder ser acreditados, los organismos de certificación deben cumplir una serie de requisitos (art. 43.2 RGPD).

Los organismos de certificación serán responsables de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del Reglamento. La acreditación se expedirá por un periodo máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el RGPD (art. 43.4).

La autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el RGPD (art. 43.7).

Bibliografía

Aparicio Salom, J. (2009). *Estudio sobre la Ley orgánica de protección de datos de carácter personal* (3.ª ed.). Navarra: Aranzadi.

Arenas Ramiro, M. (2013). La validez del consentimiento en las redes sociales on line». En: Rallo Lombarte, A; Martínez Martínez, R. (coords.). *Derecho y Redes sociales* (2.ª ed.). Cizur Menor_ Civitas-Thomson (pags. 159-201).

Boulanger, M.-H.; Poullet, Y.; Léonard, T.; Louveaux, S.; de Terwangne, C. (1997). «La protection des données à caractère personnel en droit communautaire: première partie». *Journal des Tribunaux - Droit Européen* (núm. 40, págs. 121-127).

Boulanger, M.-H.; Poullet, Y.; Léonard, T.; Louveaux, S.; de Terwangne, C. (1997). «La protection des données à caractère personnel en droit communautaire: deuxième partie». *Journal des Tribunaux - Droit Européen* (núm. 41, págs. 145-155).

Boulanger, M.-H.; Poullet, Y.; Léonard, T.; Louveaux, S.; de Terwangne, C. (1997). «La protection des données à caractère personnel en droit communautaire: troisième partie». *Journal des Tribunaux - Droit Européen* (núm. 42, págs. 173-179).

de Asís Roig, A. (2002). «Protección de datos y derecho de las telecomunicaciones». En: J. Cremades; M. A. Fernández-Ordóñez; R. Illescas. *Régimen jurídico de Internet* (págs. 201-228). Madrid: La Ley.

de Miguel Asensio, P. A. (2002). *Derecho privado de Internet* (3.ª ed.). Madrid: Civitas.

De Hert, P.; Papakonstantinou, V. (2016). «The new General Data Protection Regulation: Still a sound system for the protection of individuals?». *Computer Law & Security Review* (vol. 32, núm. 2, págs. 179-194).

Díaz-Romeral, A. (2016). «Los códigos de conducta en el Reglamento General de Protección de Datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* Madrid: Ed. Reus.

Díez-Picazo, L. M. (2005). *Sistema de derechos fundamentales*. Madrid: Civitas.

Díez-Picazo, L. M.; Ponce de León, L. (2007). *Fundamentos del derecho civil patrimonial*. Vol. I: *Introducción: Teoría del contrato* (6.ª ed.). Madrid: Civitas.

Gellert, R.; Gutwirth, S. (2013). «The legal construction of privacy and data protection». *Computer Law & Security Review* (núm. 29, págs. 522-530). http://works.bepress.com/serge_gutwirth/107

Goñi Sein, J. L. (2007). *La videovigilancia empresarial y la protección de datos personales: Estudios de protección de datos*. Madrid: Civitas.

Grimalt Servera, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Comares.

Guerrero Picó, M. C. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Navarra: Aranzadi.

Heredero Higueras, M. (1997). *La directiva comunitaria de protección de los datos de carácter personal*. Bilbao: Aranzadi, Elcano.

Le Métayer, D.; Monteleone, S. (2009). «Automated consent through privacy agents: Legal requirements and technical architecture». *Computer Law & Security Review* (vol. 25, núm. 2, págs. 136-144). http://dx.doi.org/10.1016/j.clsr.2009.02.010

Livingstone, S. (2015). «Children's digital rights». *InterMEDIA* 42 (4/5) (págs. 20-24).

Livingstone, S.; Bulger, M. (2014). «A global research agenda for children's rights in the digital age». *Journal of Children and Media* DOI: 10.1080/17482798.2014.961496.

Mantelero, A. (2014). «The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics». *Computer Law & Security Review* (vol. 30, págs. 643 -660).

Marí, J.; Vilasau, M. (coords.) (2008). *El Reglament de protecció de dades: aspectes clau*. Barcelona: UOC.

Martínez Martínez, R. (2001). *Tecnologías de la información, policía y Constitución*. Valencia: Tirant lo Blanch.

Martínez Martínez, R. y otros (2008). *Comentarios al Reglamento de desarrollo de la LOPD*. Valencia: Tirant lo Blanch.

Marwick, A.; Boyd, D. (2014). «Networked privacy: How teenagers negotiate context in social media». *New Media & Society* (vol. 16, núm. 7, págs. 1051-1067).

Miralles Miravet, S.; Baches Opi, S. (2001). «La cesión de datos de carácter personal: análisis de la legislación vigente y su aplicación a algunos supuestos prácticos». *La Ley* (vol. XXII, núm. 5306).

Oliver Lalana, D. (2002). «El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas». *La Ley* (núm. 5, págs. 1539-1546).

Puyol Montero, J. (2016). «Los Principios del derecho a la protección de datos». En: J. L. Piñar Mañas (dir.). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (págs. 135-150). Madrid: Ed. Reus.

Ribas Alejandro, J. (2000). «Riesgos legales en Internet. Especial referencia a la protección de datos personales». En: J. M. Cendoya Méndez de Vigo (coord.). *Derecho de Internet: Contratación electrónica y firma digital*. Navarra: Aranzadi.

Rodríguez Casal, C.; Loza Corera, M. (2002). «Protección de la privacidad. Aproximación al opt-in/opt-out». *Revista de la Contratación Electrónica* (núm. 23, págs. 3-18).

Suñé Llinás, E. (2000). «Introducción y protección de datos personales». En: C. Almuzara Almaida; E. Suñé Llinás.*Tratado de derecho informático* (vol. I., 2.ª ed.). Madrid: Servicio de Publicaciones; Universidad Complutense. Facultad de Derecho: Instituto de Español de Informática y Derecho.

Téllez Aguilera, A. (2001). *Nuevas tecnologías y protección de datos: Estudio sistemático de la Ley orgánica 15/1999*. Madrid: Edisofer.

Van Alsenoy, B.; Kosta, E.; Dumortier, J. (2013). «Privacy notices versus informational self-determination: Minding the gap». *International Review of Law, Computers & Technology*.

Vizcaíno Calderón, M. (2001). *Comentarios a la Ley orgánica de protección de datos de carácter personal* (1.ª ed.). Madrid: Civitas.

Vilasau, M. (2008). «¿Cómo llegar al consumidor? Entre la protección de datos y la legislación sobre la sociedad de la información». *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 18, págs. 83-101).

Vilasau, M. (2014). «El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido». *IDP. Revista de Internet, Derecho y Política* (núm. 18, págs 16-32). https://libros-revistas-derecho.vlex.es/vid/caso-google-spain-afirmacion-554660626

Zanfir, G. (2013). «Forgetting About Consent: Why the Focus Should Be on "Suitable Safeguards"». *Data Protection Law*. http://ssrn.com/abstract=2261973