Introducción a la protección de datos de carácter personal

PID_00261933

Mònica Vilasau Solana
Miquel Peguera

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Mònica Vilasau Solana

Profesora de Derecho Civil en los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya. Doctora en Derecho por la Universidad de Barcelona. Directora del posgrado de Protección de datos de la UOC.

Miquel Peguera

Profesor agregado de Derecho Mercantil en la Universitat Oberta de Catalunya. Doctor en Derecho por la Universidad de Barcelona. Affiliate Scholar, Center for Internet & Society (Stanford).

Primera edición: febrero 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Diseño: Manel Andreu
Realización editorial: Oberta UOC Publishing, SL

Índice

Introducción

Los datos de carácter personal constituyen la materia prima de la sociedad de la información; algunos autores los califican como el petróleo de la economía digital, de forma que difícilmente los servicios públicos, la sociedad del bienestar o las empresas pueden funcionar sin ellos.

En contra de lo podría parecer, estos datos (cualquier información relativa a una persona identificada o identificable) no pueden utilizarse sin más, sino que deben respetarse unas reglas que disponen cuándo y cómo tratarlos. La preocupación por establecer un marco regulador de la utilización de la información personal surgió con el advenimiento de los primeros ordenadores. En el marco internacional, las primeras iniciativas surgieron en el seno del Consejo de Europa. La Resolución de 1968 sentó las bases de unos principios que regularan el tratamiento de la información personal. A partir de ahí se fueron sucediendo las normas, en los ámbitos internacional, de la UE, nacional y autonómico. En el contexto europeo, la principal norma que regula el tratamiento de la información personal es el Reglamento general de protección de datos (RGPD), Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Esta norma establece las reglas que cualquier tratamiento de la información personal debe cumplir. Sin embargo, existen más disposiciones que regulan aspectos concretos o materias específicas de tratamiento de la información personal. Por ejemplo, la Directiva 2016/680, relativa al tratamiento para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

A nivel estatal, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales (LOPDGDD), sustituye a la Ley Orgánica de Protección de datos de carácter personal (LOPD) de 1999, adapta el derecho español al marco establecido por el RGPD y desarrolla algunos aspectos de este Reglamento que se dejan a las legislaciones nacionales. Además de esta Ley, existe un abanico de disposiciones que, de forma directa o indirecta, afectan al tratamiento de la información personal. Entre otras, cabe destacar: la Ley 9/2014, de 9 de mayo, general de telecomunicaciones, o la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Asimismo, deben destacarse normas autonómicas como la Ley 32/2010 de 1 de octubre, de la Autoridad Catalana de Protección de Datos; la Ley 2/2004 de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos, o bien la Ley 1/2014, de 24 de junio, de transparencia pública de Andalucía.

Este módulo pretende ser una introducción a las reglas básicas que permiten tratar la información personal, que luego se concretarán en sectores específicos: comercio electrónico, banca, salud o relaciones laborales. Se trata, en definitiva, de adquirir unos conocimientos básicos, la cartografía que permitirá posteriormente navegar en las normas específicas que existen en distintos niveles. Estos conocimientos deberán aplicarse a realidades que van surgiendo y que, en ocasiones, no tienen aún una regulación específica o es muy incipiente. Entre otros supuestos, el internet de las cosas, las redes sociales, la computación en la nube, el *big data* o el creciente recurso a la robótica.

En los siguientes apartados se analiza, en primer lugar, qué es un dato personal, los principios que deben regir el tratamiento de la información personal, el ámbito subjetivo (quién trata los datos y quién es el sujeto afectado) y los derechos y deberes de cada uno de estos protagonistas. Además, se dedica un epígrafe específico al derecho al olvido, en la medida que en el momento de adoptarse el RGPD se puso mucho énfasis en el mismo.

El derecho al olvido constituye una manifestación concreta de los derechos de supresión o de oposición al tratamiento. Una aplicación específica de este derecho se refiere a la posibilidad de exigir a los buscadores de internet que eliminen determinados resultados cuando las búsquedas se llevan a cabo a partir del nombre de una persona. El TJUE afirmó este derecho en su famosa sentencia del caso Google Spain, de 13 de mayo de 2014. Desde entonces, se ha ido aplicando por parte de los buscadores y lo han reconocido las autoridades de protección de datos y los tribunales. Con su aplicación práctica, se han ido consolidando algunos criterios de interpretación, pero quedan aún aspectos discutidos donde la jurisprudencia no es homogénea.

Objetivos

1. Saber cuándo resulta aplicable el RGPD.

2. Aprender e identificar los principios de protección de datos.

3. Entender el concepto de bases legales que permiten un tratamiento de datos.

4. Identificar los sujetos que intervienen en un tratamiento y conocer sus derechos y obligaciones.

5. Conocer los mecanismos de *soft law*.

6. Aprender cuáles son los derechos del afectado y las limitaciones a los mismos.

7. Saber el régimen jurídico básico de las transferencias internacionales de datos y el régimen de responsabilidades y sanciones.

1. El Reglamento general de protección de datos

Mònica Vilasau Solana

1.1. ¿Cuándo resulta aplicable el RGPD?

1.1.1. En función del ámbito material

El artículo 1.1 RGPD 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».

Asimismo, según dispone el artículo 2.1 RGPD:

> «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».

A continuación, profundizamos en los elementos mencionados para conocer el alcance de la norma:

1) Personas físicas:

Las personas físicas son las únicas objeto de la tutela que proporciona el RGPD. Quedan excluidas de dicha protección las personas jurídicas: una empresa, una asociación, una fundación o bien la Administración pública.

El RGPD no contempla los datos relativos a las personas fallecidas. El artículo 3 de la LO 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), hace referencia a esta cuestión.

LOPDGDD

La LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) se publicó en el BOE núm. 294 de 6 de diciembre de 2018.

2) Dato personal:

> «... toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4.1 RGPD).

Por lo tanto: (a) toda información (b) relativa a una persona física identificada o identificable.

a) Toda información: tanto en un sentido objetivo (hechos) como subjetivo (opiniones). Tanto información sensible (datos de salud) como la que no lo es. Tampoco es relevante el hecho de que sea hecha pública, ni es necesario que

sea «secreta»; por lo tanto, puede tratarse de información conocida por muchos (nombre, dirección postal o correo electrónico...). Es indiferente a qué ámbito afecta: al personal o al profesional. Tampoco va a tener importancia el formato o el soporte en el cual se contenga la información: alfabético, numérico, gráfico, fotográfico, sonoro o en soporte papel. Para el derecho a la protección de datos no hay datos que carezcan de interés, ni que sean inocuos.

b) Relativa a una persona **física identificada o identificable**: la cuestión es determinar si, a partir de la información disponible, es posible distinguir a una persona de entre un grupo. En cuanto a identificadores, el artículo 4.1 RGPD hace referencia a:

> «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».

Las normas del RGPD no serían aplicables a los datos anónimos. Este supuesto debe distinguirse de la **seudonimización** (art. 4.5 RGPD), en que los datos personales se tratan de modo que no puedan atribuirse a una persona concreta sin utilizar información adicional. Sin embargo, en el caso de datos seudonimizados, siguen siendo datos personales y resulta aplicable el RGPD.

En cuanto al término *datos personales*, debe tenerse en cuenta:

a) La legislación distingue, entre los datos personales, unos que califica como *categorías especiales de datos* (art. 9 RGPD) y que tradicionalmente se consideran como datos sensibles. Se trata de los datos 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 la orientación sexual de una persona física» (art. 9.1 RGPD).

El tratamiento de estos datos está sujeto, en algunos casos, a un régimen específico (por ejemplo, respecto al consentimiento).

b) Otra categoría que se debe tener presente es la relativa a los datos respecto de condenas e infracciones penales, que tienen unas peculiaridades en cuanto a su tratamiento (art. 10 RGPD).

También debe tenerse en cuenta:

c) Datos genéticos: art. 4.13 RGPD.

d) Datos biométricos: art. 4.14 RGPD.

Consultas recomendadas

Podéis consultar los siguientes dictámenes del Grupo del artículo 29:

Dictamen 4/2007 (WP 136), de 20 de junio de 2007, sobre el concepto de datos personales.

Dictamen 5/2014 (WP 216), de 10 de abril, sobre técnicas de anonimización.

3) 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 RGPD).

Se incluye tanto el tratamiento automático como el no automático; en este último caso, en la medida en que los datos sean destinados a ser incluidos en un fichero.

Ejemplos de tratamientos efectuados en papel a los que resulta aplicable el RGPD:

Resultados médicos, currículum vitae en formato papel, la hoja salarial, expedientes de clientes, siempre que los datos consten en un fichero o estén destinados a ser incluidos (considerando 15 RGPD), por ejemplo, porque están ordenados alfabéticamente.

Debe tenerse en cuenta que determinados tratamientos, a pesar de afectar a datos personales, quedan excluidos del ámbito de aplicación del RGPD, como se explica más adelante.

1.1.2. En función del ámbito territorial

Según dispone el artículo 3.1 RGPD:

«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».

El criterio que determina la aplicación de la norma europea es el criterio de la existencia de un establecimiento en la UE, con independencia del lugar en el que se lleva a cabo el tratamiento.

Pero el RGPD va más allá y dispone la aplicación del mismo incluso cuando el responsable del tratamiento (RT) no esté establecido en la Unión en dos supuestos importantes (art. 3.2 RGPD):

1) cuando se ofrezcan bienes o servicios a los interesados en la Unión, con independencia de si se requiere o no pago;

2) cuando se controla el comportamiento de los afectados, en la medida que este tenga lugar en la Unión.

Se trata de los supuestos en que empresas (RT) que tienen su sede fuera de la UE y, por lo tanto, en principio no estarían sujetas al RGPD, ofrecen bienes o servicios (por ejemplo, de mensajería, de acceso a contenidos digitales), o venden bienes a interesados en la Unión.

Por otro lado, se hace referencia a la observación del comportamiento de los interesados, concretamente, si las personas físicas son objeto de un seguimiento en internet, se elaboran perfiles, se analizan o predicen las preferencias personales, comportamientos y actitudes de los afectados (por ejemplo, se llevan a cabo prácticas de publicidad personalizada).

La finalidad de esta disposición es que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del RGPD. Para determinar la aplicación de este, se tiene en cuenta si el RT proyecta ofrecer servicios a interesados en uno o varios de los estados miembros de la Unión. Este extremo, como ha dictaminado el TJUE, se analiza teniendo en cuenta elementos como la lengua de la página web desde la que se ofrece el bien o servicio, la moneda utilizada en el pago o el lugar de la entrega de los bienes.

1.2. ¿Cuándo no se aplica el RGPD?

El RGPD no se aplica a determinados tratamientos contemplados en el artículo 2.2 RGPD.

La excepción más importante es la que se conoce como la «excepción doméstica», de forma que el RGPD no se aplica al tratamiento de datos personales «efectuado por una persona física en el ejercicio de actividades *exclusivamente personales o domésticas*» (art. 2.2.c RGPD).

> «Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas» (cdo. 18 RGPD).

Ello tiene una serie de consecuencias respecto a los usuarios de las redes sociales porque, cuando se trata de un individuo (particular) que las utiliza para relacionarse con sus amigos o familiares, el tratamiento de datos personales que lleve a cabo queda excluido del ámbito de aplicación del RGPD y, por lo tanto, de las obligaciones que se establecen en él. En cambio, lógicamente, el responsable del tratamiento, el responsable de dicha red social, sí que queda bajo el ámbito de aplicación del RGPD.

En cambio, si se trata de una empresa o asociación que hace uso de una red social para promocionar sus servicios (aunque sean gratuitos), sí resulta aplicable el RGPD.

1.3. Principios de protección de datos (art. 5 RGPD)

Los primeros textos normativos que regulaban el tratamiento de la información personal recogieron unos principios que establecieron unas directrices sobre cómo tratar los datos personales. Estos principios se han ido consolidando y constituyen las líneas maestras del tratamiento de la información personal.

El artículo 5 RGPD recoge cuáles son los principios de protección de datos. Constituye una novedad del RGPD la introducción del principio de responsabilidad proactiva (art. 5.2 RGPD). A continuación, se enumeran y analizan someramente dichos principios.

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")».

Estos términos están muy interconectados. 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.

El deber de informar se desarrolla en los artículos 12, 13 y 14 RGPD. El principio de licitud se concreta en el artículo 6 RGPD. Este precepto regula los supuestos que permiten que se lleve a cabo un tratamiento de datos.

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")».

Esto es, al recabar los datos, deberá determinarse la finalidad, por ejemplo, para llevar a cabo una campaña publicitaria de coches. En la medida que el afectado ha sido informado y ha dado el consentimiento para esta finalidad, los datos no podrían utilizarse para pedirle que se haga socio de una ONG.

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.

Por ejemplo, si se recogen datos para una tarjeta de acceso a un gimnasio, existen datos como el nombre y apellido, el número de cuenta donde domiciliar el pago, la dirección postal, la dirección de correo electrónico y el teléfono que puede considerarse adecuado solicitar. Sin embargo, no cumpliría con el principio de minimización pedir datos relativos a lugares preferidos de vacaciones o convicciones religiosas. En todo caso, si se solicitaran estos otros datos, debería quedar muy claro que el afectado no tiene por qué proporcionarlos para hacerse socio de un gimnasio.

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 (art. 19 en relación con el art. 17 RGPD).

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")».

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).

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")».

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.

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")».

La novedad que introduce el RGPD es la referencia a «capaz de demostrarlo»; ello es lo que se conoce como *accountability*, 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.

En definitiva, el RGPD establece sobre el RT la carga de adoptar determinadas medidas y estar en condiciones de poderlo demostrar.

1.4. Bases legales que permiten el tratamiento de DCP (art. 6 RGPD)

Para poder tratar los datos personales es preciso que exista una base legal, una razón que lo justifique. Esto es, en el marco de la UE, a diferencia de otros ordenamientos jurídicos (como el de Estados Unidos), no pueden tratarse los datos sin más porque a alguien le interese o porque esta sea su voluntad.

El artículo 6 RGPD enumera cuáles son estos supuestos que permiten tratar los datos, de modo que si no se da una de las circunstancias previstas en este artículo, no se pueden tratar los datos.

Según dispone el artículo 6.1 RGPD, «el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones [...]»:

1) el «consentimiento» del interesado;

2) «la ejecución de un contrato en el que el interesado es parte»;

3) el «cumplimiento de una obligación legal»;

4) «proteger intereses vitales del interesado o de otra persona física»;

5) el «cumplimiento de una misión realizada en interés público/ejercicio de poderes públicos»;

6) «la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero».

Lo más relevante del artículo 6 RGPD es que, sin uno de estos supuestos enumerados, no es posible llevar a cabo un tratamiento, si bien es cierto que existen muchos supuestos y quedarán pocos casos fuera de ellos.

Sin embargo, el hecho que concurra uno de estos supuestos es necesario, aunque no suficiente. Para tratar los datos personales es necesario, además, que se cumpla siempre con los principios de protección de datos ya expuestos (art. 5 RGPD).

Por lo tanto, para poder tratar los datos, es necesario cumplir con el artículo 5 + el artículo 6 RGPD.

Así lo estableció el TJUE, entre otros, en la sentencia de 24 de noviembre de 2011, en el caso ASNEF (C-468/10 y C-469/10).

1.4.1. El consentimiento

Características del consentimiento

El artículo 4.11 RGPD proporciona una definición del 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».

Consulta recomendada

Al respecto, ved el art. 6 LOPDGDD, que lleva por título *Tratamiento basado en el consentimiento del afectado*.

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 solicite su consentimiento. Sin embargo, el hecho de proporcionar el consentimiento se ha convertido, en muchas ocasiones, en algo automático. Ello comporta que el consentimiento se proporciona la mayoría de las veces de forma automática, sin la plena conciencia y voluntad del afectado. Por ello, deben adoptarse cautelas respecto al recurso generalizado al consentimiento.

> Pensad en las numerosas ocasiones en 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. Se da el consentimiento de una forma mecánica, sin leer toda la información proporcionada, y con la única finalidad de obtener cuanto antes el servicio o el bien deseado.

La exteriorización del consentimiento

El artículo 4.11 RGPD determina que la manifestación de voluntad debe ser inequívoca, mediante una declaración o una clara acción afirmativa. Por lo tanto, se rechaza el silencio como forma de obtener el consentimiento del afectado.

Por ejemplo, el afectado recibe una comunicación en que se le propone 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 consiguiente, en caso de que una persona no manifieste nada ante la solicitud de tratar los datos que le afectan, ello no comportará en ningún caso que consienta el tratamiento.

Categorías especiales de datos. Como ya se ha indicado al analizar el término *dato*, la gran mayoría de textos legales que regulan el tratamiento de datos personales establece una distinción entre tipos de datos, de modo que se considera que determinada información debe gozar de una mayor protección. El RGPD distingue aquellos que califica de «categorías especiales de datos». Para tratar estos datos, se exige que el consentimiento sea *explícito* (art. 9.2.a RGPD).

Condiciones para el otorgamiento del consentimiento

1) «Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales» (art. 7.1 RGPD). En definitiva, corresponde al RT acreditar la existencia del consentimiento.

2) Cuando se pida el consentimiento para tratar datos, junto con otros asuntos, deberá distinguirse claramente la solicitud para el tratamiento de datos de los otros supuestos. Debe emplearse «un lenguaje claro y sencillo» (art. 7.2 RGPD).

Este precepto determina que, entre las distintas cláusulas de un formulario o documento, se identifiquen y separen claramente aquellas relativas al tratamiento de los datos personales. La finalidad es que el sujeto pueda conocer claramente aquello que se solicita y consentir una cláusula y, por ejemplo, rechazar otra.

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

3) «El interesado tendrá derecho a retirar su consentimiento en cualquier momento» (art. 7.3 RGPD).

4) La ejecución de un contrato o la prestación de un servicio no podrá vincularse a la obtención de datos que no son necesarios para proporcionar dicho bien o servicio (art. 7.4 RGPD). Con ello se pretende garantizar que el consentimiento sea libre, no condicionado al hecho de que, si no se proporcionan determinados datos, no se obtendrá un bien o servicio.

Esto es, en la contratación de un bien o servicio, obviamente son necesarios determinados datos que deberán pedirse/proporcionarse (por ejemplo, nombre, dirección, DNI), pero no podrán exigirse otros datos no necesarios para el contrato en cuestión (por ejemplo hábitos alimentarios o si el afectado practica una determinada religión).

> Si se compra un billete de avión, deben darse los datos relativos al nombre, dirección de correo electrónico o DNI. Pero no podría supeditarse la emisión del billete al hecho de que el afectado proporcione datos sobre sus hábitos alimenticios o creencias religiosas.

El consentimiento de los menores

El RGPD hace unas referencias específicas al tratamiento de datos de los menores.

El artículo 8 RGPD dispone que, para tratar los datos personales de un menor de edad, en relación con la oferta de servicios de la sociedad de la información, si se quiere obtener el consentimiento del menor, será preciso que este tenga como mínimo dieciséis años.

> «Si el niño es menor de dieciséis 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» (art. 8.1 RGPD).

Sin embargo, «los estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años» (art. 8.2 RGPD). Este es el caso del Estado español, que en el artículo 7 de la LOPDGDD determina, como regla general, que «el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años» (art. 7.1 PLOPD). En el caso de menores de 14 años, el tratamiento de los datos, «fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela» (art. 7.2 LOPDGDD).

El RT deberá hacer los:

> «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» (art. 8.2 RGPD).

1.4.2. El interés legítimo (art. 6.1.f RGPD)

1) Para determinar qué intereses prevalecen, deben tenerse en cuenta las expectativas razonables de los interesados.

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

a) cuando exista una relación entre afectado y responsable: por ejemplo si «el interesado es cliente o está al servicio del responsable» (cdo. 47 RGPD);

b) «tratamiento de datos con fines de mercadotecnia directa» (cdo. 47 RGPD);

c) la transmisión de datos entre «responsables que forman parte de un grupo empresarial» (cdo. 48 RGPD);

d) «para garantizar la seguridad de la red y de la información» (cdo. 49 RGPD).

3) «La existencia de un interés legítimo requeriría una evaluación meticulosa» (cdo. 47 RGPD).

4) Esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones (art. 6.1.f. *in fine* y considerando 47 RGPD).

5) 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.

Lecturas recomendadas

Ved el Dictamen del Grupo del artículo 29, 6/2014 (WP 217), de 9 de abril de 2014, sobre el concepto de interés legítimo.

Ved también la STJUE en el caso ASNEF (ya citado) y la STJUE caso Google, 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).

1.5. Los sujetos que participan en el tratamiento de datos

En cuanto al ámbito subjetivo, cabe distinguir entre los sujetos que **participan en el tratamiento** y aquellos otros que lo **supervisan** (las autoridades de protección de datos y el DPO).

1.5.1. Los sujetos que tratan los datos personales

En todo tratamiento de datos, los sujetos que siempre participarán del mismo son: el responsable del tratamiento y el afectado o interesado. Asimismo, en la mayoría de los casos, también se encontrará el encargado o subencargado y los destinatarios de los datos (o terceros).

Responsable del tratamiento (RT)

El artículo 4.7 RGPD establece que el «responsable del tratamiento» o «responsable» es «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**».

Por lo tanto, lo que caracteriza al RT es el hecho de tomar una decisión, esto es, determinar los fines y medios del tratamiento.

En el caso en que exista más de un RT, los sujetos «serán considerados corresponsables del tratamiento» (art. 26 RGPD).

En cuanto a las funciones que lleva a cabo el RT, estas se pueden agrupar teniendo en cuenta, básicamente, tres momentos: cuando se inicia o proyecta el tratamiento, cuando se efectúa el mismo y cuando finaliza.

En el marco anterior al RGPD, antes de iniciar un tratamiento debía notificarse a la autoridad de control. En el marco del RGPD, puede procederse al tratamiento, si bien el RT debe tomar una serie de prevenciones y asegurarse de que cumple con la normativa y deberá poder acreditar que ello es así (principio de responsabilidad proactiva, *ex* art. 5.2 RGPD).

El RT no tiene un cheque en blanco para tratar los datos de cualquier forma, sino que, antes de llevar a cabo un tratamiento, deberá valorar, pensar, estudiar la conveniencia de este y la forma de llevarlo a cabo de acuerdo con la normativa y, especialmente, de acuerdo con los principios de protección de datos.

Cuando sea necesario, deberá llevar a cabo una valoración del impacto que el tratamiento puede comportar para la privacidad (*privacy impact assessment*) (art. 35 RGPD) e implementar, desde un primer momento, medidas de privacidad basadas en el diseño (art. 25 RGPD) y, en según qué casos, realizar una consulta previa a la autoridad de control (art. 36 RGPD).

Por otro lado, será preciso que lleve a cabo un «registro de las actividades de tratamiento» (art. 30 RGPD).

Para ello, deberá dotarse de los medios técnicos y personales adecuados. Y durante el tratamiento, también deberá adoptar una serie de garantías y especialmente dotarse de las medidas de seguridad necesarias.

El conjunto de las obligaciones que corresponden al RT vienen definidas por esta nueva perspectiva a la que se ha hecho referencia de la responsabilidad proactiva.

En definitiva, el responsable del tratamiento deberá asegurarse de que cumple con la normativa de protección de datos y estar en condiciones de poderlo demostrar.

En consecuencia, todo ello implica:

1) Antes de iniciar el tratamiento:

a) verificar que se cumple con la normativa de protección de datos,

b) respetar los principios de protección de datos,

c) verificar si el tratamiento es lícito (existe un fundamento legal para efectuarlo),

d) cuando sea necesario, llevar a cabo una valoración del impacto que puede tener, respecto a la privacidad, el tratamiento de datos que se pretende realizar (*privacy impact assessment*),

e) cuando proceda, realizar la consulta previa a la autoridad de protección de datos,

f) dotarse de los medios técnicos y personales adecuados, y

g) en caso de elegir a encargados del tratamiento, realizarlo con la debida diligencia y formalizar un contrato u otro negocio jurídico.

El RGPD también establece el principio de *data protection by design* y *data protection by default*. Deben establecerse medidas tecnológicas que favorezcan la privacidad desde el primer momento de la concepción de un producto/servicio.

2) Durante el tratamiento:

a) adoptar una serie de garantías,

b) llevar un registro de las actividades de tratamiento (art. 30.1 RGPD),

c) dotarse de los medios técnicos y personales adecuados,

d) si no se ha hecho en la fase anterior, elegir a los encargados del tratamiento con la debida diligencia y suscribir un negocio jurídico,

e) adoptar las medidas de seguridad necesarias,

f) cumplir con las obligaciones propias del responsable,

g) dar respuesta al ejercicio de los derechos por parte del afectado/interesado, y

h) poder demostrar que se cumple con la normativa (principio de responsabilidad).

3) Al finalizar el tratamiento:

a) determinar si deben suprimirse los datos o bien limitarse el tratamiento de estos,

b) hacer frente al posible ejercicio de acciones por parte del afectado/interesado,

c) valorar si se pone fin a la relación con el ET y valorar cómo se pone fin a esta, y

d) aplicar medidas técnicas y organizativas para demostrar que el tratamiento es conforme con el reglamento.

Para ello, ¿qué elementos debe tener en cuenta? Debe tenerse «en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento» (art. 24.1 RGPD) y, también, «el estado de la técnica» y «el coste de la aplicación» de dichas medidas (art. 25.1 RGPD).

Entre las obligaciones concretas del responsable del tratamiento, destacan las siguientes:

1) Llevar un registro (art. 30 RGPD), que deberá contener la información indicada en el artículo 30.1 RGPD. El registro debe constar por escrito (art. 30.3 RGPD) y ponerse a disposición de la autoridad de control (art. 30.4 RGPD).

Estas obligaciones «no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas a menos que el tratamiento pueda entrañar un riesgo» (art. 30.5 RGPD).

2) Cooperar con la autoridad de control cuando esta lo solicite (art. 31 RGPD).

3) Deberes relacionados con la seguridad. El RT debe identificar los riesgos del tratamiento para establecer mecanismos adecuados de procesamiento de la información.

Se tiene en cuenta un doble nivel de aproximación desde el riesgo. Algunas obligaciones solo resultan aplicables a las actividades que comportan un elevado riesgo. Se establecen obligaciones como la de llevar a cabo un *data protection impact assessment*, el deber de notificar a los afectados las violaciones de seguridad de los datos o la consulta previa a las autoridades de protección de datos (APD), de las que hablaremos más adelante.

El RGPD establece un conjunto de pautas en relación con el nivel de riesgo que el tratamiento de datos personales puede suponer.

Entre las medidas que establece el artículo 32 RGPD, cabe destacar:

> «a) la seudonimización y el cifrado de datos personales;
>
> b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
>
> c) la capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida [...]
>
> d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento».

Una novedad introducida por el RGPD es el deber de notificar las violaciones de seguridad (arts. 33 y 34 RGPD). Se distingue entre:

a) el deber de notificar «una violación de la seguridad a la autoridad de control» (art. 33) y

b) la «comunicación de una violación de la seguridad al interesado» (art. 34).

En cuanto a la notificación de la violación a la autoridad de control:

a) El RT la notificará a la autoridad de control sin dilación indebida, a más tardar 72 horas después de tener constancia del incidente (a menos que dicha violación no constituya un riesgo para los derechos y las libertades de las personas).

b) La notificación deberá contener la información que establece el artículo artículo 33.4 RGPD.

El RT «documentará cualquier violación de la seguridad de los datos personales» (art. 33.5 RGPD).

El otro supuesto lo constituye la comunicación de la violación de la seguridad al interesado.

Esta comunicación debe llevarse a cabo cuando sea probable que «entrañe un alto riesgo para los derechos y libertades de las personas» (art. 34.1 RGPD).

4) La evaluación de impacto relativa a la protección de datos. En determinados supuestos, debe llevarse a cabo una evaluación del impacto relativa a la protección de datos (art. 35 RGPD).

Especialmente en determinados casos:

> «a) evaluación sistemática y exhaustiva de aspectos personales [...], como la elaboración de perfiles [...]; b) tratamiento a gran escala [...] c) observación sistemática a gran escala de una zona de acceso público».

La noción de evaluación de impacto relativa a la protección de datos (art. 35 RGPD) es más conocida por sus siglas en inglés PIA (*privacy imact assessment*). El PIA debe hacerse antes de llevar a cabo el tratamiento. Existe la posibilidad de llevar a cabo PIA por sectores (tratamientos parecidos que presentan un riesgo similar).

5) Consulta previa. En determinados casos, debe llevarse a cabo una consulta previa (art. 36 RGPD).

6) Designación del encargado del tratamiento (ET). El RT, según determina el artículo 28 RGPD, elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas. El artículo 28.1 RGPD establece una obligación general de diligencia en la selección del encargado.

El encargado del tratamiento

El encargado del tratamiento (ET) o «encargado» es «la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento» (art. 4.8 RGPD). Por lo tanto, no es el sujeto que toma la iniciativa de tratar los DCP.

El artículo 28.1 RGPD dispone que el RT elegirá un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD.

La relación entre RT y ET debe regirse por un contrato u otro acto jurídico que vincule al encargado respecto al responsable (art. 28.3 RGPD), que necesariamente debe establecer «el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable».

El artículo 28.3 RGPD dispone cuál debe ser el contenido de dicho contrato o acto jurídico, esto es, cómo el ET deberá tratar los datos personales. En cualquier caso, el ET no es un mero ejecutor de las órdenes del RT, puesto que,

como dispone el artículo 28.3 *in fine*, «el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el Reglamento u otras disposiciones».

Cada encargado «llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable» (art. 30.2 RGPD). Dicho registro constará por escrito y el ET lo pondrá «a disposición de la autoridad de control que lo solicite» (art. 30.4 RGPD).

La obligación de llevar el registro no será exigible a determinadas empresas u organizaciones (art. 30.5 RGPD).

La posibilidad de que el ET recurra a otro ET (en definitiva, subcontrate sus funciones) está especialmente contemplada en el RGPD. Ello es posible si el ET tiene la autorización previa por escrito, específica o general, del responsable. Si un ET infringe el reglamento, «al determinar los fines y medios del tratamiento», será considerado RT (art. 28.10).

Cualquier sujeto que trate datos personales debe hacerlo con una determinada diligencia, sobre la base de los artículos 5.1.f) y 29 RGPD.

En definitiva, en cuanto a la relación entre el RT y el ET, debe tenerse en cuenta lo siguiente:

1) El ET realiza un tratamiento por cuenta de un responsable.

2) El RT debe elegir a quien ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

3) El ET no puede recurrir a otro encargado sin autorización previa y por escrito del RT.

4) La relación entre el RT y el ET se rige por un contrato o acto jurídico, que debe establecer, entre otros aspectos: el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales tratados, las categorías de interesados, y las obligaciones y derechos del RT.

5) El contrato o acto jurídico constará por escrito, inclusive en formato electrónico.

6) El fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado salvo que así lo haya previsto el RT.

7) El ET debe informar al responsable si, en su opinión, una instrucción infringe el RGPD.

Otros sujetos

El RGPD contempla la participación en el tratamiento de otros sujetos. El artículo 4.9 RGPD hace referencia a la figura del **destinatario**.

Destinario es:

> «La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el derecho de la Unión o de los estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento».

Los sujetos afectados por el tratamiento

Se trata de los sujetos afectados o interesados, a los que afecta el tratamiento de datos.

Entre las definiciones que se recogen en el artículo 4 RGPD, no hay una que haga referencia al interesado o afectado. En cualquier caso, se trata de la persona a quien hace referencia el tratamiento. Para el ámbito de aplicación del RGPD, ya se ha subrayado que se trata en todo caso de un sujeto, persona física, y que por lo tanto el RGPD no resulta aplicable a las personas jurídicas.

1.5.2. La supervisión del tratamiento

En este subapartado se analizan dos aspectos: las autoridades de protección (APD) y el delegado de protección de datos (DPD).

Las autoridades de protección de datos

Las autoridades de protección (APD), según el esquema del RGPD, constituyen un pilar básico en la implementación del RGPD y este refuerza su labor. Se hallan reguladas en el capítulo VI del RGPD, que establece las normas básicas de actuación, su competencia, funciones y poderes, y en el capítulo VII, que hace referencia a los mecanismos de cooperación y de coherencia.

> Según el artículo 4.21 RGPD, la «autoridad de control» es «la autoridad pública independiente establecida por un estado miembro con arreglo a lo dispuesto en el artículo 51».

Junto con las autoridades de protección, se crea el Comité Europeo de Protección de Datos (arts. 68 a 76), que sustituye al Grupo del artículo 29, creado precisamente por el artículo 29 Directiva 95/46 y que ha desarrollado una encomiable labor de interpretación y de aclaración del articulado de la directiva.

Un aspecto al que ha tratado de dar respuesta el RGPD es el cada vez mayor tratamiento transfronterizo de DCP (dentro de la UE). Para ello, el RGPD ha previsto una serie de mecanismos, y uno de ellos es el relativo a la coordinación entre autoridades de protección de datos. De este modo, las autoridades tienen determinados poderes de investigación en otros estados.

En los supuestos en que, debido al tratamiento transfronterizo de datos, puedan resultar competentes distintas APD, deberá determinarse cuál de ellas es la autoridad de control principal.

El RGPD establece un complejo sistema para determinar qué autoridad es la competente para decidir un asunto, en virtud de si existen puntos de conexión en un solo estado o en múltiples estados. También se establece un mecanismo de cooperación entre autoridades (arts. 60 a 62).

Consulta recomendada

En cuanto a la autoridad de control interesada, ved artículo 4.22 RGPD.

En la medida en que las APD toman decisiones que pueden afectar a la aplicación uniforme del reglamento, se establece un procedimiento de coherencia (arts. 63 a 67).

El Comité Europeo de Protección de Datos

El artículo 29 DPD creó un grupo de protección de las personas respecto al tratamiento de datos personales, denominado Grupo del artículo 29, que tiene carácter consultivo e independiente. El artículo 68 RGPD crea el Comité Europeo de Protección de Datos, identificado como «Comité», como organismo de la Unión, que gozará de personalidad jurídica y que sustituye al Grupo del artículo 29.

En el ordenamiento jurídico español, se hallan distintas autoridades de protección de datos: la Agencia Española de Protección de Datos, la Autoritat Catalana, la Agencia Vasca y el organismo andaluz para la transparencia.

El delegado de protección de datos

Otra de las novedades introducidas en el RGPD es la figura del delegado de protección de datos (DPD). En el caso de las AA. PP., su designación será obligatoria. En cuanto a las empresas privadas, dependerá del tipo de tratamiento que lleven a cabo.

Según dispone el artículo 37 RGDP, «el responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que»:

1) «el tratamiento lo lleve a cabo una autoridad u organismo público»;

2) las actividades principales del RT o ET «consistan en operaciones de tratamiento que [...] requieran una observación habitual y sistemática de interesados a gran escala», por ejemplo, la videovigilancia;

3) «consistan en el tratamiento a gran escala de categorías especiales de datos».

> «El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39» (art. 37.5).

El RGPD no regula qué tipo de titulación debe tener el sujeto que desempeñe las funciones de DPD. Por lo tanto, cualquier sujeto que tenga las cualidades y conocimientos exigidos en el RGPD podrá ejercer esta labor profesional. Sin embargo, la AEPD, para dotar de mayor seguridad y facilitar la acreditación de estos conocimientos, ha establecido un sistema de certificación de personas.

El artículo 38 RGPD regula la posición del delegado de protección de datos dentro de la administración, empresa u organización. Deberá garantizarse que «participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales». El DPD tiene unas funciones mínimas, recogidas en el artículo 39.1 RGPD: informar y asesorar, «supervisar el cumplimiento de la normativa, actuar como punto de contacto con la autoridad de control y cooperar con esta».

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

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 en la realización de PIA (*privacy imact assessment*), a los que ya se ha hecho referencia, la adopción de códigos de conducta y la implementación de mecanismos de certificación.

Estos mecanismos constituyen herramientas para hacer efectivo el principio de responsabilidad proactiva.

Los **códigos de conducta** tienen como objetivo conducir a la correcta aplicación del RGPD.

Las **certificaciones, sellos y marcas** ayudan a demostrar que se está cumpliendo con las disposiciones del RGPD (se trata, en definitiva, de mecanismos de *compliance*), esto es, de acreditar el cumplimiento del RGPD.

Las organizaciones independientes de certificación, o bien las APD o el CEPD (Comité Europeo de Protección de Datos), certificarán las empresas y monitorizarán el cumplimiento adecuado de la certificación. Esto es, llevarán a cabo

un seguimiento de que la empresa en cuestión cumple y se adecua a aquello que ha sido certificado. Esto también supone una novedad del RGPD respecto a la directiva.

1.6.1. Los códigos de conducta

Los códigos de conducta constituyen un mecanismo de autorregulación (*self-regulatory instrument*), cuya eficacia depende en parte del nivel de ratificación que reciben por parte de las APD u otras autoridades.

Según dispone el artículo 40.1 RGPD, «las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar dichos códigos» con objeto de especificar la aplicación del RGPD.

1.6.2. La certificación

En el marco del RGPD, se trata de un mecanismo establecido bajo el escrutinio directo/indirecto de la APD competente. Una certificación puede ser emitida por un ente certificador (en función de los criterios adoptados por la APD), o puede ser emitido (dicho certificado) por la propia APD.

> «La certificación será voluntaria y estará disponible a través de un proceso transparente» (art. 42.3 RGPD).

La certificación no limitará la responsabilidad del RT o ET 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, en virtud del presente artículo, será expedida por los organismos de certificación *ex* artículo 43, por la autoridad de control competente o por el Comité de conformidad con el artículo 63 (art. 42.5 RGPD).

1.7. Los derechos del afectado

El capítulo III del RGPD se dedica a los derechos del interesado. Dicho capítulo se divide en cinco secciones, que hacen referencia a «transparencia y modalidades» (sección 1); «información y acceso a los datos personales» (sección 2); «rectificación y supresión» (sección 3); «derecho de oposición y decisiones individuales automatizadas» (sección 4) y «limitaciones» (sección 5).

Entre los derechos reconocidos, cabe subrayar que se recogen nuevos derechos: el derecho a la limitación del tratamiento y el derecho a la portabilidad. Asimismo, el derecho de cancelación pasa a denominarse derecho de supresión. Por otro lado, el denominado derecho al olvido se menciona en el artículo 17 RGPD.

1.7.1. Transparencia y modalidades

La sección 1 del capítulo III lleva por rúbrica «transparencia y modalidades».

La información que debe proporcionarse constituye un presupuesto para poder ejercer otros derechos como el derecho de rectificación, supresión, o bien oponerse a tratamientos que comporten decisiones individuales automatizadas.

La transparencia se regula en el artículo 12. La comunicación al interesado debe hacerse:

> «en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño» (art. 12.1 RGPD).

El RT facilitará al interesado la información relativa a sus actuaciones sobre la base de la solicitud presentada por el afectado. En todo caso, en el plazo de un mes debe dar respuesta al afectado, plazo que puede prorrogarse otros dos meses más en caso necesario, informando al interesado de dichas prórrogas (art. 12.3 RGPD). La información facilitada por regla general será gratuita.

En cuanto al contenido concreto de la información que debe proporcionarse al interesado/afectado, el RGPD distingue en función de si los datos se han obtenido del afectado o no es así.

Supuestos en que los datos se obtienen del afectado (art. 13 RGPD). Se dispone que el contenido de la información debe hacer referencia a:

1) El ámbito subjetivo (RT y DPD), destinatarios o categorías de destinatarios e intención de transferir los datos a un tercer país u organización internacional.

2) En cuanto al contenido concreto, un aspecto relevante es proporcionar información de los fines del tratamiento y la base jurídica del mismo. El artículo 13.2 dispone qué otra información debe proporcionarse.

Supuestos en que los datos no se obtienen directamente del afectado. Junto con algunos aspectos similares a los del punto anterior, el artículo 14.2.f), dispone de la necesidad de informar acerca de «la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público».

Estrechamente ligado a la información es el aspecto del acceso a la misma, regulado en el artículo 15 RGPD (**derecho de acceso del interesado**): sobre la base del derecho de acceso, el interesado tendrá derecho a obtener del RT «confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales» y a la información que contempla el artículo 15.1 RGPD.

1.7.2. Rectificación y supresión

Según dispone el artículo 16:

> «El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional».

El objetivo de este derecho es, pues, que se actualicen los datos o que se completen.

El artículo 17 se dedica al derecho de supresión («el derecho al olvido»). Según este precepto (art. 17.1), «el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: **a)** Los datos personales ya no sean necesarios»; «**b)** El interesado retire el consentimiento»; «**c)** El interesado se oponga al tratamiento»; «**d)** Los datos personales hayan sido tratados ilícitamente»; «**e)** deban suprimirse para el cumplimiento de una obligación legal»; «**f)** se hayan obtenido en relación con la oferta de servicios de la sociedad de la información» a niños.

Ved también

Este derecho se analiza de forma más detallada en el apartado 2 («Derecho al olvido») de este módulo.

1.7.3. Derecho a la limitación del tratamiento

Se trata de un nuevo derecho (art. 18 RGPD), en virtud del cual «el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos» (art.18.1) cuando se cumplan determinadas condiciones. La principal diferencia respecto del bloqueo de los datos es que no se trata de una obligación, sino de un derecho del interesado.

Se distingue un abanico de supuestos. Unos son equivalentes a la cancelación cautelar (*cfr*. impugnar exactitud de datos), si bien cautelarmente deben conservarse.

1.7.4. El derecho a la portabilidad de los datos

Este derecho se halla reconocido en el artículo 20 RGPD. Sobre la base del mismo (art. 20.1), «el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado», en los supuestos que contempla el artículo 20 RGPD. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales deberán de ser tratados para dichos fines (art. 21.3 RGPD).

Al ejercer este derecho, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

> «El derecho a la portabilidad no afectará negativamente a los derechos y libertades de otros» (art. 20.4 RGPD).

Se trata de una novedad importante, como un complemento del tradicional derecho de acceso. Se trata del derecho de recibir los datos que le incumben a un interesado.

Una de las cuestiones que plantea este derecho es determinar hasta dónde alcanza.

¿Qué debe entenderse por *datos que el afectado ha facilitado* a un RT? Ello puede ser discutible. Se considera que los datos no deben limitarse a aquellos que han sido facilitados por el afectado, sino también otros en los que la actividad con el interesado da lugar a un tratamiento de datos, por ejemplo, datos de navegación del interesado.

1.7.5. Derecho de oposición y decisiones individuales automatizadas

El artículo 21 RGPD regula el derecho de oposición. Existen dos grandes supuestos en que puede ejercerse este derecho:

1) El artículo 21.1 RGPD regula el ejercicio del derecho de oposición por motivos fundados en una situación particular.

Se trata de aquellos casos en que los datos se procesan sobre la base de los artículos 6.1.e) o f) RGPD. En estos casos, el interesado tendrá derecho a oponerse en cualquier momento al tratamiento alegando la existencia de una situación particular.

La petición del afectado deberá motivarse. Si prevalece el ejercicio del derecho de oposición, el RT dejará de tratar los datos, salvo que acredite que existen motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado.

2) El artículo 21.2 contempla el ejercicio del derecho de oposición «cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa». En estas circunstancias, «el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles». «Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines» (art. 21.3 RGPD).

El artículo 22 RGPD hace referencia a las «decisiones individuales automatizadas», así como a la elaboración de perfiles. El artículo 4.4 RGPD proporciona una definición de qué se considera «elaboración de perfiles»:

> «Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».

El ingente y constante tratamiento masivo de datos favorece, sin duda alguna, la adopción de decisiones de forma automática, sin intervención humana. Sobre la base de este tipo de decisiones, una persona puede ver cómo se le deniega un crédito o se rechaza la solicitud presentada para un puesto de trabajo sin que exista, aparentemente, un motivo para ello. Asimismo, los tratamientos masivos pueden comportar la inferencia de conclusiones erróneas y ocasionar efectos discriminatorios.

En la medida en que estas decisiones cada vez son más generalizadas, el legislador dispone medidas para controlar el uso que se pueda hacer de las mismas.

La regla general es que «todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar» (art. 22.1 RGPD). Sin embargo, este derecho también reconoce algunas excepciones (art. 22.2 RGPD).

1.8. Limitaciones

El ejercicio de los derechos recogidos en el capítulo III está sujeto a una serie de limitaciones, tal y como dispone el artículo 23 RGPD.

Se podrá limitar el alcance de los derechos y obligaciones establecidos en el RGPD, a través de medidas legislativas, y siempre que se trate de una «medida necesaria y proporcionada en una sociedad democrática» para salvaguardar una serie de bienes, como son, entre otros, la seguridad del Estado; la defensa; la seguridad pública o bien la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales (art. 23.1).

1.9. Transferencias internacionales de datos

Actualmente, existe un flujo transfronterizo constante de datos, tanto dentro de la Unión Europea como fuera de ella. El régimen de protección de datos de la UE tuvo como objetivo, ya desde sus inicios, garantizar la libre circulación de datos en el mercado interior mediante la armonización de la normativa de la UE. Las transmisiones de datos fuera de la UE se conocen como transferencias internacionales de datos.

Una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos **fuera del territorio del Espacio Económico Europeo (EEE)**, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos (fuera de la UE) por cuenta del responsable del fichero establecido en territorio de uno de los estados miembros de la Unión Europea.

La regla general es que se prohíbe la transferencia de datos a terceros países que no ofrezcan un nivel adecuado de protección. Sin embargo, se establecen supuestos en que se permite dicha transmisión:

1) En los casos en que exista una decisión de adecuación previa de la Comisión Europea, según los requisitos del artículo 45 RGPD.

2) Cuando no exista una decisión de adecuación, mediante el establecimiento de garantías adecuadas (art. 46 RGPD). Entre ellas, cabe destacar las «normas corporativas vinculantes» (art. 47 RGPD).

3) Que concurra algunas de las excepciones contempladas en el artículo 49 RGPD.

1.10. Responsabilidad y sanciones

1.10.1. Responsabilidad administrativa

En los supuestos en que no se cumpla con la normativa de protección de datos, ello puede comportar que se impongan determinadas sanciones. Una de las novedades del RGPD es la imposición de elevadas sanciones económicas, aspecto que igualará los países de la UE. En el marco de la Directiva del 95, había en este ámbito importantes divergencias, de modo que existían países en que las sanciones eran prácticamente inexistentes mientras que en otros, como el caso español, se establecían multas muy elevadas.

El artículo 83 RGPD lleva por rúbrica: «Condiciones generales para la imposición de multas administrativas». En él, se determina que cada autoridad de control garantizará que la imposición de las multas administrativas «sean en cada caso individual efectivas, proporcionadas y disuasorias» (art. 83.1).

«Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual» (art. 83.2), y para decidir la imposición de una multa administrativa y su cuantía se tendrán en cuenta los elementos recogidos en el artículo 83.2.a) a k).

En relación con las cuantías, debe subrayarse que se establece una cantidad que opera como una cantidad máxima, pero también la sanción puede fijarse sobre la base de un determinado porcentaje del volumen de negocio total.

La tipificación de las sanciones es la siguiente:

1) Multa de hasta 10 M €, o para empresas se puede establecer hasta el 2 % de volumen de negocio anual a escala mundial (se optará por la de mayor cuantía), cuando se infrinjan las disposiciones que se contemplan en el artículo 83.4 RGPD.

El régimen sancionador en la LOPDGDD

Se encuentra regulado en los artículos 70 a 78 de esta norma. Se distingue entre infracciones muy graves (art. 72), infracciones consideradas graves (art. 73) y aquellas consideradas leves (art. 74).

2) Multa de hasta 20 M €, o hasta el 4 %, en el supuesto de incumplimiento de las disposiciones contempladas en el artículo 83.5 RGPD.

1.10.2. Responsabilidad civil (RC)

Es preciso no confundir el régimen sancionador de carácter administrativo con aquellos otros supuestos en que, como consecuencia del incumplimiento de lo dispuesto en la norma, los interesados sufran **un daño o lesión en sus bienes o derechos**.

La existencia de daños origina un deber de resarcir al afectado (se trata de un supuesto de responsabilidad civil). Esta RC surge cuando la existencia del daño o lesión en los derechos o bienes del afectado es consecuencia del incumplimiento de la normativa. Por ejemplo, como consecuencia de no adoptar las medidas de seguridad necesarias, se pierden una serie de datos y ello causa un perjuicio económico al afectado.

El hecho mismo de no adoptar determinadas medidas de seguridad puede comportar una sanción. Si, además, como consecuencia de esta falta de seguridad, se producen daños económicos al afectado (por ejemplo, alguien entra en sus cuentas y suplanta su identidad), esta conducta originaría el deber de resarcir los perjuicios económicos y morales ocasionados (responsabilidad civil).

Notad, además, que el destinatario de la cantidad en que consiste la sanción económica o la indemnización es distinto en uno y otro caso. Cuando se produce una infracción de la normativa de protección de datos, la sanción (la multa) tiene como destinatario la autoridad de protección. Por el contrario, en el caso de producirse un daño moral o económico, la cantidad en que consista el resarcimiento del daño tiene como destinatario al afectado.

En el RGPD, el derecho a la indemnización y responsabilidad se halla regulado en el artículo 82.1 RGPD, según el cual:

> «Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos».

Se trata de una responsabilidad objetiva, en la medida en que el artículo 82.3 RGPD dispone que:

> «El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios».

En la medida en que la responsabilidad civil y la responsabilidad administrativa obedecen a finalidades diferentes, pueden concurrir las dos o puede existir la una sin la otra.

2. Derecho al olvido

Miquel Peguera

2.1. Introducción

En los últimos años, la expresión *derecho al olvido* se ha hecho popular. Con esta expresión se suele hacer referencia al derecho a eliminar de la red información sobre una persona, que esta misma u otras hayan subido a internet. Se presenta a menudo como un derecho a no ser recordado en las redes, un derecho a «ser olvidado». Naturalmente, se trata de una cuestión muy relacionada con el derecho a la protección de datos. Como hemos visto en los apartados anteriores, el titular de los datos personales tiene –en determinadas circunstancias– el derecho a solicitar la supresión de sus datos, o bien a oponerse a su tratamiento, y estas serán las vías a través de las cuales se podrá hacer efectivo el llamado derecho al olvido. El RGPD ha querido recoger, explícitamente, la expresión «derecho al olvido» –si bien solo entre comillas y entre paréntesis– en el artículo que trata sobre el derecho de supresión de datos. Así, la rúbrica del artículo 17 RGPD habla de derecho de supresión («el derecho al olvido»). Ciertamente, ni el derecho de supresión ni el de oposición son nuevos. Ya estaban recogidos, con requisitos similares, en la Directiva 95/46. Sin embargo, el RGPD ha ampliado el alcance del derecho de supresión con una nueva previsión que quiere facilitar la cancelación de los datos que se han ido multiplicando en las redes, como veremos al final de este apartado (art. 17.2 RGPD).

A menudo, sin embargo, se entiende por derecho al olvido una manifestación más concreta: la posibilidad de limitar el uso de los buscadores de internet para obtener información sobre una persona.

Google y los otros buscadores indexan una enorme cantidad de contenidos publicados en la web. Si introducimos en el buscador el nombre de una persona, obtenemos resultados que enlazan a diferentes lugares donde aparece información referida al interesado. Estas informaciones pueden ser de muchos tipos. A veces, se trata de noticias antiguas sacadas de la hemeroteca digital de un periódico, o de entradas en blogs, o comentarios en redes sociales. Puede ser que sean informaciones inexactas, o bien obsoletas o ya no relevantes en el momento actual. En todo caso, pueden tener un impacto grave en la persona interesada, especialmente cuando los primeros resultados llevan a informaciones negativas ya olvidadas, que quedan así fuera de su contexto, y que pueden perjudicar la imagen o el desarrollo de la persona afectada.

Desde hace algunos años, este tipo de situaciones llevó a plantear si el derecho de protección de datos, y en concreto la Directiva 95/46, permitía al interesado reclamar directamente al buscador que suprimiera los resultados en cuestión.

Después de múltiples resoluciones dictadas por la Agencia Española de Protección de Datos (AEPD), que se recurrieron ante la Audiencia Nacional (AN), este último tribunal planteó la cuestión al Tribunal de Justicia de la UE (TJUE). El TJUE dictó una sentencia en la que reconoce la posibilidad de exigir a los buscadores la supresión de determinados resultados. Se trata del caso Google Spain, que examinamos a continuación, en el que se pusieron las bases del derecho al olvido en los buscadores de internet.

2.2. El caso Google Spain

El 13 de mayo de 2014, el TJUE dictó sentencia en el asunto C-131/12, Google Spain, S. L. y Google Inc. contra la Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, conocido como caso Google Spain. La persona afectada en el caso concreto era el abogado Mario Costeja. Haciendo una búsqueda por su nombre en Google aparecía, como uno de los primeros resultados, un enlace a un anuncio oficial publicado en el diario *La Vanguardia*, en 1998, referido a la ejecución de inmuebles por deudas a la Seguridad Social. El tema ya había sido solucionado años atrás, y no tenía ninguna relevancia actual, pero, aun así, seguía apareciendo al introducir su nombre en el buscador.

El TJUE, aplicando la Directiva 95/46 a la luz de los derechos a la privacidad y a la protección de datos, reconocidos en la Carta de derechos fundamentales de la UE, concluyó que el interesado tiene derecho, en determinadas circunstancias, a exigir la supresión de ciertos resultados en las búsquedas hechas a partir de su nombre.

La sentencia consideró que la indexación de las informaciones y su presentación como resultados de búsqueda son un tratamiento de datos personales. Constituyen un tratamiento diferente del que realiza la fuente donde publicaron los datos inicialmente, y el responsable de este tratamiento es el buscador. Por lo tanto, señala el tribunal:

> «el interesado puede ejercer sus derechos de protección de datos ante el buscador, concretamente los derechos de cancelación y de oposición, sin necesidad de dirigirse previamente a la fuente».

Dado que se trata de una reclamación basada en el derecho a la protección de datos, no es necesario acreditar que el interesado ha sufrido un daño como consecuencia de la aparición de la información en los resultados de búsqueda. Tampoco es necesario que la información sea falsa o ilícita. Sí es preciso, sin embargo, que concurran los requisitos para el ejercicio de los derechos de supresión o de cancelación.

Concretamente, el TJUE señaló que:

> «el interesado tiene el derecho de exigir al buscador que, cuando se haga una búsqueda por su nombre, no se muestren en la lista de resultados enlaces que conduzcan a datos que no cumplen con los principios de calidad o licitud de datos porque sean, por ejemplo, inadecuados, no pertinentes, irrelevantes o excesivos».

Ahora bien, el interesado no tendrá este derecho cuando la información sea de interés general, de forma que prevalezca el interés del público a obtenerla mediante búsquedas nominales, como puede ser el caso de datos sobre personas con relevancia en la vida pública. Es necesario, por lo tanto, hacer una valoración caso por caso para determinar qué derecho debe prevalecer en cada situación.

2.3. Aplicación del derecho al olvido

Desde la sentencia Google Spain, tanto la AEPD como los tribunales han resuelto muchos casos sobre la aplicación del derecho al olvido, y se han ido consolidando algunos criterios, aunque se trata de una materia llena de matices y en la que hay decisiones contradictorias.

Entre otras, se pueden destacar las siguientes cuestiones relevantes en la aplicación de este derecho:

1) El alcance territorial del bloqueo. En el momento de redactar este módulo, es todavía una cuestión abierta la de determinar si el buscador está obligado a remover los resultados en todo el mundo, y por tanto en todas las versiones del buscador, o si es suficiente con que lo haga solo en las versiones europeas (como por ejemplo google.es, google.fr, google.it). Hay en curso una cuestión prejudicial ante el TJUE, planteada por la autoridad de protección de datos francesa, en la que el TJUE se tendrá que pronunciar sobre este punto (asunto C-507/17, Google, *Portée territoriale du déréférencement*). En algunos países, la autoridad de protección de datos considera que resulta suficiente que el buscador, además de bloquear los resultados en los dominios europeos, bloquee también las búsquedas en cualquier otro dominio cuando sean búsquedas hechas desde la UE, recurriendo a la técnica de la geolocalización y bloqueo geográfico, para evitar que desde Europa se pueda encontrar el contenido buscando por el nombre en dominios de otros países, o en el dominio .com.

2) La comunicación entre el buscador y la fuente de la información. Otra cuestión debatida es si el buscador, una vez que ha retirado un enlace, por ejemplo, un enlace a una noticia publicada por un diario digital, puede informar de este hecho al diario. La AEPD, en una resolución de septiembre de 2016, posteriormente recurrida y aún pendiente de resolución, consideró que la comunicación al editor vulneraba el deber de secreto establecido en el artículo 10 de la entonces vigente LOPD de 1999 (Resolución R/02232/2016).

3) El ejercicio del derecho al olvido por parte de personas sin vinculación con la UE. El criterio que se ha mantenido hasta ahora es que una persona que no tenga vínculos con la UE, de nacionalidad, residencia o de otro tipo, no puede hacer valer el derecho europeo de protección de datos para solicitar la retirada de resultados en los buscadores.

4) Interés público de la información. Como ya se ha indicado, cuando se considera que hay un derecho prevaleciente del público a obtener la información de que se trata, el derecho al olvido no es procedente. En este sentido, se pueden producir situaciones paradójicas, como por ejemplo que, cuando el propio interesado del caso Google Spain pidió la retirada de los enlaces a una entrada de blog que comenta su caso, incluida la ejecución del inmueble y las deudas a la Seguridad Social, la AEPD entendió que ahora el caso ya era de interés público –y de hecho, el propio interesado había hablado públicamente del mismo en varias entrevistas– y, por lo tanto, no procedía la retirada (Resolución R/02179/2015).

Algunos ejemplos recientes en que se ha entendido que prevalece el interés público son un caso referido a comentarios negativos sobre la conducta profesional de un médico. La AEPD estimó el derecho al olvido, pero la Audiencia Nacional revocó la decisión, considerando que prevalece el interés público porque los futuros pacientes del médico tienen derecho a conocer las experiencias y opiniones expresadas por antiguos pacientes (Sentencia de 11 de mayo de 2017, ECLI: ES:AN:2017:2433).

En otro caso, la Audiencia Nacional revocó también la decisión de la AEPD y consideró que la información relativa a las listas de unas elecciones municipales es de interés público y el afectado no puede exigir su retirada en los buscadores (Sentencia de 19 de junio de 2017, ECLI: ES:AN:2017:2562).

5) Uso de protocolos de exclusión por parte de los editores, para evitar la indexación de la información. El Tribunal Supremo, en Sentencia de 15 de octubre de 2015 (ECLI: ES:TS:2015:4132), determinó que un periódico debe utilizar protocolos de exclusión (por ejemplo, el protocolo robots.txt) para asegurarse de que los buscadores no indexarán la información que contenga datos personales.

6) Integridad de la hemeroteca digital y uso de buscadores internos. En la misma STS de 15 de octubre de 2015, el Tribunal Supremo declaró que el interesado no tiene derecho a exigir que el diario modifique el contenido de su hemeroteca para anonimizar su nombre en las noticias publicadas, o para sustituirlo por iniciales. Negó también que el diario tuviera que bloquear los resultados de las búsquedas hechas por el nombre de la persona en el buscador interno de la web del diario. Esta última posición, sin embargo, ha sido contradicha por el Tribunal Constitucional, que en Sentencia de 4 de junio de 2018 estimó el recurso de amparo y anuló parcialmente la sentencia del TS, estimando que el interesado tiene derecho al bloqueo en las búsquedas por su nombre en el buscador interno del diario.

7) Retirada de contenidos en plataformas. Mientras que el TJUE declaró claramente que un buscador es responsable del tratamiento de los datos indexados, no está tan claro si las plataformas que alojan contenidos subidos por los usuarios se deben considerar también responsables del tratamiento de los datos personales incluidos en estos contenidos. La jurisprudencia es todavía confusa en este punto, pero en todo caso la AEPD estima que, una vez que la plataforma ha recibido una notificación de la presencia de contenido que vulnera los derechos de protección de datos, tiene la obligación de proceder a la retirada del material.

2.4. El derecho al olvido en el RGPD y en la Ley Orgánica 3/2018

Como indicábamos al inicio de este apartado, el artículo 17.2 RGPD recoge una previsión que quiere facilitar la supresión de datos personales en la red. Es habitual que la información que aparece en un sitio web sea enlazada desde otros, o replicada en otros sitios. El artículo 17 establece los casos en que procede el derecho a la supresión de los datos a todos los efectos, y añade en su apartado segundo que, cuando el responsable del tratamiento haya hecho públicos los datos y esté obligado a suprimirlos, tendrá que adoptar las medidas razonables para informar de la solicitud de supresión a los subsiguientes responsables, para que supriman «cualquier enlace a los datos personales, o cualquier copia o réplica de los datos». Esta obligación del responsable del tratamiento, sin embargo, queda supeditada al hecho de que las medidas sean razonables «teniendo en cuenta la tecnología disponible y el coste de su aplicación».

La **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** ha añadido una regulación específica del derecho al olvido. Por una parte, en su artículo 93 recoge la doctrina emanada del TJUE en la sentencia Google Spain en relación con la supresión de resultados en los buscadores de internet:

> «1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.
>
> Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.
>
> Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.
>
> 2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.»

Por otra parte, en su artículo 94, titulado *Derecho al olvido en servicios de redes sociales y servicios equivalentes*, establece el derecho a retirar los datos personales que el propio interesado haya facilitado para su publicación en redes sociales. Para ello basta la mera solicitud de la persona afectada. En relación con los datos aportados por terceros, se reconoce el derecho del afectado a que se supriman cuando concurran los requisitos para el ejercicio de los derechos de supresión o de oposición. Estos requisitos, sin embargo, no serán exigibles cuando los datos se refieran a menores de edad.

Resumen

Los datos personales, cualquier información relativa a una persona identificada o identificable, deben tratarse según unas normas establecidas. No existe, en el caso de la UE, una libertad total para tratar los datos, sino que debe cumplirse con las disposiciones del RGPD y la LOPDGDD y en determinados casos con la normativa específica.

Además de cumplir con los principios de protección de datos, debe existir una base legal que habilite el tratamiento de datos. El responsable del tratamiento tiene una serie de obligaciones, entre ellas, informar adecuadamente al afectado. Además, deberá llevar un registro y tratar los datos de forma adecuada, cumpliendo con el principio de responsabilidad proactiva. En el caso de recurrir a otro sujeto (encargado del tratamiento) para que trate datos por su cuenta, deberá formalizar un documento donde consten todos los extremos de dicha relación.

Las autoridades de protección de datos supervisan el cumplimiento adecuado de la normativa. En este sentido, el delegado de protección de datos constituye un nexo entre las autoridades y las empresas u organizaciones.

El RT debe garantizar el ejercicio de los derechos por parte del afectado: derecho de acceso, rectificación, supresión y oposición. El RGPD también reconoce el derecho a la portabilidad de los datos, el derecho a no ser objeto de decisiones automatizadas sin intervención humana y a la limitación al tratamiento.

La transmisión de datos fuera del EEE constituye una transferencia internacional de datos que está sujeta a unas normas específicas.

El derecho al olvido ha quedado consagrado desde la sentencia del TJUE, en el caso Google Spain, que concluyó que los buscadores de internet son responsables del tratamiento de los datos personales de todas las informaciones que indexan. Como consecuencia de ser responsables del tratamiento, los interesados pueden solicitar al buscador que, cuando se hagan búsquedas a partir del nombre de la persona, no muestre resultados que dirijan a datos personales que no cumplan con los principios de calidad o licitud, por ejemplo, por el hecho de tratarse de datos obsoletos, inexactos, irrelevantes o excesivos.

Este derecho también se ha ejercitado frente a los periódicos digitales. El TS ha considerado que no existe un derecho a anonimizar los nombres de las personas en las hemerotecas digitales. Por otro lado, el TC ha considerado que

los interesados pueden exigir que se bloqueen resultados también en los buscadores internos de un periódico cuando la búsqueda se hace por el nombre de la persona.

En el caso de no cumplirse debidamente con la normativa de protección de datos, ello comporta una infracción normativa que puede conllevar sanciones económicas importantes. Asimismo, si como consecuencia de dicho incumplimiento se ocasionan daños al afectado, surgirá una obligación de resarcirle (responsabilidad civil).

Bibliografía

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

Berrocal Lanzarot, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Madrid: Editorial Reus.

De Hert, P. J. A.; Papakonstantinou, V. (2014). «The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition». *Computer Law & Security Review: the International Journal of Technology Law and Practice* (vol. 30, núm. 6, págs. 633-642).

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

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

Llácer Matacás, M. R. (2008). «Autodeterminación informativa y valor positivo del silencio. Una lectura crítica del artículo 14 del Reglamento de Protección de Datos Personales». *Derecho privado y Constitución* (núm. 22, págs. 169-192). ISSN 1133-8768.

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

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

Peguera, M. (2015). «In the Aftermath of Google Spain: How the "Right to Be Forgotten" is Being Shaped in Spain by Courts and the Data Protection Authority». *International Journal of Law and Information Technology* (vol. 4, núm. 23, págs. 325-347). DOI: 10.1093/ijlit/eav016

Poullet, Y. (2009, noviembre). «Privacy: Conditions for its survival in our I.S.» *31.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*. Madrid.

Simón Castellano, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE efectos tras la sentencia del TJUE*. Barcelona: Editorial Bosch.

Enlaces de interés

Reglamento general de protección de datos:

https://www.aepd.es/normativa/index.html

http://apdcat.gencat.cat/ca/documentacio/RGPD/

http://www.avpd.euskadi.eus/informacion/reglamento-general-de-proteccion-de-datos/s04-5273/es/

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Autoridades de protección de datos:

Agencia Española de Protección de Datos

Autoritat Catalana de Protecció de Dades

Agencia Vasca de Protección de Datos

Supervisor Europeo de Protección de Datos

Otros recursos de interés:

Comisión Europea

International Association of Privacy Professionals

Future of Privacy Forum

LOPD y Seguridad

Cátedra de Privacidad y Transformación Digital Microsoft-UV

Article 29 working party archives 1997-2016

Normas sobre protección de datos personales dentro y fuera de la UE (Comisión Europea)

Respecto del mercado único digital, podéis consultar: Digital Single Market

En cuanto a las claves de la reforma de la normativa de protección de datos y las principales características del RGPD resulta muy interesante consultar las Conferencias organizadas por la Autoridad catalana de protección de datos que abordan las principales cuestiones del Reglamento 2016/679.