Intimidad y datos personales en Internet

PID_00266965

Mònica Vilasau

Tiempo mínimo de dedicación recomendado: 9 horas

Universitat Oberta de Catalunya

Mònica Vilasau

Profesora de Derecho Civil de los Estudios de Derecho y Ciencia Política de la UOC. Su principal línea de investigación es el estudio de los derechos a la intimidad y a la protección de datos de carácter personal.

La revisión de este recurso de aprendizaje UOC ha sido coordinada por la profesora: Raquel Xalabarder Plantada (2019)

Segunda edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

1. Las tecnologías de la información y la comunicación y los retos para la vida privada

El derecho a la intimidad se halla reconocido en la gran mayoría de las constituciones y cartas de derechos fundamentales. Las tecnologías de la información y la comunicación (TIC) han cambiado y reconfigurado este derecho que está en constante evolución, intentando definirse ante los cambios constantes de las tecnologías. En un primer momento, las TIC irrumpieron en el ámbito personal y íntimo abriendo las puertas a información a la que antes era impensable acceder, y sobre todo permiten buscar, relacionar, almacenar y transmitir dicha información. Todo ello ha ofrecido ventajas indudables; sin embargo, también las señales de alerta se dispararon ante los peligros que dichas tecnologías comportan para la vida privada. Con las tecnologías digitales la persona se convierte en un dato, en un conjunto de información. El ADN, la imagen, la voz o la práctica totalidad de la vida diaria de un sujeto (pagar con tarjetas de crédito, hablar por teléfono, comprar por Internet, conectarse a la TV digital, utilizar un GPS) pueden convertirse en bits, en información digital. Asimismo, debe tenerse en cuenta que la navegación por la red es un rastro vinculado a la dirección IP (páginas consultadas, música descargada, chats mantenidos).

Si se une esta trazabilidad de la información con la creciente velocidad de los procesadores, la utilización de potentes motores de búsqueda y de relación de datos, obtenemos como resultado que el individuo se convierte en un ser transparente y el derecho al olvido queda prácticamente anulado. Sobre la base de toda la información digital se construyen perfiles de los sujetos, se parametrizan los comportamientos y se envía publicidad personalizada.

En nuestra sociedad, la tecnología es cada vez más omnipresente y proliferan los instrumentos que permiten llevar a cabo un seguimiento más intensivo y constante del individuo. Entre ellos, cabe destacar el GPS, la generalización de las cámaras de videovigilancia, los teléfonos de última generación, la inserción de etiquetas RFID (identificación por radiofrecuencia) en los objetos, o los espacios de inteligencia ambiental. Asimismo, la tecnología alcanza tal nivel de sofisticación que con frecuencia pasa desapercibida, de modo que resulta difícil percatarse de que se deja un rastro digital.

Por otro lado, la frontera entre la esfera pública y la privada se va diluyendo en la medida en que el seguimiento descrito puede realizarse incluso en el propio domicilio. Las paredes físicas ya no constituyen un obstáculo para conocer los programas de televisión seguidos, el consumo de electricidad, la prensa *on line* consultada o los *hobbies* y adquisiciones a través de la red. Incluso en los ám-

bitos de ocio y de amistad se ha extendido el uso de las TIC; la generalización de las redes sociales constituye el ejemplo más paradigmático de lo que se está comentando.

Actualmente asistimos a una nueva revolución, principalmente de la mano de la inteligencia artificial, el *big data*, las nanotecnologías y la robótica. La cuestión más relevante es cómo podemos gobernar estas tecnologías y si efectivamente el Estado de Derecho y los principios democráticos podrán seguir regulando este nuevo contexto.

Este escenario, pone en juego continuamente el Derecho y el legislador. Uno de los retos es intentar proporcionar protección a la vida privada del sujeto para que pueda desarrollar su identidad.

Los diferentes textos constitucionales han configurado el derecho a la vida privada, y más concretamente el derecho a la intimidad, como un derecho fundamental que deriva de la dignidad de la persona y comporta la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás. En consecuencia, el titular del derecho tiene el poder de proteger este ámbito reservado frente al conocimiento y la divulgación por terceros.

Sin embargo, ante las nuevas formas de intromisión en la vida privada, deben establecerse nuevos mecanismos de protección. No basta simplemente con poner barreras, sino que hay que proporcionar al individuo nuevos instrumentos para que pueda controlar activamente su vida privada y especialmente la información que se genera en relación con su persona. Además, debe tenerse en cuenta que, en ocasiones, la información recopilada no pertenece a la estricta órbita de lo privado, puede incluso ser de conocimiento general, por lo que no quedaría protegida por el derecho a la intimidad en sentido estricto. De hecho, muchos de los datos pueden parecer irrelevantes, algunos ni siquiera se esconden. No obstante, una información poco trascendente, si entra dentro de un engranaje y se acumula a otra información, puede acabar adquiriendo un gran valor.

Por lo tanto, más que el derecho a ocultar, se trata de otorgar al individuo el control de la información. En el escenario de la sociedad de la información, y ante las nuevas formas de injerencia descritas, se fue definiendo un nuevo derecho, el derecho a la autodeterminación informativa o a la protección de datos de carácter personal.

La delimitación de este derecho quedó inicialmente configurada por la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983, sobre la ley del censo que definió el derecho a la autodeterminación informativa como corolario del derecho a la autodeterminación de la persona.

El derecho a la autodeterminación informativa comporta que el individuo pueda decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida. Según el Tribunal alemán, el libre desarrollo de la personalidad presupone, en las condiciones modernas de la elaboración de datos, la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos referentes a la persona.

Sentencia del 15 de diciembre de 1983

La Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983 puede encontrarse traducida al castellano en el *Boletín de Jurisprudencia Constitucional* (núm. 33, 1984, págs. 126 y sig.). Se presentó un recurso contra la ley del censo de 25 de marzo de 1982. Este recurso, a pesar de reconocer el derecho y el deber del Estado de obtener información, planteaba el temor de que la información pudiera ser eventualmente utilizada contra los derechos de los ciudadanos.

Las normas relativas al tratamiento de los datos de carácter personal constituyen un instrumento para salvaguardar la vida privada del sujeto. Sin embargo, a la hora de otorgar esta protección, debe ponderarse la existencia de otros derechos; especialmente la libertad de expresión y el derecho a comunicar y recibir información, así como el acceso a la información generada por el sector público.

Asimismo, en la interacción entre los sujetos interesados en el intercambio de datos, también deberá tenerse en cuenta el principio de libertad de empresa en el marco de la economía de mercado.

El entramado y equilibrio entre los derechos implicados quedaron distorsionados por un factor nuevo, la reivindicación de la seguridad. Como consecuencia de los graves atentados terroristas de setiembre de 2001 en Estados Unidos, se planteó con más fuerza la exigencia de seguridad. Ello ocasionó un control cada vez más omnipresente de la vida privada con una finalidad preventiva. En consecuencia, junto a las normas relativas a la protección de datos, se han ido aprobando normas que cada vez pretenden un control más férreo de la información, especialmente de la que circula a través de Internet, para hacer frente a las amenazas del terrorismo y del crimen organizado.

A lo largo de este módulo se expondrá cuál es el marco legislativo de la protección de datos como instrumento privilegiado para garantizar un espacio reservado a la persona. Algunos autores de referencia ponen de manifiesto que la existencia de esta esfera, estrechamente relacionada con el derecho a la autodeterminación del sujeto y al libre desarrollo de la personalidad, no es un derecho más entre los otros, sino el presupuesto para el ejercicio de otros derechos e incluso el fundamento de una sociedad verdaderamente democrática.

Lectura recomendada

Yves Poullet (2009, noviembre). "Privacy: Conditions for its survival in our I.S". *31.ª Conferencia Internacional de autoridades de protección de datos y privacidad* (pág. 4). Madrid. <http://www.privacyconference2009.org/program/Presentaciones/index-ides-idweb.html>

2. Evolución normativa sobre la protección de datos

2.1. Marco supranacional

Como se ha indicado, ante las amenazas al derecho a la intimidad y al tratamiento ilimitado de los datos personales, el derecho ha intentado dar una respuesta y salvaguardar los derechos fundamentales de la persona ponderando los intereses que hay en juego. Este impulso se ha centrado en el establecimiento de una normativa específica para regular el tratamiento de los datos personales, la adopción de medidas relativas al secreto de las comunicaciones y la creación de las agencias de protección de datos como autoridades independientes con la misión de velar por la tutela efectiva del derecho a la protección de datos.

A nivel internacional, las primeras iniciativas reguladoras surgieron en el seno del Consejo de Europa. En la Resolución de 1968 ya se subrayó que las "nuevas técnicas desarrolladas" constituyen una amenaza a los derechos y libertades individuales, especialmente al derecho de privacidad tutelado en el art. 8 CEDH. En la medida en que la legislación de la mayoría de los Estados miembros no proporcionaba una respuesta adecuada frente a dichas amenazas y algunos Estados estaban planeando revisar su legislación al respecto, se puso de relieve la necesidad de alcanzar una mayor armonización en la materia[1].

(1)A nivel nacional cabe destacar la ley aprobada por el Parlamento del estado alemán de Hessen en 1970, y posteriormente países como Suecia, Estados Unidos, Alemania, Dinamarca, Holanda, Francia, Nueva Zelanda o Canadá aprobaron normativa al respecto.

Punto 3 de la Recomendación 509

Concretamente, en el punto 3 de la Recomendación 509 se declara: "Believing that newly developed techniques such as phone-tapping, eavesdropping, surreptitious observation, the illegitimate use of official statistical and similar surveys to obtain private information, and subliminal advertising and propaganda are a threat to the rights and freedoms of individuals and, in particular, to the right to privacy which is protected by Article 8 of the European Convention on Human Rights".

Resolución de 1968

Se trata de la Recommendation 509 (1968), on human rights and modern scientific and technological developments, texto adoptado por la Asamblea el 31 de enero de 1968 (16th Sitting).

Se recomendó al Comité de Expertos en Derechos Humanos en el seno del Consejo de Europa estudiar la cuestión relativa a si el art. 8 CEDH y la legislación de los Estados miembros protegía adecuadamente el derecho de privacidad respecto a las violaciones que pudieran ser cometidas mediante el uso de las nuevas técnicas y métodos. En el caso de que la normativa existente no fuera suficiente, se aconsejaba llevar a cabo recomendaciones para mejorar la protección del derecho a la privacidad.

De acuerdo con esta invitación, se aprobaron dos resoluciones. La Resolución de 1973, que tenía como objetivo la regulación de los ficheros del sector privado, y la Resolución de 1974, dedicada a los ficheros públicos. La línea iniciada por las resoluciones de 1973 y 1974 fue continuada en el seno del Consejo de Europa, donde se gestó el Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. El objetivo de este convenio fue dotar de un marco general el tratamiento de datos personales en la medida en que se llegó a la conclusión de que el art. 8 CEDH, que tutela la vida privada, no podía cubrir ni dar respuesta a todos los supuestos de tratamiento automatizado de la información personal.

Resolución de 1973

Resolution (73) 22 On the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies).

Resolución de 1974

Resolution (74) 29 On the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (Adopted by the Committee of Ministers on 20 September 1974 at the 236 th meeting of the Ministers' Deputies).

Convenio 108 de 28 de enero de 1981

Se trata del convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este texto fue aprobado el 28 de enero de 1981 y entró en vigor el 1 de octubre de 1985, tras alcanzar cinco ratificaciones.

<http://www.coe.int/t/dghl/standardsetting/dataprotection/Global_standard/Conv%20108_es.pdf>

<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

En 1980, la OCDE adoptó unas directrices de protección de datos, cuyo objetivo principal era facilitar las transmisiones internacionales de la información personal.

Lectura recomendada

Sobre las directrices de protección de datos adoptadas por la OCDE, puede consultarse la obra de Burkert, que pone de relieve cómo la OCDE se convirtió en un foro privilegiado de intercambio entre América del Norte y Europa en relación con la legislación de protección de datos. Asimismo, también recuerda el carácter no vinculante de los principios OCDE (H. Burkert. "Privacy-Data Protection: a German/European Perspective", págs. 51-52).

Posteriormente, cabe subrayar la adopción de los principios de la ONU en 1990, que trataron de hacer frente a las múltiples cuestiones y riesgos que la creciente generalización de las TIC planteaba a la sociedad y concretamente al legislador.

Principios de la ONU de 1990

De Hert y Papakonstantinou señalan que lamentablemente los principios de la ONU de 1990 han sido dejados a un lado y ello quizá ha constituido una oportunidad perdida hacia la consolidación de unos verdaderos principios internacionales reguladores de la privacidad informacional. ("The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition" pág. 634, nota núm. 4).

Tras un largo proceso de gestación, finalmente, en el ámbito comunitario se aprobó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[2].

[(2)]Diario Oficial de la Comunidad Europea (DOCE) L 281 (23 de noviembre de 1995).

Tras dicha norma se adoptó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, modificada por la Directiva 2009/136/CE.

DOCE L 201 (31 julio 2002)

La Directiva 2002/58/CE derogó la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Directiva 2009/136/CE

La Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, modificó la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores, Diario Oficial de la Unión Europea (DOUE) L 337 (18 de diciembre de 2009). La Directiva 2002/58/CE, a su vez, está siendo objeto de reforma para alinearla adecuadamente con la agenda digital. Se inició un proceso de consulta pública que finalizó el 5 de julio de 2016. Al respecto, puede consultarse:

<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>.

Se trata de la Propuesta de Reglamento del Parlamento europeo y del Consejo, sobre el respeto a la vida privada y protección de los datos personales en el sector de las comunicaciones electrónicas y por la que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Bruselas, 10.1.2017, COM (2017) 10 final, 2017/0003 (COD); https://eur-lex.europa.eu/legal-content/es/txt/pdf/?uri=celex:52017PC0010&from=SE.

También debe tenerse en cuenta la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la cual se modifica la Directiva 2002/58/CE[3]. Esta directiva fue declarada nula por el TJUE como consecuencia del caso *Digital Rights Ireland*.

[3]DOCE L 105 (13 de abril de 2006).

Caso *Digital Rights Ireland*

Se trata de la STJUE (Gran Sala), de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12. Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros, y Kärntner Landesregierung (C-594/12) y otros. Peticiones de decisión prejudicial planteadas por la High Court of Ireland (Irlanda) y Verfassungsgerichtshof (Austria).

Finalmente, en el ámbito de la UE, debe destacarse la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, cuyos artículos 7 y 8 se dedican, respectivamente, al respeto a la vida privada y familiar y a la protección de datos de carácter personal.

Carta de los Derechos Fundamentales

Puede consultarse la Carta de los Derechos Fundamentales de la Unión Europea en la versión consolidada: DOUE, C 83 (30 de marzo de 2010).

Si la Convención del Consejo de Europa de 1981 y la Directiva 95/46 supusieron una respuesta al tratamiento de datos desde una perspectiva europea, en el ámbito de los países de la APEC (Asia Pacific Economic Cooperation) se dio también una respuesta mediante la adopción, a su vez, de unos principios en 2005. Se trata de unos principios que son aplicables, entre otros, a países tan diversos como Estados Unidos, Vietnam, Canadá, China, Japón, Rusia o Chile.

APEC Privacy Framework

En noviembre de 2004, los ministros de las economías que integran la APEC, reunidos en Santiago de Chile, adoptaron la APEC Privacy Framework, que fue desarrollada durante los años 2003 y 2004 por el Grupo de Comercio Electrónico de la APEC, subgrupo sobre la privacidad. El marco de la APEC consistía originalmente en un conjunto de nueve principios (que integraban la tercera parte del documento), precedidos por un prefacio, un preámbulo (parte I) y una segunda parte dedicada al ámbito de aplicación. La cuarta parte del Marco de privacidad de la APEC se dedicaba a la implementación de los principios, si bien solo se hacía referencia a la implementación a nivel nacional (parte A). En septiembre de 2005 se añadió una segunda parte, B, dedicada a la implementación a nivel internacional, y se completaron los principios.

APEC

La APEC está integrada por veintiún países. Puede consultarse la relación completa de países que integran esta organización en: <http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx>.

La adopción de todos los textos referidos constituyó sin duda alguna un hito importante en la regulación de las nuevas tecnologías y la consagración del derecho a la protección de datos. Sin embargo, en la medida en que las TIC evolucionan constantemente, en parte se puede afirmar que algunas de estas normas ya nacieron demasiado tarde. Concretamente se constata la limitación de estas para hacer frente a una realidad que va evolucionando, generando y transmitiendo continuamente datos personales. La digitalización y transmisión de los datos personales es un fenómeno imparable en la sociedad actual. La mayoría de los textos analizados no podían prever la revolución que constituyó Internet. Este fenómeno implica que deban repensarse y rediseñarse las normas que regulan el tratamiento de la información personal.

Un buen ejemplo de esta urgencia de alcanzar unos principios universales que den respuesta a estos nuevos retos lo constituye la adopción de la Resolución de Madrid, adoptada en 2009. Se trata de los estándares internacionales sobre protección de datos personales y privacidad, Resolución de Madrid, que fueron aprobados en la 31.ª Conferencia Internacional de Autoridades de Protección de Datos. El texto aprobado puede hallarse en: <http://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/contenido-ides-idphp.php>.

En cuanto a la revisión de los textos ya adoptados para dar respuesta a los nuevos retos, se debe hacer referencia a tres procesos distintos de actualización que tuvieron su inicio en torno al año 2010. En primer lugar, la OCDE modificó los principios de 1980, proceso que culminó el 2013 con la aprobación de unos nuevos principios.

En el Consejo de Europa también en 2010 se iniciaron los trabajos de revisión del Convenio 108. El Comité consultivo creado por dicho Convenio (T-PD)[4] decidió en su 25.º encuentro plenario en septiembre de 2009 establecer como su prioridad la preparación de enmiendas al texto de 1981. Este proceso que culminó el 2018, con el que se conoce como Convenio 108+, para responder a los nuevos retos de la era digital, permitir intercambios de datos personales más seguros a nivel internacional y fortalecer la efectiva implementación del mencionado Convenio.

[(4)]Capítulo V del Convenio 108, arts. 18-20.

Enlace de interés

En cuanto al Convenio 108+, véase: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

Finalmente, en el seno de la UE, la Comisión europea lanzó en mayo de 2009 un proceso de reforma de la Directiva 95/46. En enero de 2012, la Comisión concretó esta reforma con la presentación de dos textos normativos, una Propuesta de reglamento y una Propuesta de directiva, que tras un largo proceso

[(5)]El Reglamento 2016/679 (RGPD) se halla publicado en el DOUE de 4 de mayo de 2016, L 119/1.

de elaboración fueron aprobados en abril de 2016. Se trata del Reglamento 2016/679[5] 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 (RGPD de ahora en adelante), y de la Directiva 2016/680[6] 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.

(6)La Directiva 2016/680 se halla publicada en el DOUE de 4 de mayo de 2016, L 119/89.

El art. 99 RGPD estableció que el Reglamento en cuestión entraría en vigor a los 20 días de la publicación en el Diario Oficial de la Unión Europea, y que sería aplicable a partir del 25 de mayo de 2018. La Directiva 95/46/CE quedaba derogada con efectos a partir del 25 de mayo de 2018 (art. 94 RGPD). A lo largo de este módulo se analiza el RGPD y su interacción con la normativa española.

Reforma de la Directiva 95/46 y adopción del Reglamento 2016/679

El punto de partida de la reforma de la Directiva 95/46 y de la adopción del Reglamento 2016/679 lo constituye el reconocimiento del derecho a la protección de datos en la CDFUE (Carta de los Derechos Fundamentales de la UE 2000/C 364/01), (art. 8), así como en el Tratado de Lisboa. La base jurídica de las normas de protección de datos en el marco de las actividades reguladas por el derecho de la UE se recoge en el artículo 16 del Tratado de funcionamiento de la Unión Europea (versión consolidada del Tratado de funcionamiento de la Unión Europea, DOUE, C 115/47, de 9 de mayo de 2008).

También deben mencionarse los pasos que hicieron en Estados Unidos bajo la presidencia de Obama. En febrero de 2012 la Casa Blanca publicó un libro blanco relativo a la privacidad de los datos del consumidor en un mundo conectado. Se trataba de la propuesta de un marco para proteger la privacidad y promover la innovación en la economía global digital. Tras más de dos años de consultas entre los sectores implicados, en febrero de 2015 la Casa Blanca dio a conocer un borrador de texto relativo a la ley sobre la privacidad del consumidor; se trataba de la *Consumer Privacy Bill of Rights Act* (CPBR). Constituye una norma a nivel federal relativa al tratamiento de datos en el sector privado, cuya finalidad es configurar el marco regulador de la privacidad, así como su aplicación en la esfera comercial. Otro objetivo es el de promover la implementación de esta protección a través de códigos de conducta desarrollados por los sectores implicados.

Enlaces de interés

Al respecto podéis consultar:

En cuanto a los textos legislativos,

https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

https://www.congress.gov/bill/114th-congress/senate-bill/1158.

En cuanto a la valoración de los mismos y su evolución:

https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/.

2.2. El marco legal aplicable al Estado español

2.2.1. Marco normativo

El artículo 18.4 CE establece que

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

Partiendo de este precepto y en función de la materia de que se trate, a efectos expositivos, dividiremos la normativa existente en diferentes bloques normativos, que se aplican de manera más o menos inmediata. Además, como resultado de la distribución de competencias entre el Estado y las comunidades autónomas, también hay que tener en cuenta las normas dictadas en cada una de estas instancias.

El desarrollo del artículo 18.4 CE tuvo lugar mediante la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD[7]). Esta Ley fue derogada por la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD[8]) y desarrollada por el Real decreto 1720/2007.

(7)Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automático de datos de carácter personal.

(8)BOE n.º 298, de 14 de diciembre de 1999

> Se trata del Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[9].

(9)BOE núm. 17 de 19/01/2008.

Como consecuencia de la plena aplicación del RGPD y en la medida que tratándose de un Reglamento es directamente aplicable, había que revisar la LOPD de 1999 para adecuarla al marco legal europeo. Finalmente se dictó una nueva ley, la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD, de ahora en adelante)[10].

(10)BOE n.º 294, de 6 de diciembre de 2018.

La Disposición derogatoria única de la LOPDGDD establece que queda derogada la Ley orgánica 15/1999. Sin embargo, algunos preceptos de esta última siguen en vigor, para unos casos concretos. Al respecto hay que atenerse a aquello que prevén la disposición adicional decimocuarta y la disposición transitoria cuarta LOPDGDD (véase Disposición derogatoria única.1 LOPDGDD).

> Por otro lado, hay que preguntarse qué sucede respecto al Real decreto 1720/2007 que desarrolló la LOPD de 1999. La Disposición derogatoria única, 3 de la LOPDGDD establece que "quedan derogadas todas las disposiciones del mismo rango o inferior que contradigan, se opongan, o sean incompatibles con lo que disponen el Reglamento (UE) 2016/679 y esta Ley orgánica". Esta cláusula genérica puede interpretarse en dos sentidos. Se puede entender que en la medida que la LOPD de 1999 ha sido derogada, esta derogación arrastraría también el mencionado Reglamento de 2007 que la desarrolló (habría perdido la cobertura legal). Otra interpretación podría ser considerar que el Reglamento de 2007 sigue vigente en todo aquello que no contradiga las normas mencionadas en la Disposición derogatoria, 3. Hasta el momento no ha habido ningún pronunciamiento al respecto por parte de los Tribunales.

Así pues, un primer bloque normativo por razón de la materia lo integran aquellas normas que de manera directa regulan el tratamiento de los datos personales. Por lo tanto, se trata del RGPD (recordemos que es directamente aplicable) y de la LOPDGDD. Estos son los textos básicos y de carácter general sobre protección de datos.

Asimismo, dentro de este bloque también se encuentran normas específicas, relativas a ámbitos concretos que afectan directamente a los datos de carácter personal, como las bases de datos de ADN, los datos referentes a la salud y a los historiales clínicos, o los datos sobre comunicaciones electrónicas.

Normas específicas

Entre otras, véanse: Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica; Ley 14/2007, de 3 de julio, de investigación biomédica; Ley orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN; Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Un segundo bloque normativo estaría integrado por las disposiciones relativas al comercio y a la Administración electrónica. Asimismo, dentro del contexto de Internet y también en materia de protección de datos, hay que hacer referencia a los elementos de autorregulación que surgen. Se trata de mecanismos de autocontrol que normalmente se darán en el sector privado, pero que no son exclusivos de este ámbito. Constituyen un ejemplo de esta actividad los denominados códigos tipo, códigos[11] de conducta que pueden acordar un grupo de empresas o las administraciones públicas a fin de establecer una serie de reglas, condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad, políticas en el tratamiento de los datos personales, etcétera.

[11]Sobre los códigos en general, véase el artículo 18 LSSI, y respecto al caso concreto de la protección de datos, véanse los artículos 40 a 42 del RGPD y art. 38 LOPDGDD.

Disposiciones relativas al comercio y a la Administración electrónica

Entre otras, véanse: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI); Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público; Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información; Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; Ley 9/2014, de 9 de mayo, General de Telecomunicaciones; Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Finalmente, integran el tercer bloque normativo las disposiciones de carácter general y de diferente naturaleza que resultan aplicables en función de su rango y del bien jurídico protegido.

Disposiciones de carácter general

Por ejemplo, la Ley orgánica 1/1982, de 5 de mayo, de protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen, la legislación civil aplicable en los diferentes territorios, la legislación mercantil o el Código penal. Este último código resulta aplicable como *ultima ratio* y sanciona las conductas que se consideran más graves.

Dentro del marco regulador de la protección de datos, hay que tener en cuenta la existencia tanto de normas estatales como de normas autonómicas.La Agencia Española de Protección de Datos es la autoridad de control competente de salvaguardar el respeto del derecho fundamental a la protección de datos en lo que se refiere a los tratamientos de datos efectuados principalmente por el sector privado y por parte del sector público en los casos que no queden bajo el control de una autoridad autonómica. Cataluña y el País Vasco, dentro del marco competencial que les otorgan la CE y sus respectivos Estatutos de Autonomía, han creado sus propias Autoridades de protección y han dictado también sus propias normas.

El capítulo VI del RGPD se dedica a las autoridades de control independientes. El art. 51.1 del Reglamento prevé que en un Estado miembro pueden existir una o varias autoridades públicas independientes que supervisen la aplicación del Reglamento. El Título VII de la LOPDGDD se dedica a las Autoridades de protección de datos. El Capítulo I hace referencia a la Agencia española de protección de datos y el Capítulo II a las Autoridades autonómicas. En el Estado español hay tres autoridades de protección de datos: la estatal, la catalana y la vasca. Por otro lado, en Andalucía se ha dictado una ley que crea el Consejo de transparencia y de protección de datos. El 1 de octubre de 2019 está previsto que el Consejo de Andalucía empiece a ejercer también como autoridad de protección de datos y no solo en materia de transparencia como venía haciendo hasta el momento.

El art. 57 de la LOPDGDD

El art. 57 de la LOPDGDD contempla que las autoridades autonómicas de protección de datos puedan ejercer las funciones y potestades establecidas en los arts. 57 y 58 del RGPD cuando se refieran a determinados tratamientos.

Las Autoridades autonómicas, tienen principalmente encomendada la función de velar por los ficheros de carácter público que existen en sus respectivos ámbitos territoriales y también pueden tener competencias respecto determinados ficheros privados. Sus respectivas Leyes determinan su ámbito de actuación. En consecuencia, hay normas autonómicas que directa o indirectamente regulan y hacen referencia al tratamiento de datos personales.

2.2.2. Configuración del derecho fundamental a la protección de datos en el Estado español

La LOPD fue objeto de un recurso de inconstitucionalidad estimado parcialmente por la STC 292/2000, de 30 de noviembre. En esta sentencia, el Tribunal Constitucional puso de relieve que el derecho protegido en el artículo 18.4 CE es un derecho fundamental distinto del derecho a la intimidad del artículo 18.1 CE, ya que este último puede resultar insuficiente a la hora de proteger al individuo frente a la nueva realidad derivada del progreso tecnológico. El fundamento jurídico sexto de la sentencia plasma dicha doctrina:

"La función del derecho fundamental a la intimidad del artículo 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".

Según el Tribunal Constitucional, ¿cuáles son los rasgos que permiten configurar el derecho tutelado en el artículo 18.4 CE como un derecho autónomo respecto al del artículo 18.1 CE? Si el derecho a la intimidad (art. 18.1 CE) permite excluir ciertos datos de una persona del conocimiento ajeno, es decir, otorga al titular el poder de resguardar su vida privada de una publicidad no querida, el derecho a la protección de datos (art. 18.4 CE) garantiza a los individuos un poder de disposición sobre estos datos. Estos dos derechos comparten un mismo objetivo: ofrecer una protección constitucional eficaz de la vida privada personal y familiar. Sin embargo, también hay una serie de diferencias a causa de su función específica, que se pueden concretar desde el punto de vista de su objeto y su contenido.

Por un lado, el objeto del artículo 18.4 CE es más amplio que el derecho a la intimidad del artículo 18.1 CE. El derecho fundamental a la protección de datos no se limita a los datos íntimos de la persona, sino que extiende su garantía a cualquier tipo de datos personales, sean o no íntimos, cuyo conocimiento por parte de terceros pueda afectar a los derechos de la persona. Cualquier dato de carácter personal que identifique o permita la identificación del individuo entrará dentro del ámbito de protección del derecho fundamental a la protección de datos. Debe subrayarse que se trata de cualquier dato relativo a una persona identificada o identificable.

Por otro lado, en lo que concierne a su contenido, esto es, las facultades que dichos preceptos otorgan al titular del derecho, el artículo 18.1 CE confiere a dicho titular el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo que mediante una intromisión haya sido conocido. En cambio, el derecho a la protección de datos atribuye a dicho titular un conjunto de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone deberes jurídicos a terceros. De esta manera, se garantiza a la persona un verdadero poder de control sobre sus datos personales que solo es posible y efectivo imponiendo a terceros una serie de obligaciones: requerir el consentimiento

previo para la recogida de datos personales, informar sobre el destino y el uso de los datos recogidos, garantizar el acceso a los datos, rectificar y cancelar los datos cuando sea necesario, etcétera.

> En definitiva, el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir qué datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede obtener este tercero. Este derecho también permite al individuo conocer quién posee estos datos personales, saber con qué finalidad los posee y oponerse a esta posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales: su almacenaje y tratamiento posteriores, y también su uso posible por parte de un tercero, sea el Estado o un particular. Y este derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales requiere, como complementos indispensables, por una parte, la facultad de saber en todo momento quién dispone de estos datos personales y a qué uso los somete y, por otra parte, el hecho de poder oponerse a esta posesión y a estos usos (STC 292/2000, FJ 7).

3. El Reglamento general de protección de datos (Reglamento 2016/679): aspectos clave

El 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 (Reglamento general de protección de datos, RGPD) fue publicado en el DOUE de 4 de mayo, y como ya se ha dicho, es plenamente aplicable desde el 25 de mayo de 2018.

Este texto constituye el marco general de regulación del tratamiento de datos de carácter personal. Junto a esta norma existen otros textos que regulan el tratamiento de la información en sectores específicos. Entre otros cabe destacar: el ámbito de las comunicaciones electrónicas (Directiva 2009/136/CE, que está siendo objeto de reforma); el tratamiento por parte de las instituciones y organismos de la UE (se trata del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos, y por el cual se derogan el Reglamento (CE) no 45/2001 y la Decisión no 1247/2002 / CE); el procesamiento para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales (Directiva 2016/680) o bien el procesamiento de los datos relativos al registro de nombres de pasajeros (PNR), regulados por la Directiva 2016/681.

Directiva (UE) 2016/681

La Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, regula 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.

3.1. Introducción, objetivos y características generales

Los inicios de la reforma se remontan a los años 2009 y 2010, con la obertura de consultas acerca de la conveniencia de una reforma. 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 de directiva. La aprobación del Reglamento 2016/679 y de la Directiva 2016/680 comporta que la práctica totalidad del procesamiento de datos en la UE queda cubierto bajo una normativa reguladora. De hecho, no existirá tratamiento de datos que no esté bajo una regulación u otra.

3.1.1. Las razones de una reforma

La reforma de la DPD y la propuesta de un reglamento que la sustituya obedecen 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.

Lectura recomendada

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.

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

En segundo lugar, cada vez era más acusada una divergencia normativa entre las legislaciones de los Estados miembros. La diferencia en la transposición de la directiva por los distintos Estados suponía también un sobrecoste para las empresas en la medida en que tenían que adaptarse a las distintas legislaciones. Dicha discrepancia era relevante, y un ejemplo paradigmático lo constituye el régimen sancionador, que en algunos países era prácticamente inexistente, mientras que en otros implicaba la imposición de importantes sanciones económicas.

Estas divergencias comportan dificultades para las autoridades de protección de datos (APD) cuando tienen que dar respuesta a conflictos que afectan a distintos Estados y distintas legislaciones. En ocasiones no resulta fácil determinar qué ley resulta aplicable o qué autoridad debe intervenir.

Enlace de interés

Véase: http://www.europarl.europa.eu/ftu/pdf/es/ftu_2.4.3.pdf.

La reforma emprendida se incardinó en la agenda digital presentada por la Comisión en mayo del 2010 que tenía como objetivo afianzar la confianza en el entorno digital, a fin de potenciar y hacer crecer el comercio electrónico. La finalidad es la de facilitar y buscar un incremento de la competitividad de las empresas europeas respecto a otros entornos. Los objetivos son los de garantizar la seguridad jurídica, simplificar la regulación, eliminar cargas burocráticas, así como establecer reglas claras para las transferencias internacionales de datos (si bien este objetivo dista mucho de haber sido alcanzado).

3.1.2. Las características principales de la nueva regulación

En cuanto a las características del RGPD, en primer lugar debe subrayarse la importancia de que se trate de un reglamento, lo que comporta 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[12].

(12)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.

Hay que subrayar que, a pesar de tratarse de un reglamento y de su vocación uniformadora, han quedado algunos sectores fuera[13].

(13)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.

Se procura reforzar el papel de las APD, y de hecho la regulación de estas y su relación con la Comisión y la búsqueda de un equilibrio entre ellas fueron unos de los principales escollos en la negociación del reglamento.

Se establece un régimen sancionador, que prevé la imposición de importantes sanciones económicas.

3.2. Ámbito de aplicación

El art. 1 RGPD dispone que:

> "1. El presente Reglamento establece 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.
>
> 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
>
> 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

3.2.1. Ámbito material de aplicación

Supuestos a los que resulta aplicable el Reglamento 2016/679

Art. 2.1.

> "El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

1) Personas físicas. La norma hace referencia a datos de personas *físicas identificables*; por lo tanto, quedan excluidas las personas jurídicas. Como recuerda el considerando 14 RGPD:

> "El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto".

El RGPD no contempla los datos relativos a las personas fallecidas. Al respecto, en el caso del ordenamiento jurídico español, resulta aplicable el art. 3 de la LOPDGDD. Por otro lado, también hay que tener en cuenta el art. 96 LOPDGDD que hace referencia al derecho al testamento digital y que regula el acceso a los contenidos gestionados por los prestadores de servicios de la sociedad de la información relativos a personas difuntas.

2) Dato personal. El RGPD hace referencia a los datos personales, y se considera como tal

> "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).

Datos genéticos y datos biométricos

En cuanto a qué debe entenderse por datos genéticos, véase el art. 4 (13) RGPD. En cuanto a datos biométricos, el art. 4 (14) RGPD.

En cuanto a los denominados datos sensibles (categorías especiales de datos, art. 9 RGPD), se mantiene, en términos generales, la fórmula de la DPD.

Al configurar los datos sensibles, aspecto que será analizado con más detenimiento al tratar el consentimiento del sujeto afectado, existen dos posibles aproximaciones. Una más dinámica, que contemplaría cualquier tipo de dato que pudiera revelar información sensible; en consecuencia, podrían incluirse, por ejemplo, los datos relativos a hábitos alimentarios o incluso el apellido. Y una concepción más estática, que parte de un listado de datos que se califican como sensibles. Esta última configuración es la que adopta el art. 9 RGPD y que es, en términos generales, la que ya recogía el art. 8 DPD.

Si bien el término *revelar*, adoptado por el art. 9.1 RGPD, podría dar a entender que se sigue una perspectiva dinámica, esta no es la interpretación dada al precepto en cuestión. Se distingue los datos entre sensibles y no sensibles en función de su naturaleza y no de su uso potencial.

3) Tipos de tratamiento. 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. Se mantiene por lo tanto una situación similar a la de la DPD.

Considerando (15) RGPD

"A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento".

Supuestos a los que no resulta aplicable el RGPD

Según el art. 2.2. RGPD, "El presente Reglamento no se aplica al tratamiento de datos personales":

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del derecho de la Unión.

Considerando (16) RGPD

"El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión".

b) Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE. Se trata de los supuestos de política exterior y de seguridad común.

c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Al respecto, es fundamental tener en cuenta el considerando (18):

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

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.

d) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[14].

(14)Véanse al respecto los considerandos 19 I, 19.II y 20.

Dispone además el art. 2.3 RGPD que

"El Reglamento (CE) núm. 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) núm. 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98".

Considerando (17) RGPD

"El Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo (2) se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) núm. 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) núm. 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento".

Recordad que el Reglamento 45/2001 ha sido derogado por el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de estos datos, y por el cual se derogan el Reglamento (CE) no 45/2001 y la Decisión no 1247/2002 / CE.

Finalmente, según determina el art. 2.4 RGPD[15],

(15)Véase al respecto el considerando 21.

"El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15".

3.2.2. Ámbito territorial de aplicación

Según dispone el art. 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".

Por lo tanto, el criterio que ahora permite determinar la aplicación de la norma europea es el criterio 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.

Según prevé el art. 3.2. RGPD:

"El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago[16].

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 presente Reglamento.

Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Para determinar este extremo, se tienen en cuenta aspectos como la lengua de la página web, la moneda utilizada en el pago o bien donde se produzca la entrega de los bienes.

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

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, analiza o predicen las preferencias personales, comportamientos y actitudes de los afectados[17]".

(16)Considerando 23.

(17)Considerando 24.

Cabe tener en cuenta que en estos casos (art. 3.2 RGPD) es necesario designar un representante en la UE (art. 27.1 i 27.2 RGPD)[18].

(18)Al respecto también hay que tener en cuenta el art. 30 LOPDGDD

Finalmente, según dispone el art. 3.3, el RGPD resulta aplicable cuando ello se deriva de las normas de derecho internacional público:

"El presente Reglamento 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".

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

El art. 5 RGPD, bajo la rúbrica de "**Principios relativos al tratamiento**", recoge cuáles son los principios de protección de datos, poniendo un nombre a cada uno de ellos.

De entrada, hay que señalar que no existen grandes cambios de los principios recogidos en el RGPD respecto a los admitidos en la DPD. La única novedad como tal la representa el principio de responsabilidad proactiva (art. 5.2 RGPD).

Se trata de los siguientes Principios.

Primero, los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia", art. 5.1.a) RGPD).

Estos tres principios están muy interconectados. El principio de lealtad y el de transparencia están muy ligados, de modo que debe informarse de qué se hará con los datos. De hecho, el principio de transparencia está vinculado al ejercicio de todos los derechos.

Como se ha indicado, estos principios no representan una gran innovación ni separarse de las previsiones de la DPD.

El principio de transparencia tampoco es nuevo, el RGPD 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 [19].

(19)Al respecto hay que tener en cuenta el art. 11 LOPDGDD, que será analizado con más detalle más adelante.

En cuanto al principio de licitud, este se encuentra más desarrollado en el artículo 6 RGPD y hace referencia a los supuestos concretos en que se pueden tratar los datos personales. Se adopta una sistemática muy parecida a la de la DPD. Se trata de una lista cerrada, como se expone más adelante. Algunos de estos supuestos habilitadores se encuentran recogidos en la LOPDGDD, concretamente en los arts. 6 y 8 de la Ley estatal.

Segundo, los datos personales serán 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", art. 5.1.b) RGPD).

Hay que subrayar que el art. 5.1.b) RGPD hace referencia a que no podrán ser tratados ulteriormente de "*manera* incompatible[20]".

(20)También hay que tener en cuenta el art. 6.4 RGPD (determinados supuestos en que los datos pueden tratarse para otra finalidad)

Otra novedad que presenta el art. 5.1.b) es hacer referencia también al "tratamiento ulterior de los datos personales con fines de archivo en interés público", que no se contemplaba por el art. 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 Leyes de archivos de las distintas CCAA en caso de que existan. Pero parece que también deberían incluirse aquellos archivos privados de interés público.

El precepto en cuestión se remite al art. 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 dispone que será preciso adoptar las medidas adecuadas.

En cualquier caso, el aspecto más novedoso respecto al art. 5.1.b es que se relativiza la "incompatibilidad" respecto a las finalidades.

Efectivamente, el art. 6.4 RGPD admite en determinados supuestos destinar los datos a una finalidad distinta. En este caso, será el RT quien deberá valorar si el uso de los datos para otra finalidad es compatible o no.

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

En cuanto al cambio de finalidad, hay que tener también en cuenta el art. 23.2 RGPD (relativo a las limitaciones).

> Tercero, los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos", art. 5.1.c) RGPD).

El principio de minimización no supone tampoco en rigor un nuevo principio. Esto es, el tratamiento deberá ser proporcional a la finalidad. Este principio se tiene que poner en relación con el art. 25 RGPD (protección de datos desde el diseño y por defecto).

Ello comporta que al llevar a cabo un tratamiento, deba en primer lugar valorarse si efectivamente es preciso tratar datos personales (en adelante, DP). En caso de que deban tratarse datos: que dicho tratamiento sea aquel imprescindible para la finalidad prevista. En este punto relevante, un concepto ligado a la minimización es el de seudonimización.

Según se determina en el art. 4. (5) RGPD, se entiende por "seudonimización" el tratamiento de datos personales de tal manera 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.

El concepto de seudonimización, es un concepto nuevo, un mecanismo que permite tratar datos que se incluyen dentro de la categoría de DP, pero que al atribuirles un código comporta que terceros no tengan acceso directo a los datos identificativos; de este modo, se minimiza el riesgo.

El principio de minimización debe relacionarse con el de conservación de los datos, de modo que se crea un principio de 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 para interés público.

En relación con el plazo de conservación de los datos, hay que tener en cuenta la exigencia del RGPD y el contenido de las cláusulas informativas. Debe informarse del plazo durante el que se piensa conservar los datos. Si no es posible fijar un plazo, sí al menos establecer los criterios que permitirán determinar el plazo de conservación [art. 13.2.a) y art. 14.2.a) RGPD].

> Cuarto, los datos personales serán 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", art. 5.1.d) RGPD)[21].

[21] Véase también art. 4 LOPDGDD.

Los datos deben ser exactos y estar actualizados, de lo contrario, deben rectificarse o suprimirse.

Ello también está relacionado con el deber del RT de comunicar a los destinatarios de los datos que se ha producido su rectificación o supresión. Esta obligación está prevista en el art. 19 RGPD.

Quinto, los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("limitación del plazo de conservación", art. 5.1.e) RGPD).

Sexto, los datos personales serán 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", art. 5.1.f) RGPD)[22].

(22)Véase art. 5 LOPDGDD.

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 o la destrucción, o el daño accidental.

El contenido es casi el mismo que el del art. 9 LOPD de 1999. Se trata, en definitiva, de garantizar una seguridad adecuada respecto a la pérdida de información o a un daño en la información. Sin embargo, lo que resulta más novedoso no son los deberes de seguridad, sino los instrumentos para hacerla efectiva.

Estas herramientas son las siguientes: evaluar los riesgos que deben afrontarse al iniciar un tratamiento, implementar medidas técnicas y organizativas adecuadas, y notificar las violaciones de seguridad.

Séptimo, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva", art. 5.2 RGPD).

Se trata del nuevo principio incorporado; de responsabilidad demostrable (*accountability*). El enfoque de la LOPD de 1999 (y de la DPD) podía calificarse como de reactivo. De modo que si se produce un incumplimiento de la norma o un daño, el RT debe responder.

La aproximación del RGPD añade a dicha aproximación reactiva una proactiva. Establece la carga sobre el RT 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, dispone de las herramientas que están contempladas en el capítulo IV del RGPD. En concreto, la adopción de una política de protección de datos, el registro de operaciones de tratamiento, la protección de datos desde el diseño y protección de datos por defecto, el establecimiento y reconocimiento de códigos de conducta, de 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 diligencia al designar un ET (encargado del tratamiento) y DPO (delegado de protección de datos), 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 de manera periódica.

En definitiva, se trata de un conjunto de instrumentos para hacer efectiva la responsabilidad proactiva. Si bien esta se configura y considera como un principio, las obligaciones recogidas en el capítulo IV son auténticas obligaciones y como tales son exigibles a lo largo de todo el tratamiento.

3.4. Bases legales que permiten el tratamiento de datos de carácter personal (art. 6 RGPD)

El art. 5.1.a) RGPD determina que el tratamiento debe ser lícito, requisito que viene desarrollado en el art. 6 RGPD, que recoge las bases legales que permiten un tratamiento. La LOPDGDD no recoge una regulación general y completa de las bases legales que permiten el tratamiento de datos personales (no es necesario reproducir el art. 6 RGPD que es directamente aplicable). Pero sí que hace referencia a algunos de los fundamentos legitimadores en los arts. 6 y 8 LOPDGDD.

En este precepto se recogen los supuestos que permiten (habilitan) un tratamiento de datos, de tal modo 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 art. 7.1 DPD, que determina que "los Estados miembros dispondrán que el tratamiento de datos personales *sólo* 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 no halle cabida dentro de alguna de dichas excepciones.

El RGPD sigue el mismo patrón que el art. 7 DPD, de manera que según dispone el art. 6.1.RGPD "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones [...]".

> **a)** el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> **b)** el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> **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.
>
> 2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.
>
> 3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:
>
> a) el Derecho de la Unión, o
>
> b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. [...]".

La primera valoración que puede hacerse del art. 6 RGPD es que no aporta novedades sustanciales respecto del contenido del art. 7 DPD, que sería su equivalente. En todo caso cabe destacar la posibilidad, sometida a cautelas, de tratar los datos para una finalidad distinta de aquella para la que se recogieron (art. 6.4 RGPD) y la regulación del consentimiento del niño (art. 8 RGPD).

En cuanto al art. 6 RGPD, aquello más relevante es dejar claro que sin la concurrencia de uno de los supuestos contemplados en el precepto no es posible llevar a cabo un tratamiento[23]. Si bien es cierto que los supuestos son amplios, y quedarán pocos casos fuera, debe subrayarse la necesidad de que exista una base legal.

[23] Así lo subrayan, entre muchos, los siguientes autores: Heredero, Poullet, Aparicio y Lynskey.

Asimismo, el hecho de que concurra una base legal *ex* art. 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*. art. 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 terminología utilizada en el art. 5.1.a (en la medida en que establece que el tratamiento debe ser lícito), y el art. 6 (cuya rúbrica es "Licitud del tratamiento"). Esta conexión ya se puso 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 deba cumplirse de forma cumulativa con los art. 5 y art. 6 RGPD.

Lectura recomendada

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

Del mismo modo, tal y como recordó el TJUE en la sentencia de 24 de noviembre 2011, en el caso ASNEF[24], las bases legales constituyen una enumeración cerrada, de modo que son las que son, y no constituyen un supuesto ejemplificativo al que puedan añadirse otras categorías.

[24]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) v. Administración del Estado, asuntos acumulados C-468/10 y C-469/10.

En consecuencia, en la aplicación del RGPD no pueden añadirse más supuestos ni requisitos a los que ya constan en el texto del articulado. En cuanto al interés legítimo, debe señalarse que la LOPD de 1999 no traspuso correctamente la DPD. La LOPD no recogió en su articulado el interés legítimo como un mecanismo que por si solo permitiera el tratamiento de datos, sino que era preciso que además los DP estuvieran contenidas en fuentes accesibles al público. El TJUE estableció que no era posible añadir más exigencias a las ya previstas 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 (FAP). En definitiva, no pueden añadirse otras cargas a las exigencias existentes.

3.4.1. Supuesto específico: el interés legítimo

Esta base legal fue especialmente analizada por el TJUE en el caso ASNEF ya mencionado y también en el caso Google Spain. En el primer supuesto, el TJUE analizó si la legislación española había implementado correctamente el art. 7.f) DPD, y concretamente como se recogia la referencia al interés legítimo. Como ya ha sido expuesto, el TJUE contestó negativamente la pregunta planteada y señaló que no se pueden añadir más requisitos a la existencia del interés legítimo (como por contra había hecho el legislador español, tanto en la LOPD de 1999 como en el RLOPD).

Al respecto es conveniente consultar el Dictamen del Grupo del art 29, 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del arte. 7 DPD (WP 217), adoptado el 9 de abril de 2014.; https://ec.europa.eu/justice / article-29/documentation/ opinion-recommendation/files/ 2014/wp217_es.pdf.

Nota

STJUE (Gran Sala), de 13 de mayo de 2014, Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD) y 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 por parte de dicho buscador, la STJUE dictaminó que en este caso debía prevalecer el derecho del afectado.

3.4.2. Tratamiento de datos para otra finalidad distinta

Una novedad que introduce el art. 6.4 RGPD es la posibilidad de tratar los datos para otro fin distinto de aquel inicialmente previsto.

Si bien se dispone en el art. 5.1.b) RGPD,

> "los datos personales serán:
>
> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; [...]".

El principio de limitación de la finalidad que se enuncia en este precepto quedaría de alguna forma un poco diluído con la previsión del art. 6.4 RGPD. Este último precepto permite que los datos sean tratados para otro fin distinto de aquel para el que se recogieron los datos personales.

> El art. 6.4. RGPD dispone: "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: [...]"

Para aplicar este precepto, debe darse como presupuesto que el nuevo tratamiento no esté basado en el consentimiento del interesado ni en el derecho de la Unión o de los Estados miembros.

> Se entiende que si ya hay consentimiento, no hace falta mayor justificación porque el consentimiento es el que da cobertura al tratamiento y si se trata de una norma esta es la que habilita el tratamiento, por lo tanto, no es preciso ninguna otra causa de justificación.

En estos casos se atribuye al RT la facultad de valorar (podría decirse que la responsabilidad) si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales.

Para ello, se tendrá en cuenta, entre otras cosas[25], según dispone el art. 6.4 RGPD:

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 el que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

(25)Resulta un tanto sorprendente que se diga "entre otras cosas", de modo que parece que la lista de elementos a considerar no sea cerrada y que se trate por lo tanto de una valoración subjetiva del 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.

Nota

Recuérdese lo que se ha dicho anteriormente en relación con los principios de protección de datos y el hecho que el RGPD parece relativizar un poco la "incompatibilidad" respecto a las finalidades.

El RT deberá valorar si el uso de otra finalidad es compatible o no. ¿Cómo valorará el RT si el cambio de finalidad es posible o no? El parámetro y criterio lo proporciona, como ya se ha dicho, el art. 6.4 RGPD, si bien la aplicación de este precepto muy probablemente generará dudas tanto a los RT como a las propias APD.

3.5. En particular: el consentimiento

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

3.5.1. Características del consentimiento

El art. 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[26]".

[26]El art. 6.1 LOPDIGDD recoge esta definición de consentimiento.

Consentimiento

"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 la misma finalidad. 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" (Considerando 32 RGPD).

Es preciso subrayar que las Propuestas de la Comisión 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).

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 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.

> Piénsese en las numerosas ocasiones en que bien para instalar una app en el móvil, bien para consultar una información o acceder a un servicio, se pide el consentimiento al afectado. Ello se hace de forma 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 art. 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 DP.

Por ejemplo, el afectado recibe una comunicación en 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. En base al art. 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.

En el marco de la LOPD de 1999, el art. 14 del Reglamento que la desarrolló (RLOPD), atribuyó precisamente unas consecuencias positivas al silencio si se cumplían determinados requisitos. El art. 14 RLOPD es claramente contrario al RGPD[27] y por lo tanto no puede resulta en ningún caso aplicable.

[27]Véase al respecto Llácer Matacás, que criticaba la solución ex. art. 14 RLOPD de atribuir valor positivo al silencio en el art. 14 RLOPD.

3.5.2. Condiciones para el otorgamiento del consentimiento

El art. 7 RGPD lleva por rúbrica "Condiciones para el consentimiento". En dicho precepto se regulan distintas previsiones relativas al consentimiento.

Acreditación del consentimiento: Art. 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.

Declaración escrita con distintos asuntos: Art. 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".

El punto de partida de este precepto lo constituye aquél supuesto en 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 ello es que el sujeto pueda conocer claramente qué se está solicitando y consentir una cláusula y, por ejemplo, rechazar otra.

El art. 6.2 LOPDGDD

Una medida parecida a esta es la que prevé el art. 6.2 LOPDGDD, según el cual, "Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas". En el caso de la legislación española no se hace referencia al hecho que se pida el consentimiento para diferentes cuestiones, sino que todas ellas afectarían el tratamiento de datos personales. Pero hay que identificar y separar cada una de estas finalidades.

Por ejemplo, se contrata un servicio de telefonía y en el contrato deben distinguirse las cláusulas que afectan 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). Muy a menudo la información es entremezclada, de forma que el afectado no sabe bien a qué consiente.

Revocación del consentimiento: Art. 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".

Retirar

El término *retirar* el consentimiento es el 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 arts. 13.2.c) y 14. 2.d) RGPD.

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

Prohibición de vinculación: Art. 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".

En el mismo sentido se pronuncia también el art. 6.3 LOPDGDD, según el cual: "No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual".

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 del mismo no puede supeditarse al hecho 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 necesarias para un determinado contrato, podrá hacerlo siempre y cuando: 1) 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 art. 7.3 RGPD; 2) 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. 3) que 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 art. 7.4 RGPD.

3.5.3. El consentimiento de los menores

El art. 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 da o autoriza el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se da o autoriza.
>
> 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.

La LOPDGDD también regula esta cuestión en el art. 7.

Artículo 7. Consentimiento de los menores de edad.

"**1.** El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela".

El art. 8 RGPD hace referencia a dos aspectos diferentes: 1) requisito de una determinada edad 2) verificación de este requisito.

1) Edad

La LOPDGDD, por la facultad que le otorga el art. 8.1.ii RGPD rebaja el umbral de edad para tratar los datos con el consentimiento del propio menor a los 14 años[28]

Sin embargo, hay que indicar que la regulación de la LOPDGDD[29] es más amplia que la del RGPD. Este último hace referencia a la oferta directa a niños de servicios de la sociedad de la información (SI), mientras que la primera, al no establecer ninguna limitación, alcanza cualquier tipo de tratamiento. La LOPDGDD 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 SI (por ejemplo, los datos digitalizados tratados por una escuela). Así mismo la LOPDGDD, a diferencia del RGPD[30] comprende tanto aquellos casos en que los servicios se ofrecen a los menores directamente, como cuando no es así.

Otra diferencia que presenta la LOPDGDD es que contempla una excepción a la posibilidad que los menores que tienen 14 años puedan otorgar su consentimiento por sí solos. Concretamente el precepto prevé que: "Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento" (art. 7.1.ii LOPDGDD). El supuesto parece contemplar la existencia de dos negocios jurídicos diferentes. Por ejemplo, un negocio patrimonial (adquisición de un teléfono móvil) y un negocio de tratamiento de datos. El precepto parece indicar que si para el negocio principal (adquisición de un móvil) fuese necesaria la asistencia de los titulares de la patria potestad o tutela, para el tratamiento de los datos ligado al negocio principal no resultaría aplicable la edad de los 14 años (y por lo tanto el simple consentimiento del menor), sino que sería necesaria la asistencia de los titulares de la patria potestad o tutela. Dicho de otro modo, que en estos casos puede ser que se requiera o bien la asistencia de los representantes legales para tratar los datos, o que se exija más edad que no los 14 años.

Por debajo de los 14 años, si el tratamiento se basa en el consentimiento, el tratamiento solo será lícito si consta el consentimiento del titular de la patria potestad o tutela (art. 7.2 LOPDGDD).

2) Verificación de la edad

Otro aspecto es como se verifica la edad del menor. El art. 8.2 RGPD dispone que "El responsable del tratamiento tiene que hacer esfuerzos razonables para verificar en estos casos que el consentimiento ha sido dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible".

La LOPDGDD no establece nada al respecto, por lo cual será aplicable directamente este precepto.

La aplicación del art. 8 en realidad implica dos verificaciones diferentes y complementarias: verificar la edad del niño y verificar, en el supuesto de que el menor no llegue a los 16 años o la edad fijada por cada Estado, que el consentimiento fue dado o autorizado por los que tienen la representación legal del menor.

En cualquier caso, para poder verificar que el afectado supera la edad fijada, el GT29 señala que las medidas establecidas tienen que ser proporcionales a la naturaleza y riesgos de las actividades de tratamiento (GT29, WP 259, § 7.1.3). El RT podrá llevar a cabo comprobaciones necesarias para verificar que la declaración efectuada es cierta (si un

(28)El Proyecto de LOPD presentado el 2017 establecía el límite de los 13 años, pero este se aumentó en 1 año en la fase de enmiendas a la Ley.

(29)En el marco de la LOPD de 1999, esta cuestión se regulaba en el artículo 13.1 RLOPD. Pero actualmente, resulta aplicable el art. 7 LOPDGDD.

(30)Hay que recordar que el art. 8 RGPD hace referencia a "la oferta directa a niños de servicios de la sociedad de la información".

niño da su consentimiento a pesar de no tener edad para prestar el consentimiento válido en su propio nombre, el tratamiento de los datos no será lícito (GT29, WP 259, § 7.1.3).

Sin embargo, como sostiene el GT29, la verificación de la edad no tiene que conducir a un tratamiento excesivo de datos. En caso de que el menor diga que no tiene la edad necesaria, el RT tendrá que obtener la autorización de los padres y verificar que la persona que da el consentimiento es el titular de la patria potestad o tutela (vid GT29, WP 259, § 7.1.4). En cualquier caso, es necesario un enfoque proporcionado, de acuerdo con el Principio de minimización de datos.

Sin embargo, para acabar de conocer cuál es el marco de actuación del menor de edad respecto al tratamiento de los datos personales que lo conciernen, hay que tener en cuenta otros preceptos contenidos en la LOPDGDD, especialmente los arts. 84 y 92 LOPDGDD.

El art. 84 LOPDGDD dispone que:

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor".

Según el 2.º párrafo, la utilización/difusión de imágenes que puedan constituir una intromisión ilegítima determina la intervención del Ministerio fiscal. Esta referencia está estrechamente ligada a la LO 1/1996, de protección del menor. Concretamente el art. 4.3 de la misma. Este precepto establece que:

"Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales".

Por lo tanto, el término es muy amplio, en la medida que incluye cualquier actuación contraria a sus intereses. Cfr, un menor por ejemplo que salga bebiendo alcohol o en una fiesta en determinadas actitudes provocativas. Pero sin duda queda mucho margen a la interpretación judicial. (Cfr, ¿un chico de 15 años, con ropa interior, supone una imagen contraria a sus intereses? ¿Y si se encuentra en la playa con muy poca ropa? Seguro que gran parte de las imágenes de los menores que se cuelgan en Instagram o Facebook no pasarían este control de "contrario a sus intereses").

En estos casos, la utilización de la imagen o la difusión de la misma o de la información personal no podrá ampararse en el consentimiento del menor (aunque tenga más de 14 años), ni tampoco el consentimiento de los titulares de la patria potestad o tutela. En definitiva, aquello que prima es que el uso de esta información no pueda resultar perjudicial para el menor. La clave se encuentra en el interés superior del menor (art. 2 LO 1/1996).

También hay que atenerse a lo que establece el art. 92 de la LOPDGDD:

"Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica".

En cuanto a los incapacitados, hay que destacar que ni el RGPD ni la LOPDGDD hacen referencia en ningún caso al supuesto de los incapacitados. Posiblemente la sentencia de incapacitación establecerá algo al respecto, pero ¿y si no dice nada sobre este tema? Piénsese en todos los datos de salud de los incapacitados, ¿quién tiene que autorizar el tratamiento de estos datos? A falta de una norma sobre este tema, y si la sentencia no determina nada, tendría que otorgarse al incapacitado la facultad de poder consentir, con base en el principio que la limitación de la capacidad tiene que interpretarse siempre en el sentido menos restrictivo posible.

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

Como ya se ha indicado al analizar el término *dato*, la gran mayoría de textos legales que regulan el tratamiento de datos personales establecen una distinción entre tipos de datos, de modo que se considera que determinada información debe gozar de una mayor protección. 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 RGPD, dentro de los datos personales distingue y separa unos, los que califica como "especiales". Sin embargo, como ya ha sido expuesto, esta no es la única solución por la que habría podido optar el legislador. Otra posible solución sería reconocer y establecer *tipos o categorías de tratamientos*, de modo que el dato en sí no fuera lo que determinara un régimen u otro, sino el tipo de tratamiento (en base a la finalidad del mismo o las circunstancias en que tuviera lugar). Sin embargo el RGPD sigue el mismo patrón que la DPD al establecer tipologías de datos.

Datos especiales

El art. 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 del mismo. Estos datos especiales se conocen también como datos sensibles.

1) Datos que tienen la categoría de especiales (art. 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)[31].

[31] Al respecto leed el Considerando 51 del RGPD.

A continuación se exponen las principales diferencias entre el art. 8 DPD y el art. 9 RGPD.

Definición de datos

Véase la definición de todos los tipos datos en el art. 4 RGPD.

En el RGPD se incluyen nuevas categorías de datos respecto 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 el término dato genético comporta que ya no hay dudas acerca de que quedan protegidos de forma especial todos estos tipos de datos.

En otros supuestos se produce una variación de la redacción y de los términos utilizados.

Concretamente en cuanto a los datos relativos a la sexualidad (DPD), el RGPD establece: datos relativos a la vida sexual *o la orientación sexual* de una persona física. Por lo tanto, este último supuesto es más amplio que el de la DPD.

Otra categoría a tener en cuenta es la relativa a los datos respecto condenas e infracciones penales. Este tipo de datos si bien no son calificados como datos sensibles, sí tienen unas peculiaridades en cuanto a su tratamiento. El art. 10 RGPD 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, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".

Si bien la solución que proporciona el RGPD respecto las condenas e infracciones penales y medidas de seguridad es muy similar a la de la DPD, *no ocurre lo mismo en cuanto al tratamiento de datos relativo a sanciones administrativas o procesos civiles*. El texto 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". El RGPD nada dice al respecto.

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 preveía en el art. 8 DPD, el art. 9 RGPD parte de un principio prohibitivo del tratamiento de los datos sensibles. El art. 9.1 RGPD determina que "quedan prohibidos el tratamiento de datos personales que revelen [...]".

Sin embargo, tras establecer esta prohibición tan radical[32], se establece: "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 este precepto enumera a continuación.

[32]En cuanto al levantamiento de la prohibición de tratar estos datos particularmente sensibles, véanse los Considerandos 52 a 56 del RGPD.

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

Art. 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 art. 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 que no será tan automática la prestación del consentimiento.

En cuanto a las diferencias entre el contenido del art. 8 DPD y art. 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 1er párrafo de los respectivos artículos. Así en la DPD se disponía: "no se aplicará cuanto", 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 art. 8.4 DPD determinaba 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 art 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 cuanto "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 art. 8.4 DPD y la del art. 9.2.g) RGPD, algunos de los cuales son relevantes.

Excepciones en el tratamiento de datos

Si bien la DPD determinaba que son los Estados quienes podrán establecer otras excepciones, con lo que se deduce que como mínimo deberá adoptarse una disposición o regulación en que se ponderen los derechos en juego y especialmente la adopción de las garantías adecuadas, en cambio, en base al texto del RGPD parece ser que sin necesidad de adoptar esta disposición, pueden establecerse excepciones si concurre una circunstancia concreta: que el tratamiento sea necesario por razones de un interés público esencial. Sin embargo, no se determina ni quién debe llevar a cabo esta valoración, ni cómo debe adoptarse (mediante qué instrumento). Sólo 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 art. 9.2.g) RGPD podría incluso interpretarse en el sentido de que es el RT quien puede adoptar la decisión de tratar los datos en base a lo que él considerara un interés público esencial. Esta solución no parece la más adecuada. En cambio, del texto de la DPD parecía más claro que se tenía que adoptar una medida legislativa antes de poder introducir otra excepción.

En este sentido se considera positiva la referencia que hace el art. 9.2 LOPDGDD, que determina que los tratamientos que se mencionan tienen que estar amparados en una norma con rango de Ley. Dispone este precepto que: "2. Los tratamientos de datos que prevén las letras g), h) y i) del artículo 9.2 del Reglamento (UE) 2016/679 fundamentados en el derecho español tienen que estar amparados en una norma con rango de ley, que puede establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, esta norma puede amparar el tratamiento de datos en el ámbito de la salud

cuando así lo exija la gestión de los sistemas y los servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

Además, la redacción de la DPD establecía una ulterior garantía, en la medida que, según se disponía en el art. 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, la misma 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 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 ello 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.

Considerando 54 RGPD, DA 17.2 de la LOPDGDD

Al respecto, tened en cuenta el Considerando 54 RGPD. Véase también la DA 17.2 de la LOPDGDD, que establece una serie de criterios en relación con el tratamiento de datos en la investigación en la salud. También hay que tener en cuenta la Disposición transitoria 6.ª que hace referencia a la reutilización de los datos con finalidades de investigación en materia de salud y biomedicina, respecto a datos recogidos con anterioridad a la entrada en vigor de la LO 3/2018. Finalmente hay que tener presente la Disposición final 9.ª, que modifica la Ley 41/2002, de 14 de noviembre, en cuanto al acceso a la historia clínica.

4) Así mismo, en el RGPD se contemplan nuevos supuestos recogidos en los arts. 9.2.f); 9.2.h); 9.2.i) y 9.2.j) RGPD.

La LOPDGG regula expresamente la posibilidad de levantar la excepción contemplada en el art. 9.2.a) RGPD. Se trata concretamente de la excepción según la cual mediante el consentimiento explícito del afectado se puedan tratar categorías especiales de datos.

La Ley española (art. 9.1 LOPDGDD) es restrictiva en la medida que determina que el mero consentimiento del afectado **no es suficiente** para **levantar la prohibición del tratamiento** cuya finalidad **principal sea** identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Concretamente el art. 9.1 LOPDGDD dispone que:

"**1.** A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, 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.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda".

En cuanto a esta restricción (art. 9.1 LOPDGDD), hay que tener en cuenta que:

i.- No afecta a todos los datos contemplados como especiales *ex* art. 9.1 RGPD.

ii.- La finalidad es la de evitar situaciones discriminatorias.

iii.- Contempla los tratamientos que tienen una determinada finalidad: "identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico".

Por lo tanto, sí que se permite el tratamiento de este tipo de datos en otros casos contemplados en el art. 9.2 RGPD. Por ejemplo, el supuesto regulado en el art. 9.2.b) RGPD, cumplimiento de obligaciones y ejercicio de derechos en el ámbito laboral, o bien el art. 9.2.d) RGPD, tratamiento efectuado por parte de fundaciones o asociaciones sin ánimo de lucro cuya finalidad es política, filosófica, religiosa o sindical.

En cuanto al tratamiento de los datos relativos a la ideología, y más concretamente respecto a las opiniones políticas, y en la medida que el simple consentimiento del afectado no es suficiente (art. 9.1 LOPDGDD), la Disposición final 3.ª de la LOPDGDD modificó la Ley orgánica 5/1985, de 19 de junio, del régimen electoral general (LOREG).

Una de estas modificaciones es la introducción de un nuevo artículo 58-bis con el contenido siguiente:

"Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales está amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

2. Los partidos políticos, las coaliciones y las agrupaciones electorales pueden utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la práctica de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tienen la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas referidas anteriormente tienen que identificar de manera destacada su naturaleza electoral.

5. Se tiene que facilitar al destinatario una manera sencilla y gratuita de ejercicio del derecho de oposición."

Este precepto levantó bastante polémica. Tanto es así que la AEPD publicó la Circular 1/2019, de 7 de marzo, que establecía unas pautas relativas a la interpretación de este precepto.

Se trata de la "Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General", publicada en el BOE n.º 60 de 11 de marzo de 2019.

El TC, el 12 de marzo de 2019 admitió a trámite el recurso de inconstitucionalidad promovido por el Defensor del Pueblo contra el artículo 58 bis.1 de la Ley Orgánica 5/1985, de 19 de junio, del régimen electo-

ral general, incorporado a esta Ley orgánica por la disposición final tercera, punto dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (n.º de asunto 1405-2019). Vid: https://www.tribunalconstitucional.es/notasdeprensadocumentos/np_2019_029/p%201405-2019.pdf. El TC, en la STC 76/2019, de 22 de mayo de 2019 estimó el recurso de inconstitucionalidad y declaró nulo el precepto impugnado. Al respecto véase el BOE núm. 151 de 25 de junio de 2019.

Así mismo hay que tener en cuenta, en cuanto a los tratamientos relativos a "categorías especiales de datos", la previsión específica del art. 9.2. LOPDGDD. Este precepto determina que: "Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

3.6. Los sujetos que participan en el tratamiento de datos

En cuanto al ámbito subjetivo, resulta oportuno distinguir entre aquellos sujetos que **participan en el tratamiento** y aquellos otros que lo **supervisan** (las autoridades de protección de datos y el DPO). El primer aspecto se analiza en este apartado y el segundo en el siguiente.

El estudio de los sujetos que participan de un tratamiento puede analizarse desde la perspectiva de una relación jurídica. Dicha relación está integrada en uno de los extremos por el responsable del tratamiento y en el otro por el afectado o interesado (el sujeto a quien hacen referencia los datos objeto de tratamiento). En la mayoría de los tratamientos también pueden participar en dicha relación el encargado o subencargado y asimismo puede hallarse el (los) destinatario (s) y los terceros.

3.6.1. Los sujetos que tratan los datos personales

El RGPD no ha introducido demasiados cambios al respecto, y ello puede ser criticable. De hecho, se produce prácticamente una continuidad en este ámbito entre la regulación de la DPD y el RGPD.

Para algunos autores, resulta cuestionable el hecho de que se mantenga la distinción entre responsable y encargado del tratamiento, asignando al primero la responsabilidad principal. Ello no parece la solución más adecuada en un contexto en el que hay muchos sujetos que intervienen y no siempre es fácil identificar la responsabilidad de cada uno:

1) Por un lado, en determinados contextos, por ejemplo en la computación en la nube, no es cierto que el denominado "responsable" tenga facultad de dirigir y decidir siempre la finalidad y la evolución del tratamiento.

2) El hecho de mantener la distinción en los términos establecidos parece que sea más un mecanismo de proporcionar salida a los distintos actores/responsables potenciales y de eludir sus responsabilidades. De esta forma, el sujeto afectado se verá confundido posiblemente por no saber exactamente a quién demandar.

3) Algunos autores (De Hert, por ejemplo), consideran que todo aquel que trata los datos debería tener un mismo nivel de responsabilidad y no encuentran justificación en que aquellos que participan de alguna manera en el tratamiento de la información personal no deban hacer frente a sus respectivas responsabilidades.

El único elemento que valora favorablemente es la introducción de la responsabilidad solidaria.

En definitiva, se trata de un esquema (los sujetos existentes y la distribución de sus responsabilidades) ya un poco anacrónico, que no daría respuesta efectiva a la relación que se establece actualmente y que permite eludir responsabilidades en según qué casos a aquellos que tratan DP.

A continuación se analizará el régimen jurídico al que están sometidos los sujetos que tratan los DP según el RGPD.

Responsable del tratamiento (RT)

El art. 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**; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

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

El RGPD especialmente contempla y hace referencia a los supuestos en los que exista más de un RT, de modo que en este caso dichos sujetos serán considerados como corresponsables del tratamiento. Así lo establece el art. 26 RGPD, según el cual,

> "cuando dos o más responsables **determinen conjuntamente** los **objetivos y los medios** del tratamiento serán considerados **corresponsables** del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos[33] [...]" (art. 26.1 RGPD).

(33)Véase el art. 29 LOPDGDD, relativo a los "Supuestos de corresponsabilidad en el tratamiento, y que establece: La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento".

Dicho acuerdo reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados, y los aspectos esenciales de dicho acuerdo se pondrán a disposición del interesado (art. 26.2 RGPD).

Sin embargo, con independencia de los términos del acuerdo, los interesados podrán ejercer los derechos que les reconoce el reglamento frente a, y en contra de, cada uno de los responsables (art. 26.3 RGPD).

Por lo tanto, el art. 26.3 RGPD parece dar a entender que en las relaciones externas, ante los afectados por el tratamiento, se establecería un tipo de responsabilidad solidaria, de modo que cualquiera de los RT respondería del cumplimiento de todas las obligaciones. Esto es, los pactos internos a los que pudieran llegar, de distribución de sus respectivos cometidos y responsabilidades, no afectarían a la esfera externa y al ejercicio de los derechos por los afectados.

En cuanto a las funciones que lleva a cabo el RT, estas se pueden agrupar teniendo en cuenta básicamente tres momentos:

- un primer momento, en el que se planifica (proyecta) el tratamiento y se determinan los medios del tratamiento,
- un segundo momento, en el que se efectúa el tratamiento, y
- el tercer momento, de finalización del tratamiento.

Antes de analizar las funciones del RT y las distintas etapas en las que interviene, es preciso tener en cuenta el cambio de perspectiva que ha supuesto el RGPD en relación con la posibilidad de iniciar un tratamiento de datos.

En el marco de la Directiva (DPD) era preciso, como regla general, notificar a la autoridad de control con anterioridad a la realización de un tratamiento (art. 18.1 DPD) la voluntad de llevarlo a cabo. No obstante, en algunos casos los Estados podían disponer la simplificación o la omisión de dicha notificación

(art. 18.2 DPD) o que algunos tratamientos fueran notificados eventualmente de una forma simplificada (art. 18.5 DPD). El art. 19 DPD hacía referencia al contenido de dicha notificación.

Si bien en el marco de la LOPD de 1999 había que inscribir los ficheros, la perspectiva del RGPD es distinta: en principio, se puede proceder al tratamiento de datos asumiendo el RT una serie de obligaciones. En el marco del RGPD, si se dan las condiciones de legitimación previstas (arts. 5 y 6 RGPD), el tratamiento puede llevarse a cabo. En todo caso el RT, al iniciar el tratamiento, debe tomar una serie de prevenciones y tiene que asegurarse de que cumple con la normativa. Asimismo, deberá poder acreditar que ello es así en el caso de que se someta a un control por parte de la autoridad competente (principio de responsabilidad proactiva, *ex* art. 5.2 RGPD).

Art. 5.2

"El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)".

El RT, por lo tanto, debe ser consciente de lo que quiere llevar a cabo y valorar, antes de iniciar un tratamiento, qué estrategia seguir (*cfr*. debe sospesar adecuadamente qué datos necesita, cómo los tratará y adoptar la tecnología que sea más adecuada).

Asimismo, cuando sea necesario, deberá llevar a cabo una valoración del impacto que respecto a la privacidad puede comportar el tratamiento de datos que pretende realizar (*privacy impact assessment*). Evaluación del impacto relativa a la protección de datos (art. 35 RGPD)[34].

[34]Véase art. 28.1 LOPDGDD. El hecho de no llevar a cabo la evaluación de impacto puede constituir una infracción grave de la normativa (art. 73.t. LOPDGDD).

También deberá implementar desde un primer momento medidas de privacidad basadas en el diseño (art. 25 RGPD) y en según qué casos proceder a la consulta previa ante la autoridad de control[35] (art. 36 RGPD).

[35]Según el art. 73.d) LOPDGDD, se considera una infracción grave "La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679". Por otro lado, en cuanto a la consulta previa en el marco de la LOPDGDD, vid art. 28.1.

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

Por lo tanto, 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.

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 que sean necesarias.

El conjunto de las obligaciones que corresponden al RT vienen definidas por esta nueva perspectiva a la que se ha hecho referencia y que representa un cambio de filosofía que puede identificarse como: "de la notificación previa, al principio de *accountability*, es decir, al principio de responsabilidad proactiva".

Los deberes de notificación establecidos en la DPD pronto se descubrieron un tanto inútiles, especialmente teniendo en cuenta la infinidad de tratamientos llevados a cabo. Además, la idea originaria de que existiría un tratamiento acotado en un determinado país, bajo una autoridad de control, quedaba superada. Por ello, al poco tiempo de adoptarse la directiva se consideró que este sistema quedaba un tanto obsoleto.

En el texto del RGPD simplemente no es que se haya reemplazado técnicamente la notificación por otras disposiciones. Pero *de facto* se puede decir que ha sido sustituida por el deber de *accountability*.

Esto es, en definitiva se produce una inversión de la carga de la prueba: si antes el RT debía acreditar que cumplía ante la autoridad, ahora se trata de desarrollar diligentemente todas las funciones encomendadas al RT. Entre dichas funciones destaca: "guardar un registro" de los tratamientos efectuados, adoptar una serie de medidas (*privacy impact assessment* cuando proceda, más la adopción de medidas tecnológicas que sean *privacy friendly*, o realizar una consulta ante la autoridad de protección de datos competente) y a partir de ello poder demostrar que se cumple con la normativa de protección de datos cuando sea requerido.

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. A la hora de adoptar determinadas medidas, por ejemplo, llevar a cabo una evaluación de impacto o plantear una consulta previa ante la Autoridad de control, tiene que tener en cuenta determinados riesgos a que se puede ver sometido el tratamiento (art. 28.2 LOPDGDD).

En consecuencia, ello implica:

1) Antes de iniciar el tratamiento:

- verificar que se cumple con la normativa de protección de datos,
- respetar los principios de protección de datos,
- verificar si el tratamiento es lícito (existe un fundamento legal para él),
- 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*),

- cuando sea necesario, realizar la consulta previa a la autoridad de protección de datos competente,
- dotarse de los medios técnicos y personales adecuados, y
- en caso de elegir a encargados del tratamiento, realizarlo con la debida diligencia y formalizar un contrato u otro negocio jurídico.

En cualquier caso, debe tenerse en cuenta el cambio de perspectiva que representa la adopción del RGPD. Uno de los principios básicos del nuevo marco legal es el de *data protection by design* y *data protection by default*.

El RGPD establece nuevas obligaciones para implementar las medidas tecnológicas que favorezcan la privacidad desde el primer momento de la concepción de un producto/servicio que comporte el tratamiento de información personal. También deben seleccionarse las técnicas que son más protectoras de la protección de la privacidad de un sujeto. Principios todos ellos que son fundamentales para las empresas en el momento de diseñar nuevos productos.

2) Durante el tratamiento:

- adoptar una serie de garantías,
- llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, con la información exigida en el art. 30.1 RGPD,
- dotarse de los medios técnicos y personales adecuados,
- en caso de elegir a encargados del tratamiento, realizarlo con la debida diligencia y suscribir un negocio jurídico,
- adoptar las medidas de seguridad necesarias,
- cumplir con las obligaciones propias del responsable,
- dar respuesta al ejercicio de los derechos por parte del afectado/interesado, y
- poder demostrar que se cumple con la normativa (principio de responsabilidad = *accountability*). Entre las formas de acreditar que se está cumpliendo debidamente con la normativa cabe destacar:
  - el hecho de tener un *privacy seal*,
  - estar vinculado por unas BCR y cumplirlas.

3) Al finalizar el tratamiento:

- determinar si deben suprimirse los datos o bien limitarse el tratamiento de estos,
- hacer frente al posible ejercicio de acciones por parte del afectado/interesado y
- valorar si se pone fin a la relación con el ET y en todo caso ver cómo se finaliza esta (si deben o no devolverse los datos).

¿Cuál es el marco de actuación del RT? Según se dispone en el art. 24.1 RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

Por lo tanto, el RT debe adoptar una serie de medidas en relación con el tratamiento.

Para ello, ¿qué elementos debe tener en cuenta? Debe tenerse en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento, así como los riesgos de diversa probabilidad/gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas (art. 24.1 RGPD), y también el estado de la técnica y el coste de la aplicación de dichas medidas (art. 25.1 RGPD). Tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, el RT actúa y toma decisiones teniendo en cuenta una serie de elementos: el estado de la técnica, el coste de la aplicación y la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas (art. 25.1 RGPD). Por lo tanto, estos elementos le servirán al RT como "parámetro" para determinar si se ha actuado adecuadamente y también lógicamente serán tenidos en cuenta a la hora de evaluar cómo ha desempeñado su labor[36].

[36]Véase art. 28.2 LOPDGDD.

¿Qué medidas deben adoptarse? El RT aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas (art. 24.2 y 25.1 RGPD), y entre las medidas técnicas y organizativas apropiadas se señala la seudonimización. Estas medidas apropiadas tienen como objetivo aplicar de forma efectiva los principios de protección de datos. Entre estos principios se destaca el principio de minimización de los datos, para de este modo poder integrar las garantías necesarias en el tratamiento (art. 25 RGPD).

Y sobre la base de estos parámetros, el RT adopta medidas técnicas y organizativas apropiadas. Concretamente se consideran como tales

> "la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados" (art. 25.1 RGPD).

Asimismo, se considera un elemento clave, a la hora de tomar las medidas que se consideren oportunas, el respeto a los principios de protección de datos. Singularmente, los principios de minimización de los datos:

Art. 25.2

"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas" personas físicas[37].

(37)Constituye una infracción grave de la LOPDGDD "La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento [...]" (art. 73.e). LOPDGDD).

Por lo tanto, el principio de minimización deberá cumplirse en distintos momentos y respecto a distintos aspectos:

- La cantidad de datos recogidos.
- La extensión del tratamiento.
- El plazo de conservación/accesibilidad.

Y todas estas medidas, ¿para qué? A fin de garantizar y poder demostrar que el tratamiento es conforme con el reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario (art. 24.1 RGPD) y a fin de cumplir los requisitos del presente RGPD para proteger los derechos de los interesados (art. 25.1).

Art. 25.3.

"Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

Por otro lado, debe tenerse en cuenta que en aquellos casos en los que el RT o el encargado del tratamiento (ET) no estén establecidos en la Unión, deberán designar un representante en la Unión, según dispone el art. 27 RGPD. Este precepto también prevé supuestos en los que no es preciso designar dicho representante, y en cualquier caso, su designación se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado (art. 27.5 RGPD).

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

1) Llevar un registro. Dentro del deber de diligencia del tratamiento de los DP se encuentra el deber de llevar un registro de las actividades de tratamiento efectuadas.

El art. 30 RGPD ("Registro de las actividades de tratamiento") dispone que:

"**1.** Cada responsable o su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad".

Art. 30.3.

"Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico".

Art. 30.4.

"El responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de control que lo solicite".

Art. 30.5.

"Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10".

En el marco de la LOPDGDD, el art. 31 establece el deber de responsables y encargados del tratamiento de mantener un registro de las actividades, tal y como se establece en el art. 30 RGPD. Por otro lado, en el supuesto de que se designe un delegado de protección de datos, habrá que comunicarle cualquier adición, modificación o exclusión en el contenido del registro (art. 31.iii LOPDGDD). Así mismo constituye una infracción grave según la LOPDGDD, el hecho de no disponer de un Registro de actividades del tratamiento (art. 73.n. LOPDGDD).

2) Cooperar con la Autoridad de control. El RT debe cooperar con la Autoridad de control cuando esta lo solicite. Así lo dispone el art. 31 RGPD:

Artículo 31

"El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones[38]".

[38]Constituye una infracción grave el hecho de no colaborar con la autoridad de control (art. 73.o. LOPDGDD).

3) Deberes relacionados con la seguridad. En cuanto a los deberes de seguridad, el RGPD introduce una nueva perspectiva: la del riesgo. En base a esta corresponde al RT identificar los riesgos a que puede estar sometido el tratamiento de la información personal para poderlos prevenir.

La aproximación basada en el riesgo consiste en ajustar las obligaciones relativas al tratamiento de datos a los riesgos que presenta un determinado tratamiento a fin de establecer mecanismos adecuados de procesamiento de la información. Para esta valoración se tiene en cuenta la naturaleza, el contexto y la finalidad del tratamiento, así como la probabilidad y la gravedad de los riesgos que un tratamiento puede representar para los derechos y libertades de los individuos.

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 para los DP. En este sentido, se establecen obligaciones como la relativa a llevar a cabo un *data protection impact assessment*, el deber de notificar a los afectados las violaciones de datos o la consulta previa a las APD.

La perspectiva del riesgo aparece de nuevo en las disposiciones relativas a *privacy by design* y *by default*; la designación de un representante, requisitos relativos a la documentación del tratamiento, así como respecto a la adopción de las medidas de seguridad.

En este sentido, es preciso proporcionar una serie de guías y pautas a las empresas para que sean conscientes del nivel de riesgo que el tratamiento de datos personales puede suponer.

Artículo 32 Seguridad del tratamiento

"**1.** Teniendo en cuenta: el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que si procede incluya[39], entre otros:

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 personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. 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.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

(39)En el marco de la LOPDGDD constituye una infracción grave la falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento (art. 73.f. LOPDGDD) y el incumplimiento, como consecuencia de la falta de la diligencia debida, de las medidas técnicas y organizativas que se hayan implantado (art. 73.g. LOPDGDD).

Una novedad importante que ha introducido el RGPD es el deber de notificar las violaciones de seguridad, regulado en los arts. 33 y 34 RGPD.

- Estos preceptos distinguen entre, por un lado, el deber de notificar una violación de la seguridad de los datos personales a la autoridad de control (art. 33) y

- la comunicación de una violación de la seguridad de los datos personales al interesado (art. 34).

En cuanto a la notificación de la violación de la seguridad de los datos a la autoridad de control:

- La regla general es que en caso de una violación de la seguridad, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido *constancia de ella*, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación[40] (art. 33.1 RGPD).

(40)En el marco de la LOPDGDD constituye una infracción grave el incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo que prevé el artículo 33 del RGPD (art. 73.r. LOPDGDD).

- Asimismo, el encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de las que tenga conocimiento (art. 33.2 RGPD).

Art. 33.4 RGPD

"**3.** La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual".

El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo (art. 33.5 RGPD).

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

La comunicación al interesado no debe realizarse en todos los casos, sino "cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas", en cuyo caso el RT debe comunicarlo al interesado sin dilación indebida[41] (art. 34.1 RGPD).

[41]Constituye una infracción grave de la LOPDGDD, el incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo que prevé el artículo 34 del RGPD si el responsable del tratamiento ha sido requerido por la autoridad de protección de datos para llevar a cabo la notificación mencionada (art. 73.s. LOPDGDD).

La comunicación al interesado describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad y contendrá como mínimo la información y las medidas referidas en el art. 33.3 § b), c) y d) (art. 34.2 RGPD).

Como se ha indicado, no siempre debe cumplirse el deber de comunicación al interesado. Concretamente esta no será precisa si se cumple alguna de las condiciones siguientes (art. 34.3 RGPD):

a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

b) El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1.

c) Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle o bien que lo haga o bien la adopción de determinadas medidas (art. 34.4 RGPD).

4) La evaluación de impacto relativa a la protección de datos.

Otra novedad que incorpora el RGPD es la necesidad de llevar a cabo, en determinados supuestos, una evaluación del impacto relativa a la protección de datos. Esta medida se incardina en la filosofía a la que ya se ha hecho referencia, relacionada con el principio de responsabilidad proactiva[42] (art. 5.2 RGPD).

[42]Véanse al respecto art. 28 LOPDGDD y art. 73.t) LOPDGDD respecto a las consecuencias en el caso de no llevarse a cabo la mencionada evaluación.

Ya se ha señalado el cambio de perspectiva que ha supuesto el RGPD, de modo que se ha evolucionado de un deber de tener que pedir autorización para llevar a cabo un tratamiento, a la responsabilidad del RT que comporta, entre otros aspectos, valorar si se puede efectuar el tratamiento previsto y en todo caso cumplir con las exigencias legales.

Según dispone el art. 35 RGPD,

"**1.** Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto.

6. Antes de adoptar las listas la autoridad de control competente aplicará el mecanismo de coherencia si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a

d) las medidas previstas para afrontar los riesgos,

8. El cumplimiento de los códigos de conducta por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto.

[...]

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento".

***Privacy Impact Assessment* (PIA)**

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*) y proviene del derecho medioambiental y de la responsabilidad por los daños al medio ambiente. La evaluación de impacto deberá llevarse a cabo, según el parecer del propio responsable del tratamiento, y según su valoración personal, cuando dicho responsable considere que el tratamiento puede comportar un riesgo relevante respecto a los derechos y libertades del sujeto. Los casos en los que ello puede suceder están listados en el RGPD; asimismo, existen unos casos en los que ya de por sí existe dicho riesgo. Se trata de supuestos de *profiling*, o de realización sistemática de seguimiento de la persona. También en el tratamiento de datos sensibles.

En cualquier caso, el PIA debe hacerse antes de llevar a cabo el tratamiento.

La evolución del texto, desde su presentación por parte de la Comisión, ha sufrido pocos cambios. Quizá lo más remarcable es la posibilidad de llevar a cabo PIA por sectores, de modo que las PYMES no sufran demasiados perjuicios por el coste que estos PIA comportan. Concretamente se dispone que un solo PIA (una sola valoración) puede ser suficiente para tratamientos parecidos que presentan un riesgo similar. Por ello, se dispone que algunos PIA pueden tener un alcance horizontal, a fin de cubrir operaciones similares de tratamiento, asumiendo de alguna forma el papel de un código de conducta para un sector determinado.

Ello puede considerarse un intento muy positivo de aligerar la carga que tiene para las PYMES el coste financiero de la implementación del RGPD y proporcionar flexibilidad.

5) Consulta previa. Otra de las medidas relacionadas con este nuevo enfoque del rol del RT es la necesidad de llevar a cabo una consulta previa (art. 36 RGPD). Sin embargo, ello no supone una novedad tan radical si se tiene en cuenta que el art. 20 DPD ya preveía una medida similar[43] en determinados casos.

[43] Véase art. 28 LOPDGDD y art. 73. LOPDGDD respecto a las consecuencias en el caso de no efectuarse esta consulta previa.

El art. 20 Directiva 95/46 disponía que

"**1.** Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.

2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos, quien, en caso de duda, deberá consultar a la autoridad de control.

3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías".

El art. 36 RGPD prevé que:

"**1.** El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo es susceptible de prorrogarse.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

[...]

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública".

En cuanto a las diferencias entre el art. 20 DPD y art. 36 RGPD, quizá la diferencia más notable entre un supuesto y el otro es que en el caso de la DPD este deber de control pesaba sobre la autoridad de protección: "comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del RT [...]". En cambio, en el marco del RGPD parece que es el RT quien tiene que someterlo a dicha consulta. Esto es, que la iniciativa corresponde al RT en este último supuesto.

El art. 20 DPD hacía referencia a "controles previos", y el art. 36 RGPD a "consulta previa", pero existe algún elemento similar: el hecho de que ante determinados tratamientos, que son susceptibles de generar una mayor amenaza para los derechos y libertades de los sujetos, se deba consultar a la autoridad de protección de datos correspondiente.

6) Designación del encargado del tratamiento (ET).

En cuanto a la posibilidad de designar un ET, se debe tener en cuenta el art. 28 RGPD.

Art. 28.1.

"Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado".

Este aspecto se analizará en el subapartado siguiente. En definitiva, el art. 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 DP.

Según dispone el art. 28.1 RGPD, cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente a un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del reglamento y garantice la protección de los derechos del interesado[44].

(44)Hay que tener en cuenta que puede constituir una infracción grave de la LOPDGDD "la contratación por parte del responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas de conforme a lo establecido en el capítulo IV del RGPD" [art. 73.j] LOPDGDD).

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[45].

(45)En este sentido, puede constituir una infracción grave de la normativa estatal el hecho de encargar un tratamiento de datos a un 3.º sin la previa formalización de un contrato u otro acto jurídico escrito (art. 73.k) LOPDGDD.

Asimismo, según el art. 28.3 RGPD, dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32 (relativas a la seguridad del tratamiento);

d) en caso de recurrir a un subencargado del tratamiento, deberán respetarse las exigencias previstas en el art 28.2 y 28.4;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 (seguridad del tratamiento, comunicación de violación de seguridad y evaluación de impacto);

g) suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías.

En cualquier caso, el ET no es un mero ejecutor de las órdenes del RT, puesto que como dispone el art. 28.3. *in fine*

> "el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros".

Asimismo, en cuanto al contrato celebrado entre RT y ET, debe tenerse en cuenta que sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico podrá basarse, total o parcialmente, en las cláusulas contractuales tipo (art. 28.6. RGPD). Asimismo, dicho contrato o acto jurídico constará por escrito, inclusive en formato electrónico (art. 28.9).

En cuanto a la normativa estatal, hay que tener en cuenta, según el art. 73 LOPDGDD, que pueden constituir una infracción grave: (l) la contratación por un encargado del tratamiento de otros encargados sin contar con la au-

torización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles. (m) la infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

De la misma forma que el RT tiene la obligación de llevar un registro del tratamiento, el ET también debe hacerlo. Tal y como lo dispone el art. 30.2 RGPD, cada encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable[46], que contenga:

(46)Véase también art. 31 LOPDGDD.

a) el nombre y los datos de contacto del encargado y del RT por cuenta del cual actúe y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Tal y como se establece respecto al RT, dicho registro constará por escrito (incluso en formato electrónico), *ex* art. 30. 3 RGPD, y el ET lo pondrá a disposición de la autoridad de control que lo solicite (art. 30.4 RGPD).

En todo caso, debe tenerse en cuenta que la obligación de llevar el registro no será exigible a determinadas empresas u organizaciones.

Concretamente, no será exigible a aquellas que empleen a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos personales *ex* art. 9.1 RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el art. 10 RGPD (art. 30.5 RGPD).

La posibilidad que el ET recurra a otro ET (en definitiva, subcontrate sus funciones) está especialmente contemplada en el RGPD. Según dispone el art. 28.2, el ET puede recurrir a otro encargado si tiene la autorización previa por escrito, específica o general, del responsable. El ET informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al RT la oportunidad de oponerse a dichos cambios.

Según el art. 28.4 RGPD, cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante con-

trato u otro acto jurídico, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado (esto es, el primer contrato que se celebró), en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del RGPD. Si ese otro encargado (se trata de un subencargado) incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

En cuanto a la responsabilidad del ET, debe tenerse en cuenta que la adhesión del encargado del tratamiento a un código de conducta aprobado *ex*. art. 40 RGPD o a un mecanismo de certificación aprobado *ex*. art. 42 podrá utilizarse como elemento para demostrar la existencia de garantías suficientes (art. 28.5).

Asimismo, si un ET infringe el reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento (art. 28.10).

Sobre la obligación de diligencia en el tratamiento de datos hay que tener en cuenta que, finalmente, cualquier sujeto que trate datos debe hacerlo con una determinada diligencia. Esto es:

> "Los datos personales serán 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".

Este principio de integridad y confidencialidad se concreta en el art. 29 RGPD, que dispone que

> "el encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros".

En definitiva, en cuanto a la relación entre RT y 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 formato electrónico.

6) El fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado.

7) Obligación de informar al responsable "si, en su opinión, una instrucción infringe el presente Reglamento o las disposiciones nacionales o de la Unión en materia de protección de datos".

8) Posibilidad de utilizar contratos modelo.

Otros sujetos

El RGPD contempla la participación en el tratamiento de otros sujetos. El art. 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.

Ello está relacionado con los deberes de información. Al informar al sujeto afectado por el tratamiento, deben indicarse los posibles destinatarios de los datos. A estos efectos, las autoridades públicas no se consideran destinatarios y, por lo tanto, no debe informarse de la transmisión de datos a estas en los supuestos contemplados en el art. 4.9 RGPD.

Por otro lado, en cuanto a la figura del **tercero**, el art. 4.10) RGPD reconoce como tal: la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

3.6.2. 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 art. 4 RGPD, ninguna hace referencia al interesado o afectado (tampoco existía en el art. 2 DPD de 1995, en el elenco de definiciones que se proporcionan). 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.

Los interesados o afectados tienen una serie de derechos, que serán analizados más adelante. También cabe preguntarse hasta qué punto tienen deberes. Por ejemplo, ¿tienen el deber de proporcionar datos que no sean falsos? Asimismo, en determinados entornos, ¿tienen el deber de tratar los datos a los que tengan acceso –por ejemplo, redes sociales– de forma diligente? Parece que esta última cuestión no quedaría resuelta por el RGPD en la medida que esta norma excluye de su ámbito de aplicación los tratamientos con fines domésticos. Por lo tanto, los sujetos que participan en una red social a nivel doméstico (relaciones familiares o de amistad), quedarían fuera del conjunto de obligados a cumplir con los deberes que se exigen en el RGPD. En todo caso, los conflictos que se puedan suscitar deberán resolverse de acuerdo con las normas generales (por ejemplo, acudiendo o bien a las reglas relativas a la responsabilidad civil contenidas en el Código civil, o bien a la LO 1/82 en caso de lesionar los derechos al honor, intimidad o imagen de otro sujeto).

Algunos autores han defendido que los deberes de *accountability* también serían exigibles a los sujetos afectados por el tratamiento, esto es, que les sería exigible un determinado nivel de diligencia. Sin embargo, es una cuestión que no aparece abordada en el RGPD.

3.7. La supervisión del tratamiento

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

3.7.1. Las autoridades de protección de datos

El art. 8 de la CDFUE, tras reconocer que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan" (art. 8.1), dispone que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

Las autoridades de protección (APD) ya reguladas en la DPD (art. 28) constituyen un pilar básico en la implementación del reglamento, y por ello en dicho texto se incluyen un conjunto de artículos destinados a profundizar en su labor de coordinación para alcanzar la coherencia en la aplicación del reglamento en la UE.

El RGPD implica un reforzamiento del papel que desempeñan las autoridades de control. La regulación de estas se halla 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 art. 4.21 GDPR, la "autoridad de control" es la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.

Junto a las autoridades de protección, se crea el Comité Europeo de Protección de Datos (arts. 68 a 76), que sustituye al Grupo del art. 29, creado precisamente por el art. 29 DPD 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 DP (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, en función de dónde se halle el afectado y el RT (sección 2 del capítulo VI). A partir de estos criterios, en aquellos asuntos que afecten a más de un Estado se determina quién es la autoridad de control principal, que podrá recabar la ayuda de otras autoridades afectadas. Por ello, se establece un mecanismo de cooperación entre autoridades (arts. 60 a 62).

El art. 4.22 GDPR define "autoridad de control interesada" como la autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control.

En la medida en que las autoridades de protección deben tomar decisiones que pueden afectar a la aplicación uniforme del reglamento (por ejemplo, aprobación de códigos de conducta, determinación de tratamientos que requieren realizar una valoración del impacto, autorizar transferencias de datos), es preciso asegurar que las decisiones tomadas compartan unos mismos criterios. Para asegurarlo, se establece un procedimiento de coherencia (arts. 63 a 67), de tal modo que ante determinadas cuestiones y materias planteadas, las autoridades de control deberán pedir un dictamen del Comité Europeo de Protección de Datos y este comunicar determinadas decisiones a la Comisión.

En relación con los mecanismos de consistencia, es competencia del Comité Europeo de Protección de Datos establecer los criterios para lograr estos mecanismos de consistencia y de coherencia y cooperación. De modo que en muchos casos las autoridades deben solicitar la opinión previa de dicho Comité, y justificar si se apartan de su opinión.

Como ya se ha mencionado, el Capítulo VI del RGPD regula las autoridades de control independientes. En el marco de la legislación española, el Título VII de la LOPDGDD hace referencia a las Autoridades de protección de datos (arts. 44 a 62). Dentro del mencionado Título, el Capítulo I se dedica a la Agencia española de protección de datos y el Capítulo II a las Autoridades autonómicas.

Autoridades de control

También se ha hecho referencia al hecho que en el art. 51 LOPDGDD prevé que en un Estado miembro puedan existir una o varias autoridades de control.

En cuanto a la Agencia española, esta se rige por el RGPD, por la propia LOPDGDD y las disposiciones que la desarrollen (art. 45.1 LOPDGDD). El Gobierno, a propuesta de la AEPD, tiene que aprobar el Estatuto de la mencionada agencia[47] (art. 45.2 LOPDGDD).

[47]según se establece en la Disposición transitoria 1.ª LOPDGDD, "el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo que establecido en el Título VIII de esta ley orgánica"

Las funciones de la AEPD son las de supervisar la aplicación de la LO 3/2018 y del RGDP y ejercer las funciones previstas en los arts. 57 y 58 RGPD (art. 47 LOPDGDD).

Por otra parte, el art. 48 LOPDGDD regula la presidencia de la AEPD y establece nuevas reglas en cuanto a la elección de la presidencia (art. 48.3 LOPDGDD). También se regula el Consejo Consultivo de la mencionada agencia (art. 49 LOPDGDD).

En cuanto a las funciones específicas de la AEPD, los arts. 51 a 54 hacen referencia a las potestades de investigación y planes de auditoría.

Respecto a las autoridades autonómicas, sus competencias se regulan en el art. 57 LOPDGDD. Según determina este precepto, podrán ejercer las funciones y las potestades que establecen los artículos 57 y 58 del RGPD, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la comunidad autónoma correspondiente o de las entidades locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos que lleven a cabo personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la Administración autonómica o local correspondiente.

c) Tratamientos que estén previstos expresamente, si procede, en los estatutos de autonomía respectivos.

En el ámbito autonómico, existen las siguientes Autoridades de protección de datos que han desarrollado la normativa que a continuación se cita::

a) Autoridad catalana de protección de datos: https://apdcat.gencat.cat/ca/inici/.

En cuanto a la normativa reguladora de la Autoridad, hay que tener en cuenta el Estatuto de autonomía de Cataluña (especialmente el art. 31 que reconoce el derecho a la protección de datos personales) y el art. 156 que establece la competencia de la Generalitat en materia de protección de datos), 182.3); La Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos

(DOGC n.º 5731, de 8.10.2010) y el Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos (DOGC n.º 3835, de 04.03.2003).

b) Agencia Vasca de Protección de Datos: http://www.avpd.euskadi.eus/s04-5213/se/.

En cuanto a la normativa reguladora, véase 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.

c) En el caso de Andalucía, hay que tener en cuenta la Ley **1/2014**, de 24 de junio, de Transparencia pública de Andalucía, por la que se crea el Consejo de Transparencia y Protección de Datos de Andalucía. Sin embargo, actualmente únicamente se han asumido funciones de transparencia (https://www.juntadeandalucia.es/boja/2014/124/1), si bien está previsto que a partir de octubre de 2019 asuma también competencias en materia de protección de datos.

d) Por otro lado, la Comunidad de Madrid dictó la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid (BOCM de 25 de julio de 2001). Esta norma fue derogada por la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas (BOCM de 29 de diciembre de 2012), por lo cual la Agencia de Protección de datos de la Comunidad de Madrid se extinguió. www.madrid.org.

La LOPDGDD hace referencia a las relaciones entre las diferentes Autoridades de protección de datos (art. 58), al tratar de la cooperación institucional. Sin embargo, la AEPD tiene una clara supremacía y ejerce un rol de supervisión a nivel estatal, en la medida que, según dispone el art. 59 LOPDGDD, "Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

El Comité Europeo de Protección de Datos

El art. 29 DPD creó un grupo de protección de las personas respecto al tratamiento de datos personales, denominado Grupo del art. 29, que tuvo un carácter consultivo e independiente. La labor y rol llevado a cabo por dicho grupo fue de una grandísima relevancia. Sus integrantes eran miembros de las distintas APD nacionales, de modo que sus decisiones eran rápidamente seguidas por los distintos estados. Prueba de su influencia se halla en su papel relativo a múltiples cuestiones, desde el mismo concepto de dato de carácter personal, a las responsabilidades atribuidas al RT y ET, las posiciones adoptadas respecto al Internet de las cosas, el *big data*, el *cloud computing*, la delimitación del interés legítimo como causa de habilitación del tratamiento, la adopción de criterios respecto al ejercicio del derecho al olvido o la negociación de transferencias internacionales de datos tras la anulación del *safe harbour* (como consecuencia del caso Schrems).

Enlace de interés

Véase: https://edpb.europa.eu/about-edpb/about-edpb_es.

Sin embargo, tras la aprobación del RGPD, debía dotarse a este grupo consultivo e independiente de un nuevo marco, especialmente porque el RGPD se implementa en 29 estados y por ello es preciso garantizar la coherencia entre los distintos ordenamientos.

El art. 68 RGPD crea el Comité Europeo de Protección de Datos (European Data Protection Board), identificado como "Comité", como organismo de la Unión, que goza de personalidad jurídica. Dicho Comité está representado por su presidente y compuesto por el director de una autoridad de control de cada Estado miembro y por el supervisor europeo de protección de datos o sus representantes respectivos.

El mecanismo de coherencia adoptado funciona de tal modo que las APD, antes de adoptar decisión alguna importante, deben dirigirse al Comité, al que también se otorgan mecanismos para dirimir controversias entre las distintas autoridades implicadas.

Asimismo, el Comité conserva y amplía las facultades consultivas que tenía el Grupo del art. 29. Especialmente importante son las competencias relativas a certificación.

En general, puede decirse que el Comité se ha convertido en la autoridad y el cuerpo más importante en materia de protección de datos a nivel comunitario. Este refuerzo ha ido incrementándose respecto al texto inicialmente presentado por la Comisión. Esta, en la propuesta de enero de 2012 tenía reservado bastante poder y control y tenía en bastantes casos la última palabra mediante la posibilidad de dictar actos delegados. Paulatinamente, en el proceso de adopción del reglamento, el papel del Comité ha ido ganando peso e incrementándose. Quizá puede afirmarse que ha alcanzado el poder que la Comisión se había reservado para sí misma inicialmente.

3.7.2. 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.

El art. 37 RGPD regula en qué casos hay que designar un delegado de protección de datos (DPD). El RT y el ET designarán un DPD cuando:

a) El tratamiento lo efectúa una autoridad o un organismo público, a excepción de los tribunales que actúan en el ejercicio de su función judicial.

b) Las actividades principales del RT o del ET consisten en operaciones de tratamiento que, por razón de su naturaleza, de su alcance o de sus finalidades, requieren una observación habitual y sistemática de interesados a gran escala.

c) Las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos (art. 9 RGPD) o bien de los datos relativos a condenas e infracciones penales (art. 10 RGPD).

Por otro lado, un grupo empresarial puede nombrar un único delegado de protección de datos (art. 37.2 RGPD) y cuando el RT o ET sea una autoridad o un organismo público, se puede designar un único delegado de protección de datos para varias de estas autoridades u organismos (art. 37.3 RGPD).

El RGPD no regula qué tipo de titulación debe tener el sujeto que desempeñe las funciones de DPD. En cualquier caso, deberá tratarse de personas cualificadas, que tengan un potencial liderazgo en el seno de las organizaciones. El objetivo es que el DPD conozca bien los flujos de información personal y su gestión en el seno de una organización para protegerla en todas las fases del tratamiento y garantizar los derechos de las personas que el RGPD otorga.

Asimismo, la normativa obliga a la divulgación de este derecho.

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de derecho, a 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 art. 37.7 RGPD dispone que el RT o el ET tiene que publicar los datos de contacto del delegado de protección de datos y los tiene que comunicar a la autoridad de control.

Siguiendo con este mandato, el art. 34.3 LOPDGDD establece que “los responsables y encargados del tratamiento tienen que comunicar en el plazo de diez días a la Agencia Española de Protección de Datos o, si procede, a las autorida-

des autonómicas de protección de datos, las designaciones, los nombramientos y los ceses de los delegados de protección de datos tanto en los supuestos en que estén obligadas a su designación como en el caso en que sea voluntaria".

Para facilitar esta comunicación, las diferentes Autoridades de protección de datos han establecido mecanismos para notificar quién es el DPD.

La AEPD ha habilitado un enlace para hacer esta comunicación (Comunicación del Delegado de Protección de Datos):

https://sedeagpd.gob.es/sede-electronica-web/vistas/formdelegadoprotecciondatos/procedimientodelegadoproteccion.jsf.

El APDCAT también ha establecido un canal para comunicar quién es el DPD (Comunicación designación DPD):

https://apdcat.gencat.cat/ca/seu_electronica/tramits/comunicacio/.

Por otro lado, el art. 34.4 LOPDGDD dispone que "La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos".

Enlace de interés

El APDCAT ha habilitado un medio para consultar quién es el DPD de una determinada empresa o institución: https://apdcat.gencat.cat/ca/drets _i_obligacions/responsables/obligacions /delegat-proteccio-dades/consulta-dpd/.

El art. 38 RGPD regula la posición del delegado de protección de datos dentro de la administración, empresa u organización. En cualquier caso, deberá garantizarse que participe en tiempo oportuno y de forma adecuada en todas las cuestiones relativas a la protección de datos personales.

Asimismo el RT y el ET respaldarán al delegado de protección de datos en el desempeño de las funciones y le facilitarán los recursos necesarios para llevar a cabo sus funciones y acceder a los datos personales y a las operaciones de tratamiento. Tanto responsable como encargado garantizarán que el delegado no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones. Además, rendirá cuentas al más alto nivel jerárquico y estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.

El delegado de protección de datos tiene unas funciones mínimas, recogidas en el art. 39.1 RGPD y que consisten en:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados de las obligaciones que les incumben (art. 39.1.a).

- Supervisar el cumplimiento de lo dispuesto en el RGPD y otras disposiciones de protección de datos, así como de las políticas del RT o ET en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes (art. 39.1.b).

- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación (art. 39.1.c).

- Cooperar con la autoridad de control (art. 39.1.d).

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto (art. 39.1.e).

En el desempeño de sus funciones, el delegado deberá hacerlo prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento (art. 39.2).

El art. 34 LOPDGDD, en relación con el art. 37 RGPD, detalla supuestos concretos en los que hay que designar un DPD. Así mismo la norma estatal también hace una referencia expresa a la calificación del DPD, de forma que según establece el art. 35 LOPDGDD: "El cumplimiento de los requisitos que establece el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, ya sea una persona física o jurídica, se puede demostrar, entre otros medios, a través de mecanismos voluntarios de certificación que tienen que tener particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos".

Por otro lado, el art. 36 LOPDGDD concreta determinados aspectos relativos a la posición del DPD en la empresa, organización o administración y el art. 37 se dedica a la intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

3.8. 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, Autoridades de protección de datos 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.

3.8.1. Los códigos de conducta

Durante el proceso de adopción del RGPD, se puso de relieve el hecho de que la aplicación del mismo podía suponer un coste elevado para las PYMES. Una de las medidas para tratar de responder a esta crítica fue la introducción de códigos de conducta, que ya habían sido recogidos en el art. 27 DPD, si bien habían pasado un tanto desapercibidos y no habían tenido demasiado juego en el marco de la directiva.

Ved también

Los códigos de conducta ya se mencionaban en la DPD, si bien no se les proporcionó demasiada atención.

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.

Actualmente, con la excepción de algunos sectores específicos, existen pocos códigos de conducta aprobados.

Sin embargo, cada vez se pone más de relieve su potencial para regular el tratamiento de información personal y cada vez se les presta mayor atención.

En esencia, el seguimiento del cumplimiento de un código de conducta puede ser llevado a cabo por una organización que tiene un nivel apropiado de experiencia en el sector concreto del que se trata y resulta acreditada para ello (para desempeñar dicha función) por la autoridad competente. Se considera que es una medida adecuada hacia la autorregulación.

Según dispone el art. 40.1 RGPD,

> "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 RGPD. A estos efectos deben tenerse en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas".

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, como en lo que respecta a:

El tratamiento leal y transparente; los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos; la recogida de datos personales; la seudonimización de datos personales; la información proporcionada al público y a los interesados; el ejercicio de los derechos de los interesados; la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño; las medidas y procedimientos técnicos adecuados, así como las medidas para garantizar la seguridad del tratamiento (art. 40.2 RGPD).

Asimismo, los responsables o encargados a los que no se aplica el reglamento podrán también adherirse a códigos de conducta que tengan validez general (art. 40.3 RGPD).

Los códigos de conducta promovidos por las asociaciones y otros organismos representativos contendrá mecanismos que permitan al organismo supervisor previsto en el art. 41 RGPD 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 (art. 40.4 RGPD).

Las asociaciones y otros organismos que proyecten elaborar un código de conducta o modificar o ampliar un código 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).

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 art. 40.9 RGPD (art. 40.10 RGPD).

El Comité 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).

Un elemento clave, respecto a la adopción e implementación de los códigos de conducta es su supervisión. Esta supervisión debe efectuarse por un organismo externo respecto al que trata los datos personales y debe cumplir con una serie de requisitos.

Sin perjuicio de las funciones y los poderes de la autoridad de control competente, 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 (art. 41.1 RGPD).

A fin de que un organismo pueda ser acreditado para supervisar el cumplimiento de un código de conducta, deben cumplirse una serie de requisitos contemplados en el art. 41.2 RGPD. Concretamente, 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 como 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.

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).

Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo 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 estas a la autoridad de control competente (art. 41.4 RGPD).

Nota

El capítulo VIII del RGPD lleva por rúbrica: "Recursos, responsabilidad y sanciones".

La autoridad de control competente revocará la acreditación de un organismo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el reglamento (art. 41.5 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).

3.8.2. La certificación

La idea de la certificación tiene sus orígenes en Estados Unidos, donde ya se implementaron desde 1990. En la UE han empezado a adoptarse si bien no tienen una firme base ni teórica ni legal. La filosofía a que responden a cada lado del Atlántico es distinta.

Concretamente, el modelo de Estados Unidos es de una autorregulación total, mientras que, 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 proporcionaba mucha más iniciativa a esta, sobre la base del mecanismo de dictar actos delegados. El texto final optó por un modelo más concreto. De modo que 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.

A estos efectos, se 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" (art. 42.1 RGPD).

"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" (art. 42.2 RGPD).

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 en virtud del presente artículo 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, que tengan un nivel adecuado de pericia y que expedirán y renovarán las certificaciones una vez informada la autoridad de control. En cualquier caso, debe garantizarse que dichos organismos de certificación sean 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).

Los códigos de conducta se encuentran regulados en el art. 38 de la LOPDGDD. Se establece que los mencionados códigos serán aprobados por la Agencia Española de Protección de Datos o, si procede, por la Autoridad autonómica de protección de datos competente (art. 38.3).

Así mismo, las Autoridades de protección de datos tendrán que someter los proyectos de código al mecanismo de coherencia *ex* art. 63 RGDP, cuando corresponda por el art. 40.7 del RGPD. El procedimiento queda suspenso mientras el Comité Europeo de Protección de Datos no emita el dictamen preceptivo (art. 38.4).

Las Autoridades de protección de datos tienen que mantener registros de los códigos de conducta que aprueben, que tienen que estar interconectados entre sí y coordinados con el registro que gestiona el Comité Europeo de Protección de Datos. El registro tiene que ser accesible a través de medios electrónicos (art. 38.5).

Por otro lado, el art. 39 LOPDGDD hace referencia a la acreditación de instituciones de certificación.

3.9. Derechos del afectado/interesado

El capítulo III del RGPD se dedica a los Derechos del interesado. Dicho capítulo se divide en 5 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 de entrada que se recogen nuevos derechos: el derecho a la limitación del tratamiento y el derecho a la portabilidad. Así mismo, el derecho de cancelación pasa a denominarse como derecho de supresión. Por otro lado, el denominado derecho al olvido se menciona en el art. 17 RGPD como un equivalente a derecho de supresión y realmente queda muy desnaturalizado.

En cuanto a la LOPDGDD, el Título III regula los Derechos de las personas. El Capítulo I hace referencia a la transparencia e información. El Capítulo II, al ejercicio de los Derechos. En este Capítulo hay un precepto dedicado a las disposiciones generales (art. 12) y otros artículos que regulan de forma más o menos detallada el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos y oposición (arts. 13 a 18 LOPDGDD).

3.9.1. Transparencia y modalidades

La sección 1 del Capítulo III lleva por rúbrica "transparencia y modalidades".

De entrada debe subrayarse que el RGPD configura la transparencia a la vez como:

- Un Principio de protección de datos [art. 5.1.a) RGPD], recuérdese que este precepto dispone que: 1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia")].

- Como un derecho de las personas a recibir determinada información.

Así mismo la transparencia estaría vinculada al ejercicio de otros derechos. Esto es 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[48].

[(48)]Respecto a la transparencia e información, conviene consultar los Documentos del Grupo del art. 29, WP 187 y WP 260, que analizan con detalle este derecho/obligación.

Por lo tanto, al hablar de transparencia se hace referencia a que el tratamiento sea lícito y leal.

Artículo 12: Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.

El artículo 12 hace referencia a tres aspectos:

1) Referencia general a la transparencia. La referencia a la transparencia, además de relacionarla con el art 5.1.a) RGPD debe ponerse en relación con el Principio de responsabilidad proactiva (art. 5.2 RGPD), de forma que el RT debe actuar de forma diligente y proporcionar todos los mecanismos (entre ellos proporcionar la información precisa), para hacer efectivos los derechos del afectado.

2) Forma de comunicación. La comunicación al interesado debe hacerse de forma "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). La información será facilitada por escrito o por otros medios, inclusive por medios electrónicos. Si lo solicita el interesado también podrá facilitarse verbalmente, si se demuestra la identidad del interesado (art. 12.1 RGPD).

El RT facilitará al interesado la información relativa a sus actuaciones en base a 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, hay que informar al interesado de dichas prórrogas (art. 12.3 RGPD).

La información facilitada será gratuitas. Sin embargo, si las peticiones son manifiestamente infundadas o excesivas (por su carácter repetitivo), el RT podrá cobrar un canon razonable o bien negarse a actuar respecto de la solicitud (art. 12.5 RGPD).

Un aspecto importante es la previsión de la posibilidad de que la información que deba facilitarse a los interesados se haga en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto (art. 12.7 RGPD). Esta iniciativa ya se propuso en ocasiones anteriores, y en todo caso su implementación se deja a la Comisión (art. 12.8 RGPD). De alguna forma se pretende incorporar las imágenes visuales de los *creative commons*, de forma que sea claramente identificable para los afectados.

3) Modalidades de ejercicio de los derechos por parte del interesado.

3.9.2. Información y acceso a los datos personales

La sección 2 del Capítulo III se dedica a la Información y acceso a los datos personales.

En cuanto al contenido concreto de la información que debe proporcionarse al interesado/afectado, el RGPD, igual que hacía la DPD, 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:

- el ámbito subjetivo: quién es el responsable del tratamiento y el delegado de protección de datos. Así como los destinatarios o categorías de destinatarios de los datos y la intención de transferir los datos a un tercer país u organización internacional.

- En cuanto al contenido concreto, un aspecto relevante es proporcionar información de los fines del tratamiento y la base jurídica del mismo. Una novedad es que en aquellos casos en que la base jurídica sea el interés legítimo [(art. 6.1.f)], deberá especificarse cuál es este (art. 13.1.d. RGPD).

Así mismo, según dispone el art. 13.2, deberá proporcionarse información relativa a:

- El plazo durante el cual se conservarán los datos personales, y si ello no es posible, los criterios utilizados para determinar este plazo.

- La existencia de los derechos que tiene el afectado (acceso, rectificación, supresión, limitación, oposición y portabilidad).

- La existencia del derecho a revocar el consentimiento (el texto del RGPD hace referencia a "retirar", el consentimiento si bien el término más apropiado es el de revocarlo).

- El derecho a presentar una reclamación ante la autoridad competente.

- El carácter obligatorio o no de facilitar los datos.

- Un aspecto de gran trascendencia es la necesidad de comunicar la existencia de decisiones automatizadas, incluida la elaboración de perfiles (art. 22 RGPD), así como información significativa sobre la lógica aplicada, así como las consecuencias previstas de dicho tratamiento para el interesado. Esto es debe proporcionarse Información específica relativa a las decisiones automatizadas [véase art. 13.1. (f)].

Según establece el art. 13.3, en aquellos supuestos en que el RT proyecte el tratamiento ulterior de datos para un fin que no sea aquel para el que se recogieron los datos, deberá proporcionar al interesado, con anterioridad a dicho tratamiento ulterior, información sobre este otro fin (vid también art. 6.4 RGPD).

Esta información deberá facilitarse al interesado en el momento en que se obtengan los datos (art. 13.1).

En aquellos supuestos en que el interesado ya disponga de la información contemplada, no será preciso proporcionársela (art. 13.4 RGPD).

Supuestos en que los datos no se obtienen directamente del afectado. Junto a algunos aspectos que son similares a los del punto anterior, en este caso hay aspectos nuevos (véased art. 13 RGPD).

Este es el caso del art. 14.2.f), que dispone 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;

En cambio, *no* es preciso proporcionar información sobre:

Lo que dispone el art. 13.2.e) RGPD si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos; ello es obvio, porque en este caso los datos no los proporciona el afectado (no se solicitan de él), sino que se obtienen de otra fuente o de un tercero.

Por otro lado, en la medida que los datos no se obtienen del afectado, es importante determinar en qué momento se le proporcionará la información. El art. 14.3 establece distintos supuestos:

La regla general es la de un plazo razonable, una vez obtenidos los datos, y como máximo dentro de un mes en base de las circunstancias en las que se traten los datos.

En los casos en que los datos se utilicen para comunicarse con el interesado, como máximo en el momento de la primera comunicación a dicho interesado. Si se comunican a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

También prevé la norma supuestos en que no es preciso proporcionar la información al afectado:

- Si el interesado ya dispone de la información.

- Cuando la comunicación resulte imposible o implique un esfuerzo. desproporcionado, especialmente con fines de archivo en interés público, fines de investigación científica, histórica o con fines estadísticos. En este caso, sin embargo deberán cumplirse con las garantías del art. 89 RGPD. En tales casos el RT adoptará las medidas adecuadas para proteger los de-

rechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información (art. 14.5.b) RGPD).

- La obtención o comunicación está expresamente establecida por la legislación.

- Cuando los datos personales deban seguir teniendo carácter confidencial, sobre la base de una obligación de secreto profesional, regulada en el Derecho de la unión o de los EM, incluida una obligación de secreto de naturaleza estatutaria.

La LOPDGDD regula el derecho a la transparencia e información al afectado en el art. 11, en el Título III (Derechos de las personas), Capítulo I (transparencia e información).

El art. 11, siguiendo el RGPD, distingue también los supuestos en los que los datos se obtienen directamente del afectado y los casos en los que no es así.

1) Supuestos en los que los datos han sido obtenidos del afectado (art. 11.1 y 2 LOPDGDD)

Artículo 11. Transparencia e información al afectado.

> **1.** Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
>
> **2.** La información básica a la que se refiere el apartado anterior deberá contener, al menos:
>
> **a)** La identidad del responsable del tratamiento y de su representante, en su caso.
>
> **b)** La finalidad del tratamiento.
>
> **c)** La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
>
> Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

El GT29 hace referencia a la posibilidad de proporcionar la información al afectado por niveles (WP 260, § 35). Esta posibilidad también ha sido recomendada por las autoridades de protección de datos españoles en la *Guía para el cumplimiento del deber de informar*, elaborada por las autoridades de protección de datos españolas.

Enlace de interés

Puede consultarse esta Guía en: https://www.aepd.es/media /guias/guia-modelo-clausula- informativa.pdf. En concreto vid § 5 Información por capas; § 6 Información básica (primera capa); § 7 Información adicional (segunda capa), de esta Guía.

De alguna manera esta posibilidad viene recogida en el art. 11 LOPDGDD. Este precepto prevé la posibilidad que el responsable del tratamiento dé cumplimiento al deber de información proporcionando determinada información

que califica como básica y que se facilite una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información. Por lo tanto, se establecerían dos categorías de información la "básica" y el "resto". En cuanto a la información básica, se trata, *ex* art. 11.2 LOPDGDD, de la relativa a: (a) La identidad del responsable del tratamiento y de su representante, si procede; (b) La finalidad del tratamiento y (c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado tuvieran que tratarse para la elaboración de perfiles, la información básica comprenderá así mismo esta circunstancia (art. 11.2.ii LOPDGDD).

El art. 11.3 LOPDGDD, al hacer referencia a la información que hay que proporcionar en el caso de datos no recogidos del afectado también establece estos dos niveles de información.

En definitiva, el art. 11 LOPDGDD de alguna manera establece dos categorías de información, al distinguir entre información básica y el resto de la información. Es cuestionable que este art. 11 haya recogido correctamente las exigencias de proporcionar información *ex* art. 13 y 14 RGPD en la medida que el art. 11 no recoge todos los ítems que se enumeran en los arts. 13 y 14 RGPD.

Por ejemplo, entre otros, falta la referencia a los datos de contacto del delegado de protección de datos (art. 13.1.bi c RGPD), la base jurídica del tratamiento (art. 13.1. b y c. RGPD) o bien los destinatarios o categorías de destinatarios (art. 13.1.e. RGPD). Se trataría en todo caso del "resto de la información" a la que alude el art. 11 LOPDGDD.

Sin duda el art. 11 LOPDGDD ha intentado primar la accesibilidad de la información, que esta sea leída y que el afectado no se pierda en una lista a la que difícilmente prestará atención. Por eso ha optado por proporcionar la información por niveles.

A pesar de recurrir a esta solución (que me parece realista y potenciadora de un mínimo interés para el afectado), es fundamental que toda la información *ex* art. 13 y 14 (según proceda) se proporcione, se encuentre en la página web o espacio donde se facilite la información al interesado. El GT29, al hacer referencia a la posibilidad de proporcionar la información por niveles, recuerda que en todo caso la información también tiene que estar disponible en un solo lugar o en un documento completo único (WP 260, § 17).

Por lo tanto, para cumplir debidamente con el RGPD de alguna manera se tendría que asegurar que todos los ítems respecto de los que se tiene que informar se proporcionen en el mismo momento.

2) Supuestos en los que los datos no han sido obtenidos del afectado (art. 14 RGPD y art. 11.3 LOPDGDD)

El art. 11.3 LOPDGDD dispone lo siguiente:

> **3.** Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.
>
> En estos supuestos, la información básica incluirá también:
>
> **a)** Las categorías de datos objeto de tratamiento.
>
> **b)** Las fuentes de las que procedieran los datos.

En cuanto a la LOPDGDD, la información básica que se tiene que proporcionar para cumplir el deber de información *ex* art. 14 RGPD, además de la prevista en el art. 11.1 LOPDGDD, incluiría también (a) las categorías de datos objeto de tratamiento y (b) las fuentes de las que procedieran los datos. También se indicará una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata al resto de la información.

En cuanto al contenido concreto de la información que hay que proporcionar *ex* art. 11.3 LOPDGDD y si esto satisface plenamente las exigencias del art. 14 RGPD, me remito a las consideraciones ya expuestas.

Información que hay que proporcionar en los casos de elaboración de perfiles: Como ya se ha indicado, la LOPDGDD también hace referencia al deber de informar en estos casos (art. 11.2 *infine*).

Estrechamente ligado a la información es el aspecto del acceso a la misma, regulado en el art. 15 RGPD (**Derecho de acceso del interesado**):

En base al derecho de acceso el interesado tendrá derecho a obtener del responsable del tratamiento 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 art. 15.1 RGPD. (Art. 15.1 RGPD).

La información a la que se tiene acceso es la relativa a:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;
- los destinatarios o las categorías de destinatarios de los datos; plazo previsto de conservación de
- los datos personales o los criterios utilizados para determinar este plazo;

- La existencia de los derechos que corresponden al afectado; el derecho a presentar una reclamación ante una autoridad de control; cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles y en tales casos, información significativa sobre la lógica aplicada, así como las consecuencias previstas de dicho tratamiento para el interesado.

En los casos en que se transfieran datos a un tercer país o una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas

Un aspecto novedoso del RGPD es que se determina que el RT facilitará una copia de los datos personales. Hasta el momento, la práctica del derecho de acceso no se ejercía proporcionando acceso directo a los datos, por lo que ello exigirá un cambio en la modalidad del ejercicio de este derecho (art. 15.3 RGPD). En los casos en que se soliciten ulteriores copias se podrá percibir un canon razonable por ello. Si la solicitud se presenta por medios electrónicos, y a menos que el interesado solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. (art. 15.3 RGPD).

En cualquier caso, el derecho a obtener copia no afectará negativamente a los derechos y libertades de otros sujetos (art. 15.4 RGPD).

3.9.3. Rectificación y supresión

La sección 3 del Capítulo III lleva por rúbrica "rectificación y supresión".

Como ya se ha indicado, en la nueva regulación la referencia al derecho de cancelación ha sido sustituida por la de supresión.

Artículo 16: Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional[49].

(49)Téngase también en cuenta el art. 86 LOPDGDD.

El objetivo de este derecho es pues que se actualicen los datos o que se completen[50].

(50)Véase art. 14 LOPDGDD

La referencia a "sin dilación indebida" no parece que deba entenderse que el plazo es distinto de aquel previsto de forma general para el ejercicio de los demás derechos, esto es, de 1 mes.

Así mismo, en aquellos supuestos en que se proceda a la rectificación, deberá comunicarse a los destinatarios que dicha rectificación ha tenido lugar, salvo que ello sea imposible o implique un esfuerzo desproporcionado. Así mismo el afectado también tendrá derecho a saber quién ha sido el destinatario de los datos.

Artículo 17: Derecho de supresión ("el derecho al olvido")

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 en relación con los fines para los que fueron recogidos o tratados.

b) El interesado retire el consentimiento en que se basa el tratamiento (se trata del supuesto de la revocación del consentimiento).

c) El interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el mismo.

d) Los datos personales hayan sido tratados ilícitamente.

e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros.

f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1. (Se trata de la oferta realizada a niños, entendidos estos como menores de 18 años).

El art. 17.2 dispone que en los casos en que el RT haya hecho públicos los datos personales y esté obligado, en virtud del art. 17.1 RGPD a suprimir dichos datos, el RT, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Por lo tanto, el RT inicial, deberá adoptar medidas razonables para comunicar a ulteriores RT la solicitud del afectado de querer suprimir cualquier enlace a los datos personales. Se trata de una obligación de medios, de forma que el RT inicial no tiene que asegurar en todo caso que los destinatarios de los datos (los otros RT) los dejan de tratar, sino que pone los medios de los que disponga para llevar a cabo esta comunicación.

Sin embargo el propio art. 17.3 establece supuestos en que el derecho a eliminar datos y enlaces no resultará aplicable. Concretamente en aquellos casos en que la permanencia de estos es necesario:

1) para ejercer el derecho a la libertad de expresión e información;

2) para el cumplimiento de una obligación legal que requiera el tratamiento de datos o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

3) por razones de interés público en el ámbito de la salud pública

4) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1,

5) para la formulación, el ejercicio o la defensa de reclamaciones.

¿Qué ha quedado del denominado derecho al olvido?

La medida que recoge el art. 17.2 RGPD trata de evitar multiplicar los efectos de réplica de los enlaces sucesivos de la información.

A pesar de que la rúbrica del art. 17 hace referencia entre paréntesis al derecho al olvido, se hace una referencia confusa al mismo. De hecho la utilización de esta terminología no es más que una consecuencia de arrastrar textos anteriores a la aprobación del RGPD. El denominado derecho al olvido, tal y como se halla regulado en el RGPD, no es tal, sino que es una manifestación de los derechos de oposición y cancelación. Las características y requisitos del derecho al olvido se hallan en la STJUE, en el caso Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González (C 131/12), de 13 de mayo de 2014.

> En lugar de hacer referencia al derecho al olvido parece más correcto hablar del derecho a ser eliminado de la lista de resultados de los motores de búsqueda (*right to be delisted*). En rigor, lo que el afectado puede solicitar es que al llevarse a cabo búsquedas en internet en base a su nombre, deje de aparecer en los resultados que ofrece el motor de búsqueda. Esta petición tiene posibilidades de prosperar si la información es irrelevante y obsoleta. El motor de búsqueda (no el editor de la información) lleva a cabo una ponderación de los derechos implicados (el del afectado vs el derecho del público a obtener información). En todo caso el interesado siempre podrá acudir a la APD y a la autoridad judicial. Sin embargo, en caso de prosperar la petición de ser eliminado de la lista de resultados, la información permanece en su fuente original (la hemeroteca de un periódico o un boletín oficial).

Según dispone el art. 17.2 RGPD, cuando el RT haga públicos los datos y tenga la obligación de suprimirlos, dicho RT tiene la obligación de informar al tercer responsable de la solicitud del interesado de supresión de cualquier enlace a los datos.

Se trata de una obligación de informar a los terceros, en función de los medios de que disponga el RT (de la tecnología y de los costes) y es una obligación de medios (no de resultado).

Derecho al olvido

En la ponderación que hay que llevar a cabo para determinar si procede o no el derecho a ser desindexado, hay cuestiones que todavía quedan abiertas, que son objeto de análisis bien por las autoridades de protección de datos, bien por los tribunales.

Entre estas cuestiones se puede destacar: el alcance del ámbito territorial del bloqueo; si el buscador puede comunicar a la fuente original de información el hecho que ha procedido a eliminar el enlace; quién puede ejercer el derecho al olvido; cuándo tiene que prevalecer el interés público de la información; el uso de robots que no permitan hacer búsquedas; la integridad de la hemeroteca digital o bien la responsabilidad de las plataformas.

Lecturas recomendadas

Respecto a estas cuestiones podéis consultar:

STS 15 octubre 2015 (ECLI: SE:TS:2015:4132) y la STC 58/2018, de 4 de junio de 2018, (BOE n.º 164, de 7 de julio de 2018).

Respecto a la doctrina, véase:

PEGUERA, M (2016): The Shaky Ground of the Right tono Be Delisted, Vanderbilt Journal of Entertainment & Technology Law Quiere 18(3) p. 507-561 (2016).

En cuanto a la legislación española, la LO 3/2018 dedica dos artículos al derecho al olvido.

Por un lado, el art. 93 LOPDGDD recoge la jurisprudencia del TJUE en el caso de Google Spain y lleva por título "Derecho al olvido en búsquedas de Internet". Este precepto hace referencia al derecho a pedir la desindexación de aquellos resultados que se obtengan después de hacer una búsqueda efectuada a partir del nombre, si los enlaces publicados contienen información que sea inadecuada, inexacta, no pertinente, no actualizada o excesiva, o bien haya resultado como tal por el transcurso del tiempo.

En cualquier caso, hay que tener en cuenta el tiempo transcurrido y la naturaleza y el interés público de la información.

Por otro lado, el derecho a la desindexación subsiste, aunque sea lícita la conservación de la información publicada en el sitio web al que se dirija el enlace y este no proceda a borrarla de forma previa o simultánea.

Por el otro, el art. 94 hace referencia al derecho al olvido en servicios de redes sociales y servicios equivalentes.

"**Artículo 94.** Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes 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 a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 18: Derecho a la limitación del tratamiento

1) Como se ha indicado, se trata de un nuevo derecho en virtud del cual el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumplan determinadas condiciones:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2) Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3) Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Se trata de un nuevo derecho de consecuencias importantes. 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. También si se ejercita el derecho de oposición ex art 21.1 por parte del interesado, mientras se verifica su procedencia.

Se produce una inversión de la carga de la prueba de modo que cuando el RT alegue un interés (publico, o legítimo) deberá demostrarlo. Otro supuesto es aquél que responde a la voluntad del afectado, por ejemplo, para que el interesado pueda obtener determinadas pruebas.

¿Cuáles son las consecuencias de la limitación del tratamiento? Ex art. 18.2 RGPD, las consecuencias son que el tratamiento se limita a la conservación de los datos, salvo que se den distintos supuestos. El art. 19 también dispone la necesidad de comunicarlo a los destinatarios de la comunicación.

Se refuerza este derecho de forma que antes de levantar la limitación, el RT debe informar al afectado. No puede levantarse la limitación sin que el afectado lo sepa (art. 18.3 RGPDPD). También debe proporcionarse información sobre los destinatarios de la información (art. 19.3 RGPDPD).

Para hacer efectivos los derechos de rectificación, supresión y limitación del tratamiento, se habilitan una serie de medidas especialmente cuando los datos se hayan transmitido a terceros. Según dispone el art. 19 RGPD, el RT comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.

Así mismo el RT informará al interesado acerca de dichos destinatarios, si este así lo solicita.

El art. 16 LOPDGDD hace referencia al derecho a la limitación del tratamiento. Aparte de remitirse al art. 18 RGPD, el art. 16 establece que el hecho de que el tratamiento de los datos personales esté limitado tiene que constar claramente en los sistemas de información del responsable (art. 16.2).

Artículo 20: el derecho a la portabilidad de los datos

Otra medida relevante es el derecho a la portabilidad de los datos recogida en el 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 las había facilitado[51], cuando:

(51)El art. 17 LOPDGDD hace referencia al derecho a la portabilidad de los datos y simplemente establece que el ejercicio de este derecho se ejercerá de acuerdo con el art. 20 RGPD.

a) el tratamiento esté basado en el consentimiento o en un contrato y

b) el tratamiento se efectúe por medios automatizados.

2) Al ejercer su derecho a la portabilidad de los datos (ex. art. 20.1), el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3) El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

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/afectado.

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.

Hay que pensar no solo en los datos facilitados por el propio afectado, sino aquellos que se obtienen de forma indirecta. Sin embargo, aquellos tratamientos adicionales que pueda hacer el RT no serán objeto de portabilidad.

Otro aspecto importante es el derecho a transmitir los datos a otro RT sin que ello lo impida el RT inicial. Se trata pues de un derecho muy adecuado a la prestación de servicios en internet, especialmente en el caso de las redes sociales.

Lógicamente es impensable que cada interesado tenga capacidad y la tecnología suficiente para poder guardar y migrar los datos. En consecuencia, la efectividad del derecho quedaría menoscabada. Por ello es una medida muy positiva que se establezca que los datos pueden transmitirse a otro RT.

Para que se pueda aplicar este derecho es preciso que la base del tratamiento sea una muy concreta.

En cuanto a la modalidad de ejercicio de este derecho ya se ha indicado que es posible la transmisión a un 3º de los datos, de modo que se estimula el desarrollo de sistemas interoperables en la prestación del servicio.

Lógicamente también existen limitaciones a este derecho, cuando existe una base jurídica distinta que habilita al RT a seguir conservando los datos o bien cuando el fundamento de la conservación se basa en una obligación legal.

3.9.4. Derecho de oposición y decisiones individuales automatizadas

La sección 4 del Capítulo III lleva por rúbrica "Derecho de oposición y decisiones individuales automatizadas".

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

El art. 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 en base a los arts. 6.1.e) o f) RGPD. El art. 6.1.e) es aquél en que 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. El art. 6.1.f) habilita el tratamiento cuando es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento.

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 o bien para la formulación, el ejercicio o la defensa de reclamaciones.

La AEPD admite un concepto amplio y flexible de la exigencia de motivación.

Art. 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 en la medida en que esté relacionada con la citada mercadotecnia. En este caso los datos personales dejarán de ser tratados para dichos fines (art. 21.3). Se trata de un supuesto de *opt-out* inmotivado, el afectado puede oponerse en cualquier momento.

Como máximo en la primera comunicación que se realice con el interesado, deberá informarse al mismo del derecho de oposición ex art. 21.1 y 21.2 (art. 21.4 RGPD).

En cuanto al tratamiento de datos personales con fines de investigación científica o histórica o fines estadísticos (ex art. 89. 1 RGPD), el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público (art. 21.6 RGPD).

Junto con esta regla general contenida en el art. 21 RGPD, existe legislación específica en que cabe la posibilidad de ejercer el derecho de oposición. Por ejemplo, en la legislación sobre telecomunicaciones o bien en el marco de la LSSI. Por ejemplo, el derecho a no recibir llamadas telefónicas que no son automáticas.

En otros casos, más que el ejercicio del derecho de oposición lo que se producirá será una revocación del consentimiento otorgado (art. 7.3 RGPD). Ello podrá darse en aquellos supuestos en que el fundamento legal del tratamiento es el consentimiento del afectado[52] [art. 6.1.a) o bien art. 9.2.a) RGPD].

[52]El art. 18 LOPDGDD hace referencia al derecho de oposición y a los derechos relacionados con las decisiones individuales automatizadas pero simplemente se remite a los arts. 21 y 22 RGPD.

El art. 22 RGPDPD hace referencia a las decisiones individuales automatizadas así como la elaboración de perfiles

De entrada es preciso tener en cuenta el art. 4.4 RGPD que proporciona una definición de qué se considera “elaboración de perfiles”. Se entiende como tal

> "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. En base a este tipo de decisiones, una persona puede ver como se le deniega un crédito o se rechaza la solicitud presentada para un puesto de trabajo sin que exista aparentemente un motivo para ello. Así mismo los tratamientos masivos pueden comportar la inferencia de conclusiones erróneas y ocasionar efectos discriminatorios.

En la medida 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. 22.3 RGPD), de modo que la previsión general no será aplicable si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión vid art. 22.3 RGPD).

Así mismo, como regla general, las decisiones automatizadas no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, esto es, los denominados datos sensibles, véase art. 22.4 RGPD).

En cuanto a la valoración general del precepto, debe recordarse que no se trata solo de derechos, sino también de garantías para poder predicar la existencia de un tratamiento leal y transparente y que se cumplen los principios básicos del RGPD. En definitiva, se trata de corregir elementos que pueden generar inexactitudes y reducir los riesgos de error.

3.9.5. Limitaciones

La sección 5 del Capítulo III lleva por rúbrica "Limitaciones".

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

El art. 23.1 RGPD establece que:

> "El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar: (entre otros), a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, e) otros objetivos importantes de interés público; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas; h) una función de supervisión, inspección o reglamentación; i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles.
>
> Sin embargo, las medidas legislativas adoptadas deberán especificar, entre otros extremos (art. 23.2.c), las garantías para evitar accesos o transferencias ilícitos o abusivos; f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento; g) los riesgos para los derechos y libertades de los interesados, y h) el derecho de los interesados a ser informados sobre la limitación."

En la enumeración de las limitaciones, la mayor parte son las tradicionales, si bien se incluyen algunas nuevas como las relativas a motivos económicos financieros, sanidad pública, protección independencia judicial.

Se exigen garantías complementarias en relación con la finalidad, las categorías de datos. Así mismo en este supuesto las medidas de seguridad tienen un papel muy relevante. Y todos estos aspectos se tienen en cuenta en base a los riesgos que pueden amenazar los datos de los afectados.

3.10. Transferencias internacionales de datos

El Capítulo V RGPD se dedica a las transferencias internacionales de datos y lleva por rúbrica: "Transferencias de datos personales a terceros países u organizaciones internacionales".

La LOPDGDD también hace algunas referencias a las transferencias internacionales en el Título VI, arts. 40 a 43.

Se considera que hay una transferencia de datos cuando se transmiten datos por parte de un RT o ET que está en la UE a un RT u otro sujeto que se halla fuera de la UE. Por lo tanto, las comunicaciones de datos entre sujetos que se hallan en el territorio de la UE no se consideran una transferencia internacional de datos y no existen limitaciones para las mismas. De hecho, uno de los objetivos de la D 95/46 era precisamente el de facilitar la circulación de los datos entre los países de la Unión.

Tal y como dispone el art. 44 RGPD, las transferencias internacionales tienen como destinatarios "terceros países o bien organizaciones internacionales".

La regulación que proporciona el RGPD de las transferencias internacionales no plantea novedades sustanciales respecto del régimen contenido en la DPD. La idea que preside el actual régimen legal es que cuando los datos salgan de la UE se siga aplicando el mismo nivel de protección de que gozaban en la UE. Esto es, que cuando los datos se exporten, no disminuyan las garantías de los sujetos interesados. Así se dispone, entre otros, en el art 44 RGPD que dispone:

> "Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

El modelo es pues el de continuidad del nivel de protección. La normativa trata de obtener y perseguir que el nivel de protección garantizado por la normativa europea se mantenga allí donde se hallen los datos.

Las transferencias internacionales de datos se pueden basar en tres posibles fundamentos, de tal forma que las transferencias pueden tener lugar si:

1) Existe una *decisión de adecuación* (art. 45 RGPD). Se trataría del nivel básico que trata de asegurar un nivel de protección adecuado respecto de un territorio concreto, mediante la adopción de una declaración de adecuación. Cuando existe tal decisión ello significa que se ha producido el análisis conforme al cual el destino de los datos (territorio, país), ofrece un nivel de protección adecuado al que se establece en UE.

2) En defecto de decisión de adecuación, solo podrán transmitirse datos personales a un tercer país u organización internacional *si se ofrecen garantías adecuadas* y a condición que los interesados cuenten con derechos exigibles y acciones legales efectivas (art. 46 RGPD).

3) En aquellos casos en que no exista un nivel de protección adecuado, ni tampoco se hayan podido otorgar garantías suficientes, *se entra dentro de los supuestos de excepciones*. Se podrán transferir los datos si concurren una serie de excepciones y ello obedece a un interés de mayor valor, de mejor calidad.

Por lo tanto, en primer lugar se busca la adecuación del nivel de protección de un país o territorio a las exigencias de protección que plantea la UE. En defecto de esta declaración de adecuación, se busca la adopción de garantías suficientes que en este caso se otorgan respecto de un ámbito concreto o bien de una organización. En defecto de dicho otorgamiento entran en juego las excepciones que permiten las transferencias internacionales de datos.

3.10.1. Principales novedades del régimen de transferencia de datos

El objetivo de la Comisión y de los colegisladores, al regular las transferencias de datos era el de introducir mayor flexibilidad en dicho régimen, que se criticaba por ser excesivamente burocratizado. Así mismo se cuestionaba también el modelo existente de adecuación, en la medida que existían pocas declaraciones y las existentes eran muy heterogéneas.

Por otro lado debe tenerse en cuenta que las transferencias internacionales no son la excepción, sino que se han convertido en la regla general. En cuanto a las principales novedades cabe destacar:

1) Referencia a que el exportador puede ser tanto el RT como el ET. En algunos países ya se podía manejar este concepto, por ejemplo en el marco de la LOPD de 1999. En cambio en otros países solo podían adoptar la decisión de enviar datos fuera de la UE los RT. Así mismo, las garantías pueden proporcionarlas tanto el RT como el ET.

2) Las transferencias pueden hacer referencia tanto a un país como a una Organización internacional. La DPD solo hacía referencia a países o territorio, no OI. En la práctica las transferencias a estas OI son frecuentes. Estas pueden ser intergubernamentales o bien privadas.

3) Por primera vez se da cabida a las normas corporativas vinculantes (conocidas también por sus siglas en inglés: BCR, Binding Corporate rules). Se trata de una construcción desarrollada por la práctica y por el Grupo del art. 29, que había fijado un conjunto de requisitos para su implementación, pero no habían recibido apoyo legal. El RGPD las recoge y las regula detalladamente.

3.10.2. Transferencias basadas en una decisión de adecuación

Según se dispone en el art. 45.1 RGPD

> "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica".

La decisión la adopta la Comisión, mediante un procedimiento normativo propio y en dicho proceso son consultadas las APD a través del órgano que las agrupa y que constituye el Comité europeo de protección de datos.

Según dispone el art. 45.2 RGPD, al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

- El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales y la legislación pertinente.

- La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país.

- Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate.

La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado. Un aspecto importante es que se establecerán mecanismos de revisión periódica, al menos cada cuatro años, que tengan en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional, para decidir si se mantiene o no la decisión de adecuación (art. 45.3. RGPD).

En consecuencia, en los casos en que se muestre que el lugar de destino de los datos no garantiza un nivel de protección adecuado, la Comisión derogará, modificará o suspenderá sin efecto retroactivo, la decisión de adecuación (Art. 45.5).

La Comisión hará pública la información relativa a los territorios, sectores u organizaciones internacionales que tienen un nivel de protección adecuado y cuales no lo han dejado de tener (art. 45.8 RGPD).

Según dispone el art. 45.9. RGPD, las decisiones de adecuación ya adoptadas seguirán en vigor en tanto que la Comisión no las sustituya, modifique o derogue.

En definitiva, aquello relevante es que la Comisión, una vez efectuada la decisión de adecuación deberá seguir supervisando y monitorizando la situación en los destinos que se declaran como de protección adecuada.

Este seguimiento debe interpretarse a la luz de la STJUE en el caso Schrems en que el TJUE consideró que el concepto de adecuación debe interpretarse como un concepto de protección esencialmente equivalente y que la Comisión debe supervisar diligentemente las condiciones existentes en los países que se declaran adecuados.

Caso Schrems

Se trata de la STJUE de 6 de octubre de 2015, C-362/14, Schrems.

3.10.3. Transferencias basadas en garantías adecuadas

El art. 46.1 determina que

> "A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas."

En cuanto a las garantías adecuadas, debe distinguirse dos supuestos:

1) Garantías adecuadas que no precisan de autorización previa. Se trata de aquellas garantías recogidas en el art. 46.2 RGPD que podrán ser aportadas, *sin que se requiera ninguna autorización expresa de una autoridad de control*, mediante:

a) Instrumentos jurídicamente vinculantes y ejecutables entre autoridades u organismos públicos

b) Normas corporativas vinculantes (BCR) ex art. 47 RGPD, tanto respecto al RT como respecto al ET.

c) Cláusulas contractuales estándar aprobadas por la Comisión

d) Cláusulas contractuales estándar aprobadas por una APD nacional y aceptadas por la Comisión[53].

(53) Al respecto, véase art. 41.1 LOPDGDD.

e) Códigos de conducta y esquemas de certificación, que incluyan compromisos vinculantes y ejecutables por parte del RT o el ET en el tercer país a fin de garantizar suficientemente la tutela de los derechos del interesado.

En los supuestos contemplados en el art. 46.2) RGPD, el hecho que no sea preciso autorización previa comporta que puedan efectuarse transferencias amparándose en cláusulas generales o BCR sin tener que pedir autorización previa en cada caso. Una vez la BCR es aprobada, podrán llevarse a cabo al amparo de la misma transferencias de datos sin tener que pedir cada vez autorización ante transferencias concretas.

Las BCR se regulan detalladamente en el art. 47 RGPD. Según dispone el art. 47.1 RGPD, la autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63[54], siempre que estas:

(54) Véase art. 41.2 LOPDGDD.

- Sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros del grupo empresarial o unión de empresas

- Confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales

- Incluyan los aspectos contemplados en el art. 47.2 RGPD

Entre los aspectos que deben incluir las BCR (recogidos en el art. 47.2 RGPD) destacan:

La estructura y los datos de contacto del grupo empresarial o de la unión de empresas y de cada uno de sus miembros

Transferencias incluidas, interesados afectados y finalidades, las categorías de datos personales, el tipo de tratamientos y sus fines así como los destinatarios de los datos.

Las medidas dirigidas a garantizar la seguridad de los datos

Aplicación de los principios de protección de datos

Los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, así como el Derecho a presentar reclamación ante APD y ante los tribunales

La aceptación por parte del RT o ET que transfieren datos de la responsabilidad por cualquier violación de las BCR por parte de los destinatarios no establecidos en la UE

Los mecanismos internos de supervisión y de cooperación con la autoridad de control

Los procedimientos de reclamación

En definitiva, el contenido de las BCR es parecido a un código de conducta o política de privacidad, de hecho su contenido comprende prácticamente todo el programa de privacidad y protección de datos de una corporación.

El procedimiento de adopción de las BCR se halla en las normas del RGPD dedicadas a los mecanismos de consistencia. El órgano competente del establecimiento principal de la corporación en la EU deberá dirigirse a autoridad principal (competente) y negociar con la misma el contenido de BCR. Al emitir una autorización, la autoridad principal deberá someterla a opinión del Comité europeo protección datos, que no será directamente vinculante.

Otro instrumento para ofrecer garantías suficientes es la adhesión a códigos de conducta o adhesión a esquemas de certificación, siempre que esta adhesión incluya compromisos vinculantes y ejecutables [art. 46.2.e) y f)]. Dichos compromisos vinculantes se plasmarán la mayoría de las ocasiones a través de un contrato.

2) Garantías adecuadas que sí precisan de autorización previa. Art. 46.3. RGPD:[55]:

(55)Véase art. 42 LOPDGDD.

"Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o (se trata de las cláusulas *ad hoc* autorizadas por APD nacional)

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados."

En este caso puede tratarse por ejemplo de un Memorando de entendimiento entre autoridades públicas de países distintos.

Todos estos instrumentos han de contener derechos exigibles y acciones legales efectivas para los interesados.

Así mismo, aquellas decisiones de APD tomadas en base a la DPD continuaran siendo válidas por el momento (art. 46.5 RGPD).

3.10.4. Las excepciones para situaciones específicas

Según prevé el art. 49.1 RGPD, en ausencia de una decisión de adecuación o de garantías adecuadas, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional *únicamente* se realizará si se cumple alguna de las condiciones siguientes:

- el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

- la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

- la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

- la transferencia sea necesaria por razones importantes de interés público;

- la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

- la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

- la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos (así lo establece el art. 49.1[56] *infine* RGPD).

[56] Véase art. 43 LOPDGDD.

En cuanto a las excepciones que plantea el RGPD, tampoco se plantean grandes novedades. Las excepciones previstas son prácticamente las mismas que las de la DPD.

Sin embargo el RGPD introduce una novedad que consiste en la posibilidad de transferir datos sobre la base del interés legítimo del RT.

Esto será posible si se cumplen unos determinados parámetros: limitarse a supuestos en que las transferencias no son repetitivas, no se suceden en el tiempo, y afectan un número limitado de interesados. En cuanto a qué debe entenderse por número limitado de interesados es algo que se irá determinando y analizando en la práctica.

El RT en este caso deberá llevar a cabo una ponderación entre el derecho a transferir los datos y el derecho e intereses de los afectados y concluir que no prevalecen sobre los del RT. En este caso será preciso establecer medidas de salvaguardia. Todo ello debe quedar documentado y debe informarse al interesado y a la APD.

En cuanto al Privacy Shield

El Privacy Shield se basa en una decisión de adecuación de la Comisión que se adoptó tras el vacío que dejó la anulación de los Principios de Puerto seguro (Safe Harbour), como consecuencia de la STJUE en el caso Schrems.

Las transferencias de datos entre EEUU y Europa, hasta la anulación de los Principios de puerto seguro, se regían por una decisión de la Comisión según la que las empresas americanas que cumplían con la normativa aprobada se convertían en destinos seguros (safe harbour) y podían transmitirse datos a las mismas.

Tras la anulación de los Principios de puerto seguro, la Comisión y los EEUU negociaron un nuevo marco que permitiera el intercambio de datos y se aprobó el Privacy Shield. Sin embargo este sistema también está sujeto a bastantes críticas. El grupo del art. 29 declaró que dicho acuerdo no cumplía con todos los aspectos que exige la normativa europea de protección de datos (Opinión 1/2016). En octubre del 2018 tuvo lugar la segunda reunión conjunta entre la Comisión europea y el EDPB para revisar el estado de la cuestión del "Privacy shield". Las conclusiones de la Comisión se publicaron el 19 de diciembre del 2018. El EDPB, del 22 de enero de 2019, publicó sus conclusiones, en el documento: "Privacy shield: EU - U.S. Privacy Shield - Second Annual Joint Review, Adopted on 22 January 2019", que puede encontrarse aquí: https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en. Por otro lado, el TJUE tendrá que pronunciarse sobre si el "Privacy Shield" se adecua a la normativa europea en el caso planteado: C-311/18 (Facebook Ireland and Schrem).

3.11. Responsabilidad y sanciones

3.11.1. Responsabilidad administrativa

Al plantear, al inicio de estos materiales, las razones de la reforma que llevó a la adopción del RGPD se subrayó el hecho que existía una diversidad legislativa cada vez mayor entre los Estados miembros. Uno de los ámbitos donde se pone más en evidencia la existencia de esta diversidad era en relación al régimen sancionador. Efectivamente, existen países en que el régimen sancionador era prácticamente inexistente mientras que en otros se establecían sanciones económicas muy importantes, que podían llegar hasta 600.000 € de multa (como es el caso de España).

La aprobación del RGPD tendría que solucionar esta divergencia normativa.

Según dispone el art. 57.1.a) RGPD, sin perjuicio de otras funciones, corresponde a cada autoridad de control, en su territorio, controlar y garantizar la aplicación del Reglamento.

Para poder llevar a cabo esta y otras funciones se otorgan a las autoridades de control una serie de poderes, recogidos en el art. 58. Este precepto distingue entre poderes de investigación (art. 58.1 RGPD) y poderes correctivos (art. 58.2). Entre estos últimos hay que hacer referencia a la posibilidad de sancionar al RT o ET con una amonestación cuando las operaciones de tratamiento hayan infringido el Reglamento (art. 58.2.b) y también imponer multas administrativas (art. 58.2.i).

La imposición de multas se regula en el Capítulo VIII RGPD (recursos, responsabilidad y sanciones).

El art. 83 RGPD lleva por rúbrica: "Condiciones generales para la imposición de multas administrativas".

Merece la pena subrayar el hecho que se establezca 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 y pueden ser a título adicional o a título sustitutivo de las medidas que prevé el artículo 58.2 (art. 83.2 RGPD). Para decidir la imposición de una multa administrativa y su cuantía se tendrán en cuenta los elementos recogidos en el art. 83.2. a) a k).

En relación a las cuantías, debe subrayarse que se establece una cantidad que opera como una cantidad máxima pero también la sanción puede fijarse en base a un determinado porcentaje del volumen de negocio total. Este último elemento ha sido acogido favorablemente. Las sanciones en base a una cantidad fija pueden ser muy graves para una empresa y no serlo tanto para otra. En cambio, el hecho de fijar la cantidad en concepto de multa en base a un porcentaje, parece más equitativo.

La tipificación de las sanciones (art. 83.4, 5 y 6) es la siguiente:

- Multa hasta 10 M € o, para empresas, se puede establecer hasta el 2 % de volumen de negocio anual a nivel mundial. (Se optará por la de mayor cuantía), para los supuestos contemplados en el art. 83.4)
- Multa hasta 20 M € o hasta el 4 %, para los casos contemplados en el art. 83.5 RGPD.
- Multa hasta 20 M € o hasta el 4 %, en determinados supuestos de incumplimiento de las resoluciones.

En cuanto a la legislación española, el Título IX de la LOPDGDD se dedica al régimen sancionador.

El art. 70 hace referencia a los sujetos responsables, que incluye a los RT, ET, representantes de ambos, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta. En cambio, el régimen sancionador establecido en el Título IX no es aplicable al delegado de protección de datos (art. 70.2).

El art. 72 regula los supuestos que constituyen una infracción muy grave de la normativa de protección de datos. El art. 73 los supuestos constitutivos de infracciones consideradas graves y el art. 74 las consideradas leves.

Por otro lado, el art. 75 contempla la interrupción de la prescripción de la infracción y el art. 76 hace referencia a sanciones y medidas correctivas.

Entre las medidas correctivas, hay que subrayar la prevista en el art. 76.4 LOPDGDD:

> "Tiene que ser objeto de publicación en el «Boletín Oficial del Estado» la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción sea superior a un millón de euros y el infractor sea una persona jurídica.
>
> Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, hay que atenerse a su normativa aplicable".

Al respecto, hay que subrayar que el legislador español ha mantenido la distinción, en cuanto al régimen sancionador entre los llamados ficheros de titularidad privada y los de titularidad pública, tal y como hacía la LOPD de 1999. En el caso de los ficheros de titularidad pública, no se establecen sanciones económicas. El RGPD deja este aspecto (decidir si se sancionan económicamente los tratamientos efectuados por el AAPP) a la decisión de cada Estado.

La LOPDGDD complemento del RGPD

En realidad la LOPDGDD no tipifica (regula) las conductas constitutivas de infracción, ya que esto lo hace el RGPD. Lo que hace la LOPDGDD es solo complementar el RGPD a título ejemplificativo. De hecho el preámbulo de la LOPDGDD establece que la clasificación se ha hecho solo a los efectos de determinar los plazos de prescripción.

La LOPD de 1999

En la LOPD de 1999, el régimen sancionador relativo a los ficheros privados se regulaba en los arts. 44 y 45 LOPD, y en el caso de los ficheros relativos a las AAPP, en los artículos 46 y 48 LOPD.

En el caso de determinados responsables o encargados de tratamientos, como por ejemplo la Administración General del Estado, las administraciones de las comunidades autónomas y las entidades que integran la Administración local (art. 77.1.c LOPDGDD), resulta aplicable el art. 77.

En este caso (a pesar de que no hay sanciones económicas), se establecen las siguientes medidas:

> Cuando los sujetos nombrados en el art. 77.1 cometan alguna de las infracciones tipificadas en la Ley, la autoridad de protección de datos competente tiene que dictar una resolución que las sancione con una amonestación. La resolución tiene que establecer así mismo las medidas que proceda adoptar porque cese la conducta o se corrijan los efectos de la infracción que se haya cometido.
>
> La resolución se tiene que notificar al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, si procede, y a los afectados que tengan la condición de interesado, si procede (art. 77.2).
>
> Así mismo, "Sin perjuicio de lo que establece el apartado anterior, la autoridad de protección de datos tiene que proponer también la iniciación de actuaciones disciplinarias cuando haya indicios suficientes para hacerlo. En este caso, el procedimiento y las sanciones que se tienen que aplicar son los que establece la legislación sobre régimen disciplinario o sancionador que sea aplicable.
>
> Así mismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no se hayan atendido debidamente, en la resolución en que se imponga la sanción se tiene que incluir una amonestación con la denominación del cargo responsable y se tiene que

ordenar la publicación en el «Boletín Oficial del Estado» o autonómico que corresponda" (art. 77.3)[57].

(57)La previsión del art. 77.3 LOPDGDD ya estaba en parte recogida en el art. 46 LOPD de 1999. Pero la diferencia más importante es la que contiene el art. 77.3.2 de la LOPDGDD, que prevé incluir también una amonestación pública, cuando las infracciones sean imputables a autoridades o directivos, si se acredita la existencia de informes técnicos o recomendaciones para el tratamiento que no se hayan atendido debidamente.

3.11.2. Responsabilidad civil

Es preciso no confundir el régimen sancionador previsto en la legislación con aquellos otros supuestos en que como consecuencia del incumplimiento de lo dispuesto en la norma, los interesados sufran daños y perjuicios.

El art. 82 RGPD (Derecho a indemnización y responsabilidad), prevé que: "cualquier persona que ha sufrido daños y perjuicios, materiales o inmateriales, como consecuencia de una infracción de este Reglamento, tiene derecho a percibir una indemnización del responsable o del encargado del tratamiento por los daños y perjuicios sufridos".

Se trata de una responsabilidad objetiva, en la medida que el art. 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".

Nota

En ningún momento se hace referencia a la posibilidad de exonerarse de responsabilidad acreditando que no ha concurrido culpa o negligencia.

Grimalt, haciendo referencia a la LORTAD, señala que "[...] el legislador hace depender el régimen de responsabilidad civil de un incumplimiento del estatuto jurídico del responsable del fichero; no vincula el deber de reparar el daño a la mera existencia de un tratamiento [...] es necesario que se pueda imputar al responsable un incumplimiento y que de este se derive el daño".

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

Efectivamente, constituye una infracción grave [en base al artículo 73.f) LOPDGDD, "la falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679".

Por lo tanto, la falta de adopción de las medidas mencionadas puede constituir un supuesto de infracción grave. Pero, además, si a consecuencia de esta falta de seguridad se producen daños económicos al afectado, esta conducta origina así mismo el deber de resarcir los perjuicios económicos y morales ocasionados (responsabilidad civil).

Lectura recomendada

Al respecto, vale la pena consultar Pedro Grimalt Servera (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales* (pág. 147). Granada: Parteras. (A pesar de que la obra hace referencia al antiguo marco regulador, los conceptos que se tratan son claves para entender este aspecto.)

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

Para concluir también debe quedar claro que en la medida que la responsabilidad civil y la responsabilidad administrativa obedecen a finalidades diferentes, pueden concurrir las dos o puede existir la una sin la otra.

3.12. Garantía de los derechos digitales

El Título X de la LOPDGDD se dedica a la garantía de los derechos digitales. Este título también fue introducido en la fase de enmiendas, no estaba contenido en el Proyecto inicialmente presentado.

El art. 79 declara que "Los derechos y libertades consagrados en la Constitución y en los tratados y convenios Internacionales en los que España sea parte son plenamente aplicables a Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet tienen que contribuir a garantizar su aplicación".

Los derechos reconocidos en este título son de naturaleza diversa. Hay algunos que tienen el carácter de derecho fundamental (como, por ejemplo, el art. 87 que hace referencia al derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral) y otros que no tienen este rango como, por ejemplo, el derecho a la seguridad digital (art. 82).

Por otro lado, el objeto de estos derechos es bastante diferente.

Por un lado, se pueden distinguir aquellos artículos que hacen referencia al funcionamiento de la red: como, por ejemplo, el derecho a la neutralidad de Internet (art. 80), el derecho de acceso universal a Internet (art. 81), el derecho a la seguridad digital (art. 82) o el derecho de portabilidad en servicios de redes sociales y servicios equivalentes (art. 95).

Otros preceptos hacen referencia a los menores y ya han sido analizados en otros epígrafes de estos materiales como, por ejemplo, el derecho a la educación digital (art. 83); la protección de los menores en Internet (art. 84) y la protección de datos de los menores en Internet (art. 92).

Otro grupo de artículos están más vinculados al ejercicio de la libertad de expresión y sus límites en relación con la intimidad y protección de datos: derecho de rectificación en Internet (art. 85), derecho a la actualización de informaciones en medios de comunicación digitales (art. 86), derecho al olvido en búsquedas de Internet (art. 93) o el derecho al olvido en servicios de redes sociales y servicios equivalentes (art. 94).

Hay que remarcar que hay un conjunto de preceptos que hacen referencia al ámbito laboral: derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87); derecho a la desconexión digital en el ámbito laboral (art. 88); derecho a la intimidad ante el uso de dispositivos de videovigilancia y de grabación de sonidos en el puesto de trabajo (art. 89); derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90), o bien los derechos digitales en la negociación colectiva (art. 91).

Finalmente, se reconoce un derecho al testamento digital (art. 96) que hace referencia al acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas difuntas y la posibilidad de acceder a los contenidos de las personas muertas e impartir instrucciones a los prestadores relativas a la utilización, destino o supresión de los contenidos.

Cierra esta relación de Derechos un precepto que hace referencia a las políticas de impulso de los derechos digitales (art. 97).

Bibliografía

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

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

Burkert, H. (1999). "Privacy-Data Protection: a German/European Perspective". En: *Second symposium of the German American Academic Council's Project "Global Networks and Local Values"* (pág. 43-69). Massachusetts: Woods Hole. Disponible en: http://www.coll.mpg.de/text/second-symposium-german-american-academic-council%E2%80%99s-project-global-networks-and-local-values-wo

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". En: *Computer Law & Security Review: the International Journal of Technology Law and Practice* (vol. 30, núm. 6, pág. 633-642).

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

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

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

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.

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

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

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.

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).

Peguera, Miquel. *The Shaky Ground of the Right to Be Delisted* (Agosto 10, 2015). 18 Vanderbilt Journal of Entertainment & Technology Law 507 (2016). Available at SSRN: https://ssrn.com/abstract=2641876 or http://dx.doi.org/10.2139/ssrn.2641876

Peguera, Miquel. *In the Aftermath of Google Spain: How the 'Right to Be Forgotten' is Being Shaped in Spain by Courts and the Data Protection Authority* (Julio 1, 2015). International Journal of Law and Information Technology (vol. 23, núm. 4, pág. 325-347). Available at SSRN: https://ssrn.com/abstract=2669081

Pizzo Chiacchio, A. di (2016). "Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso «Google Spain» la interpretación de la responsabilidad de los

gestores de motores de búsqueda en la implementación del derecho al olvido digital". *Revista jurídica de Catalunya* (vol. 115, núm. 4, págs. 939-976). ISSN 1575-0078.

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. http://www.privacyconference2009.org/program/Presentaciones/index-ides-idweb.html

Rallo Lombarte, A. (dir.) (2019). "Tratado de Protección de Datos actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales" . Valencia: Tirant lo Blanch.

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).

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

Suné Llinás, E. (2000). "Introducción y protección de datos personales". En: *Tratado de derecho informático* (vol. I, 2.ª ed.). Madrid: Servicio de Publicaciones de la 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* (pág. 150). Madrid: Edisofer.

Vilasau Solana, M. (2019). "Las exigencias de información en el RGPD y en la LO 3/2018 de Protección de Datos y garantía de los derechos digitales, ¿contribuyen a la formación de un consentimiento de mejor calidad?". En: R. García Mahamut y B. Tomás Mallén (Eds.). *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (pág. 209-236). Valencia: Tirant lo Blanch.

Vilasau Solana, M. (2019). "El consentimiento general y de menores". En: A. Rallo Lombarte (dir.), Tratado de Protección de Datos actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (pág. 197-251). Valencia: Tirant lo Blanch.

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