GABILEX
Nº 6
JUNIO 2016
www.gabilex.jccm.es

"CONTENIDO Y NOVEDADES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE (REGLAMENTO UE 2016/679, DE 27 DE ABRIL DE 2016)"

D. ROBERTO MAYOR GÓMEZ

Letrado de la Junta de Comunidades de Castilla-La Mancha

Fecha de finalización del trabajo: 15 de junio 2016

SUMARIO

1. LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA: ANTECEDENTES

En primer lugar, resulta conveniente hacer una breve referencia a la evolución de la regulación normativa de la protección de datos en la Unión Europea con carácter previo a la reciente publicación en el Diario Oficial de la Unión Europea, de fecha 4 de mayo de 2016, del 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), en adelante RGPD[1].

Así, en cuanto a la regulación jurídica de la protección de datos en Europa, cabe señalar que las normas más relevantes en este ámbito han tenido una influencia indudable en las normativas nacionales de los Estados miembros de la Unión Europea, implicando un aumento del nivel de protección y un efecto homogeneizante.

[1] Para mayor información sobre la evolución de la normativa en protección de datos, véase la obra de Rebollo Delgado, L y Serrano Pérez, Mª: *Manual de protección de Datos,* págs 39-58, Dikynson. Madrid 2014.

El primer texto normativo, en el ámbito estrictamente europeo, que garantiza como derecho fundamental el respeto a la vida privada está representada por el artículo 8 del Convenio Europeo de Derechos Humanos, aprobado en Roma en 1950.

Posteriormente, el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que entró en vigor el 1 de diciembre de 2009, contiene una referencia expresa a la protección de datos de carácter personal, reconociéndose a toda persona el derecho a la protección de los datos de carácter personal que la conciernan, que se tratarán de modo leal, para fines concretos, y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, así como el derecho a acceder a los datos recogidos que la conciernan y a su rectificación. También se prevé expresamente que el respeto de estas normas quedará sujeto al control de una autoridad independiente.

En sentido similar, en el artículo 16 del Tratado de Lisboa de 2007, que modifica el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea, se reconoce a toda persona el derecho a la protección de los datos de carácter personal que la conciernan, que el respeto de estas normas quedará sujeto al control de una autoridad independiente, y que el Parlamento Europeo y el Consejo serán los encargados de establecer las normas sobre protección de datos.

Hay que partir de la base que, en todo caso, ya en el Convenio n.º 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, quedó fijado un marco amplio de protección de los derechos de la persona frente a las posibles intromisiones por parte de la informática, si bien, obviamente adaptada a la tecnología del momento, y, por tanto, necesitada de un desarrollo normativo posterior. En el mencionado Convenio ya se enumeraban una serie de principios esenciales en materia de protección de datos (pertinencia de los datos, utilización no abusiva, derecho de olvido, lealtad, exactitud, publicidad, acceso individual, seguridad…).

En el Acuerdo de Schengen, de 14 de junio de 1985, que tiene como principal finalidad hacer efectiva la libertad de circulación de ciudadanos en la Unión Europea mediante la supresión gradual de las fronteras interiores, se contienen también algunas referencias específicas a la protección de datos de carácter personal para facilitar la coordinación y el control entre los países miembros en sus artículos 7 y 9.

Una de las normas comunitarias más relevantes que han sido aprobadas en el ámbito de la protección de datos, sin duda, ha sido la Directiva 95/46/CE del Parlamento Europeo y del Consejo[2], de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que

[2] El artículo 94 del 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) señala que: *«1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018. 2.Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.».*

respecta al tratamiento de datos personales y a la libre circulación de estos datos, que tenía como principal objetivo armonizar las normas de los Estados miembros al contenido de la misma.

Las definiciones de conceptos fundamentales en este ámbito son, esencialmente, los ya establecidos en el Convenio de 28 de enero de 1981 del Consejo de Europa, si bien en cuanto al ámbito de aplicación se extiende no solamente a los ficheros automatizados sino también a los manuales, fijándose un plazo de 12 años para su transposición (en España se produjo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD), y se excluye expresamente de su ámbito de aplicación, entre otras, el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, seguridad pública, defensa...

También se incluyen dentro del campo de aplicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, que afecten al tratamiento de datos de carácter personal.

En cuanto a los principios que resultaban de aplicación se distinguía entre: los principios relativos a la calidad de los datos (artículo 6); y los principios relativos a la legitimación del tratamiento (artículo 7).

Dentro de los principios relativos a la calidad de los datos se enumeraban los siguientes, que requieren que los datos personales sean:

a) tratados de manera leal y lícita

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines, considerando que no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente

d) exactos y, cuando sea necesario, actualizados, y que deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

En cualquier caso, se contemplaba que los Estados miembros establecieran las garantías apropiadas para que los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

Respecto a los principios relativos a la legitimación del tratamiento, se disponía que los Estados miembros tenían que disponer que el tratamiento de datos personales sólo podía efectuarse en alguno de los supuestos específicos que incluía:

a) el interesado ha dado su consentimiento de forma inequívoca

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento

d) es necesario para proteger el interés vital del interesado

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva 95/46/CE.

Hay que tener en cuenta que en los considerandos que precedían al articulado se contenían importantes principios o reglas de interpretación sobre conceptos esenciales (tratamiento ilícito, consentimiento, finalidad, derecho de acceso, seguridad…).

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, regulaba también un aspecto importante como es el concerniente a la transferencia de datos personales a terceros países, en su capítulo IV, estableciendo como regla general que solamente podía efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, "*el país tercero de que se trate garantice un nivel de protección adecuado".*

En cuanto a que debe entenderse por carácter adecuado del nivel de protección, en la propia Directiva se aclaraba que se evaluaría atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos, y que en particular, "*se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

En todo caso, en el artículo 26 de la citada Directiva se contenían unas excepciones en las que se podía efectuar una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido anteriormente (el interesado haya dado su consentimiento inequívocamente a la transferencia prevista; 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 tomadas a petición del interesado; la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero…).

El Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo[3], de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, tienen por finalidad garantizar en toda la Unión Europea una aplicación coherente y homogénea de las normas de protección de los derechos y las libertades fundamentales de las personas en lo que respecta al tratamiento de los datos personales. También se persigue que se especifiquen las obligaciones de los responsables del tratamiento dentro de las instituciones y los organismos comunitarios en materia de tratamiento de datos y que se cree una autoridad de control independiente responsable de la vigilancia de los tratamientos de datos personales efectuados por las instituciones y los organismos comunitarios.

Como aspectos destacables del Reglamento n.º 45/2001 del Parlamento Europeo y del Consejo[4] hay que resaltar los siguientes:

a) el tratamiento reforzado de la prohibición de tratamiento de los datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad, salvo las excepciones contempladas (artículo 10).

b) la creación de la figura del Supervisor Europeo para la Protección de Datos de carácter personales (artículo 41 y ss).

c) la creación de una tabla de derechos para los interesados, y así, el derecho a la información, derecho de acceso, derecho de rectificación, derecho de bloqueo, derecho de supresión, derecho de oposición, obligación de notificar a terceros… (artículos 11 y ss).

d) fijación de los criterios para la licitud del tratamiento de datos (artículos 5 y 6)

e) establecimiento de reglas para la transmisión de datos personales según los destinatarios sean o no distintos de las instituciones y los organismos comunitarios (artículos 8 y 9).

Finalmente, otras importantes normas comunitarias que han regulado aspectos esenciales del ámbito de la protección de datos son:

---

[3] Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

[4] El artículo 2.3 del 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) señala que: «*El Reglamento (CE) nº 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) nº 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*».

· La Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones que tiene por objeto establecer la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad (artículo 1).

· La Directiva 2000/31/CE del Parlamento Europeo y del Consejo[5], de 8 de junio de 2000, cuyo objetivo es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

· La Directiva 2002/58/CE del Parlamento Europeo y del Consejo[6], 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, cuyo objetivo es armonizar las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.

2.- EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE: PROCESO DE ELABORACIÓN, ESTRUCTURA, OBJETO, ÁMBITO DE APLICACIÓN, Y PRINCIPIOS DE LA NORMA

[5] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

El artículo 2.4 del 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) señala que: *«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».*

[6] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

El artículo 95 del 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) señala que: *«El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE».*

2.1 PROCESO DE ELABORACIÓN

El nuevo marco jurídico propuesto para la protección de los datos personales en la UE es el resultado de un proceso largo e intenso cuyo origen se puede situar, desde un punto de vista institucional, en el año 2010 cuando el Consejo Europeo invitó a la Comisión Europea a evaluar el funcionamiento de los instrumentos de la UE en materia de protección de datos y a presentar, en caso necesario, nuevas iniciativas legislativas y no legislativas[7]. Así, en su resolución sobre el Programa de Estocolmo el Parlamento Europeo[8] mantuvo una posición favorable a la elaboración de un régimen general de protección de datos en la UE, y la Comisión Europea[9] también planteó la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplicase de forma coherente en el contexto de todas las políticas de la UE.

En el seno de la Unión Europea se empieza a considerar la necesidad de establecer un marco más sólido y coherente en materia de protección de datos en la UE, que evite la excesiva fragmentación en la aplicación de la protección de datos de carácter personal en el ámbito de la Unión Europea, y que fortalezca la seguridad jurídica de los ciudadanos europeos, operadores económicos y las autoridades públicas.

Se comienza así a realizar una amplia consulta a los actores interesados, mediante conferencias, seminarios, grupos de trabajo…[10] que desembocan finalmente en la Resolución del Parlamento Europeo, de 6 de julio de 2011, que aprobó un informe favorable a reformar el marco de la

[7] «Programa de Estocolmo: Una Europa abierta y segura que sirva y proteja al ciudadano», DO C 115 de 4.5.2010, p.1.

[8] Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos: Programa de Estocolmo», adoptada el 25 de noviembre de 2009 [P7_TA (2009)0090].

[9] Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», COM (2010) 609 final.

[10] Consulta sobre el marco jurídico para el derecho fundamental a la protección de datos de carácter persona (9 de julio al 31 de diciembre de 2009); consulta sobre el enfoque global de la Comisión sobre la protección de datos de carácter personal en la Unión Europea (4 de noviembre de 2010 al 15 de enero de 2011); mesa redonda sobre la reforma de la protección de datos organizada por la Vicepresidenta de la Comisión Europea Viviane Reding (noviembre de 2010); la Comisión Europea y el Consejo de Europa organizaron una conferencia de alto nivel con el fin de debatir cuestiones relacionadas con la reforma del marco jurídico de la UE y con la necesidad de establecer unas normas de protección de datos comunes a escala mundial el Día de la protección de datos (28 de enero de 2011); las presidencias húngara y polaca del Consejo acogieron sendas conferencias sobre protección de datos (16 y 17 de junio de 2011 y el 21 de septiembre de 2011); el «Grupo de Trabajo del Artículo 29» emitió diversos dictámenes y realizó aportaciones útiles a la Comisión Europea [«El futuro de la intimidad» (2009, WP 168); sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (1/2010, WP 169); sobre la publicidad del comportamiento en línea (2/2010, WP 171); sobre el principio de la obligación de rendir cuentas (3/2010, WP 173); sobre la legislación aplicable (8/2010, WP 179), y sobre el consentimiento (15/2011, WP 187)]; el Supervisor Europeo de Protección de Datos también emitió un dictamen general sobre los temas planteados en la Comunicación de la Comisión de noviembre de 2010.

protección de datos[11]. En sus conclusiones, adoptadas el 24 de febrero de 2011, el Consejo de la Unión Europea manifestó igualmente su apoyo a la voluntad de la Comisión Europea de reformar el marco de protección de datos. También el Comité Económico y Social Europeo se mostró a favor del objetivo de la Comisión de garantizar una aplicación más coherente de las normas de la UE en materia de protección de datos en todos los Estados miembros y una revisión adecuada de la Directiva 95/46/CE[12].

En fecha 27 de enero de 2012 por la Comisión Europea se elaboró una Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos).

El texto de la Propuesta de Reglamento del Parlamento Europeo y del Consejo, de fecha 27 de enero de 2012 fue sometido a numerosas modificaciones durante más de 3 años, hasta que el Parlamento y la Comisión alcanzaron el acuerdo sobre el texto del reglamento general de protección de datos el 15 de diciembre de 2015, y en una reunión extraordinaria, la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (LIBE) aprobó el texto acordado en los diálogos tripartitos el 17 de diciembre de 2015.

En fecha 18 de diciembre de 2015, el Comité de Representantes Permanentes (COREPER) confirmó los textos transaccionales acordados con el Parlamento Europeo sobre la reforma de la protección de datos que se presentarían para su adopción por el Consejo, y posteriormente por el Parlamento, por lo que la previsión era ya en aquel momento que el Reglamento entrara en vigor en la primavera de 2018[13].

Finalmente, en el Diario Oficial de la Unión Europea, de fecha 4 de mayo de 2016, se publicó 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), en adelante RGPD.

2.2 ESTRUCTURA

En cuanto a la estructura del RGPD, está constituida por 173 considerandos previos, y 99 artículos divididos en 11 capítulos:

Capítulo I, “Disposiciones Generales” (artículos 1-4)

[11] Resolución del PE, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)

[12] SEC (2012) 72.

[13] Rodriguez Ballano, S y Vidal, M: *Año nuevo..., Reglamento de Protección de Datos nuevo,* Actualidad jurídica Aranzadi, ISSN 1132-0257, Nº 915, 2016, pág. 10.

Capítulo II, "Principios" (artículos 5-11)

Capítulo III," Derechos del interesado" (artículos 12-23), divido en cinco secciones: Transparencia y modalidades**;** Información y acceso a los datos personales; Rectificación y supresión; Derecho de oposición y decisiones individuales automatizadas; y Limitaciones.

Capítulo IV, "Responsable del tratamiento y encargado del tratamiento" (artículos 24-43), divido en cinco secciones: Obligaciones generales; Seguridad de los datos personales; Evaluación de impacto relativa a la protección de datos y consulta previa; Delegado de protección de datos, y Códigos de conducta y certificación

Capítulo V, "Transferencias de datos personales a terceros países u organizaciones internacionales" (artículos 44-50)

Capítulo VI, "Autoridades de control independiente" (artículos 51-59), dividido en dos secciones: Independencia; y Competencia, funciones y poderes

Capítulo VII, "Cooperación y coherencia" (artículos 60-76), dividido en tres secciones: Cooperación y coherencia; Coherencia; y Comité europeo de protección de datos

Capítulo VIII, "Recursos, responsabilidad y sanciones" (artículos 77-84)

Capítulo IX, "Disposiciones relativas a situaciones específicas de tratamiento" (artículos 85-91)

Capítulo X, "Actos delegados y actos de ejecución" (artículo 92 y 93)

Capítulo XI, "Disposiciones finales" (artículo 94-99)

Por otra parte, el RGPD deroga expresamente la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018, indicando además que cualquier referencia que se contenga a la citada Directiva que se deroga, se entenderá hecha a dicho RGPD. De la misma manera, cualquier referencia al Grupo de protección de las personas en lo que refiere al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se tiene que entender hecha al Comité Europeo de Protección de Datos establecido por este RGPD (artículo 94).

También se contempla que el RGPD no impondrá obligaciones adicionales a las personas físicas o jurídicas, en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE (artículo 95).

Respecto a los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido ya celebrados por los Estados miembros con anterioridad al 24 de mayo de 2016, y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, se dispone que seguirán en vigor hasta que sean modificados, sustituidos o revocados (artículo 96).

Finalmente, en cuanto a la entrada en vigor y aplicación de este RGPD, se declara que entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea, aunque será aplicable a partir del 25 de mayo de 2018 (artículo 99).

2.3 OBJETO

En el artículo 1 del RGPD se contiene cual es el objeto o finalidad de la norma comunitaria, que es regular 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, así como la protección de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. También se contempla como principio programático que 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.

2.4 ÁMBITO DE APLICACIÓN

2.4.1 MATERIAL

Un aspecto esencial es el relativo al ámbito de aplicación material del RGPD, que está descrito en el artículo 2 del RGPD donde se indica que será de aplicación 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.

También se contemplan una serie de supuestos que están excepcionados del ámbito de aplicación, y así se dispone que el RGPD no se aplicará, en particular:

- Al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión

- A la actividad de las autoridades 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

- A las actividades de los Estados miembros comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE

- Al tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

2.4.2 TERRITORIAL

En relación al ámbito territorial de aplicación del RGPD hay que subrayar como novedad que se ha producido una importante extensión, ya que conforme a lo dispuesto en su artículo 3 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 Europea o no. Además, el RGPD se aplica también al tratamiento de datos personales de residentes en la Unión Europea por parte de un responsable o encargado no establecido en la Unión Europea, cuando las actividades de tratamiento estén relacionadas con los aspectos que enumera:

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

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

En definitiva, el RGPD resulta también de aplicación al tratamiento de datos fuera de la Unión Europea, lo que amplía de forma considerable su ámbito de aplicación ya que permitirá, por ejemplo, que sea aplicable a empresas que, hasta este momento, podían estar tratando datos de personas en la Unión Europea y que, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea.

2.5 PRINCIPIOS DE LA NORMA

Los principios aplicables al tratamiento de datos en el RGPD están regulados en su artículo 5, y son básicamente:

- Licitud, lealtad y transparencia; recogidos con fines determinados, explícitos y legítimos («limitación de la finalidad»)

- Limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)

- Exactos y, si fuera necesario, actualizados («exactitud»)

- 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 («limitación del plazo de conservación»)

- Tratados de tal manera que se garantice una seguridad adecuada de los datos personales («integridad y confidencialidad»)

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

3.- PRINCIPALES NOVEDADES

A continuación, procederemos a realizar una enumeración y descripción de las novedades más importantes que introduce el RGPD:

1º) SE CONTIENEN EXPRESAMENTE NUEVOS PRINCIPIOS APLICABLES A LA PROTECCIÓN DE DATOS (ARTÍCULO 5 RGPD)

En concreto, se reconoce en el artículo 5.1 a) RGPD, dentro de los principios relativos al tratamiento, el principio de transparencia en el tratamiento de los datos de carácter personal, que supone el derecho que tiene el titular de los datos a estar informado de manera clara e inequívoca sobre dicho tratamiento, de manera que el interesado debe poder conocer en todo momento quién, cómo y para qué están tratando sus datos personales, así como qué datos personales exactamente están siendo tratados e incidencias que se produzcan sobre los mismos. Se refuerza la información que se debe facilitar a los titulares de los datos, tanto en el supuesto de que los datos se recaben directamente del interesado como si los datos se obtienen de otra fuente ya que, además de la información obligatoria ya establecida en la normativa española actualmente vigente, se tiene que facilitar la información respecto otros elementos (base jurídica del tratamiento, la intención de realizar transferencias internacionales, el plazo de conservación de los datos, el derecho a la portabilidad de los datos…).

El reconocimiento del principio de transparencia implicará, indirectamente, un aumento de la información que el responsable del fichero debe facilitar al titular de los datos con carácter previo al momento de obtener sus datos personales o al momento de aplicar los ya recabados a una nueva finalidad.

Además, en el artículo 5.2 RGPD se menciona expresamente el principio de responsabilidad (accountability), que es objeto de desarrollo en el artículo 24 RGPD[14], que impone al responsable del fichero estar en condiciones de demostrar que cumple los principios aplicables a la protección de datos de carácter personal.

2º) REGULACIÓN DE LOS REQUISITOS PARA ENTENDER VÁLIDAMENTE PRESTADO EL CONSENTIMIENTO (ARTÍCULO 7 RGPD)

El RGPD exige que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco[15]. Para poder considerar que el consentimiento es "inequívoco", se requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado, de

[14] El artículo 24 RGPD, dentro de la **r**esponsabilidad del responsable del tratamiento señala que: "*1. 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 presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. 2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. 3.La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*"

[15] En el artículo 4, apartado 11, se contiene la definición completa del «consentimiento del interesado», como *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".*

manera que el consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos. También se exige que la solicitud de consentimiento sea presentada, si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

Además, el Reglamento prevé que el consentimiento haya de ser "explícito" en algunos casos, como puede ser, por ejemplo, para autorizar el tratamiento de datos sensibles. Se añade, por tanto, un requisito más estricto, reforzando la voluntariedad real del consentimiento puesto que el consentimiento no podrá entenderse que ha sido concedido de forma implícita mediante algún tipo de acción positiva. En definitiva, será necesario que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

Por otra parte, será tan fácil retirar el consentimiento como darlo, y hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento

3º) CONDICIONES APLICABLES AL CONSENTIMIENTO DEL NIÑO EN RELACIÓN CON LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN (ARTÍCULO 8 RGPD)

El RGPD establece cual es la edad en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información[16] (por ejemplo, en las redes sociales) que será a los 16 años (por debajo de esta edad, sería necesario el consentimiento de padres o tutores). En todo caso, se permite rebajar esa edad y que cada Estado miembro establezca la suya propia, siempre que no sea inferior a 13 años, que se considera el límite mínimo[17]. Como cláusula de salvaguarda se

[16] En el artículo 4, apartado 11, se contiene la definición del concepto «servicio de la sociedad de la información», que es *"todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo"* [Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1)].

[17] En el caso de España, ese límite continúa en 14 años, ya que en el informe de la Agencia Española de Protección de Datos (AEPD) 2000-000 se concluye que: "*En consecuencia, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales*".

Este informe se puede consultar en el siguiente enlace de la página de la AEPD: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/index-ides-idphp.php (fecha de la consulta: 5 de junio de 2016).

Además, en relación con el tratamiento de los datos de los menores de edad, el artículo 13 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 señala actualmente que:

dispone que lo anteriormente dispuesto no afectará a las disposiciones generales del derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

En el caso de las empresas que recopilen datos personales, en los supuestos anteriores, el consentimiento tiene que ser verificable y que el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender

4º) SE CONTEMPLAN NUEVAS CATEGORÍAS ESPECIALES DE DATOS PERSONALES (ARTÍCULO 9 RGPD)

A las categorías especiales de datos personales ya existentes hasta este momento (origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, y las infracciones o condenas), se añaden los datos genéticos y los datos biométricos, cuyo tratamiento, en consecuencia, pasa a estar prohibido, con carácter general, en este caso siempre que se lleve a cabo con el fin de identificar de forma única una persona[18].

5º) RECONOCIMIENTO DE NUEVOS DERECHOS EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS (ARTÍCULOS 12-21 RGPD)

"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales".

[18] En el artículo 4, apartados 13 y 14, del RGPD, se contiene la definición completa de los «datos genéticos», como los *"datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona"*; y de los datos biométricos», que se describen como *los "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".*

En el Capítulo III del RGPD (artículos 12 a 21) se contienen los derechos de los interesados, que suponen, al menos en lo que se refiere a la normativa nacional en materia de protección de datos[19], la introducción de nuevos derechos (supresión o derecho al olvido y portabilidad de datos) en el ámbito de la protección de datos y la superación de los denominados derechos ARCO (acceso, rectificación, cancelación y oposición).

El RGPD se refiere ahora a los siguientes derechos:

- Transparencia (art. 12)
- Información (arts. 13 a 14)
- Acceso (art. 15)
- Rectificación (Art. 16)
- Supresión o derecho al olvido[20] (art. 17)
- Limitación del tratamiento (art. 18)
- Portabilidad de datos (art. 20)
- Oposición (art. 21)

Este nuevo derecho a la portabilidad implica, básicamente, que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable en determinadas condiciones[21]. Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado.

El ejercicio del derecho a la portabilidad, que no puede afectar negativamente a los derechos y libertades de otros, se entiende sin perjuicio del derecho de supresión, "derecho al olvido", y no se aplica 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.

6º) REGULACIÓN DEL DERECHO DE SUPRESIÓN, "EL DERECHO AL OLVIDO" (ARTÍCULO 17 RGPD)

En el artículo 17 del RGPD se reconoce expresamente un nuevo derecho, el derecho de supresión, más comúnmente conocido como "derecho al olvido", el cual ya había sido objeto de

[19] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE núm. 298 de 14 de diciembre de 1999) y 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 (BOE núm. 17 de 19 de enero de 2008).

[20] Este nuevo derecho es objeto de análisis en un epígrafe específico del presente trabajo.

[21] El artículo 20 RGPD exige la concurrencia de los siguientes presupuestos: *"a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b); y b) el tratamiento se efectúe por medios automatizados."*

reconocimiento por la jurisprudencia[22], que tiene por objeto garantizar el derecho de los sujetos titulares de los datos a obtener, sin dilación indebida, la supresión de los datos personales que le conciernan del responsable del tratamiento en determinados supuestos, entre otros, cuando los datos no sean necesarios para las finalidades para las que fueron recogidos, cuando los datos personales hayan sido tratados ilícitamente o cuando los datos personales deban suprimirse para cumplir con una obligación legal establecida en la legislación aplicable al responsable del tratamiento.

El responsable que esté obligado a suprimir datos personales deberá adoptar medidas razonables, teniendo en cuenta la tecnología disponible y el coste de su aplicación, así como 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.

El RGPD establece, no obstante lo anteriormente dispuesto, una serie de supuestos tasados que se configuran como excepciones al ejercicio del derecho de supresión:

a) Para ejercer el derecho a la libertad de expresión e información.

[22] El denominado «derecho al olvido» ya había sido reconocido por la jurisprudencia europea y nacional, y así en la Sentencia de 13 de mayo de 2014 del Tribunal de Justicia (UE) Gran Sala, nº C-131/2012, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González, viene a reconocer el «derecho al olvido» en Internet, atribuyendo a los motores de búsqueda la responsabilidad de ponderar los intereses en juego en cada caso (y sin que se eliminen necesariamente los resultados en la web de origen), incluso si están sitos fuera de la Unión Europea, como es el caso de Google Inc.

Por su parte, en la jurisprudencia española, por el Tribunal Supremo, Sala 1ª, se dictó la Sentencia nº 545/2015, de 15 de octubre de 2015, rec. 2772/2013, (Pte: Sarazá Jimena, Rafael), que se pronuncia por primera vez sobre el alcance del llamado "derecho al olvido digital". El TS considera que la difusión de una noticia a través de la página web de una hemeroteca digital supone una vulneración del derecho al honor. En todo caso, se declara que el llamado derecho al olvido digital no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día, ya que la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos, como puede ser los nombres de las personas que aparecen en tales informaciones o su sustitución por las iniciales.

Desde un punto de vista doctrinal, el "derecho al olvido digital" ha sido analizado recientemente, entre otras, en las siguientes obras:

- María Álvarez Caro: *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Editorial Reus, 2015. ISBN 978-84-290-1836-3

- Pere Simón Castellano: *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, 2015. ISBN 978-84-9090-021-5

- Artemi Rallo Lombarte: *El derecho al olvido en internet: Google versus España,* Centro de Estudios Políticos y Constitucionales, 2014. ISBN 978-84-259-1593-2

b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por la legislación aplicable al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

c) Por razones de interés público en el ámbito de la salud pública.

d) Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el ejercicio del derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

e) Para la formulación, el ejercicio o la defensa de reclamaciones

7º) RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS POR LA ADOPCIÓN Y ACTUALIZACIÓN DE LAS MEDIDAS ADECUADAS (ARTÍCULO 24 RGPD)

El RGPD atribuye, en determinadas condiciones, al responsable del tratamiento la aplicación de medidas técnicas y organizativas apropiadas, que se revisarán y actualizarán cuando sea necesario, a fin de garantizar y poder demostrar que el tratamiento es conforme a esta normativa (por ejemplo, la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos).

Para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento se mencionan expresamente la adhesión a códigos de conducta o a un mecanismo de certificación.

8º) REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO (ARTÍCULO 30 RGPD)

En el RGPD se elimina la obligación de comunicar el tratamiento de datos personales a las autoridades de control y se sustituyen por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas.

Así, ahora será cada responsable, encargado y, en su caso, su representante quienes llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, que deberá contener una información de mínimos que se regula en el propio RGPD[23]. En cuanto al funcionamiento de estos registros, constarán por escrito, inclusive en formato electrónico, y estarán a disposición de la autoridad de control que lo solicite.

[23] Las obligaciones anteriormente indicadas 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 (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), o datos personales relativos a condenas e infracciones penales en los términos contemplados en el artículo 10 RGPD.

9º) NOTIFICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL Y COMUNICACIÓN A LOS INTERESADOS DE LAS VIOLACIONES DE SEGURIDAD (ARTÍCULOS 33 Y 34 RGPD)

En el RGPD se introduce una importante novedad en aquellos supuestos en los que se haya producido una violación de la seguridad de los datos personales, ya que hasta este momento no existía ninguna obligación de informar a las autoridades cuando se producía una brecha de seguridad, ya que el responsable del tratamiento deberá notificarla 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. En el caso de que la notificación a la autoridad de control no tenga lugar en el plazo de 72 horas, deberá ir acompañada de la explicación de los motivos de la dilación.

Además, no es suficiente con informar solo a las autoridades, también se requiere, como regla general, comunicar al interesado sin dilación indebida y en un lenguaje claro y sencillo la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias.

Esta comunicación, que debe realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control siguiendo sus orientaciones o las de otras autoridades competentes como las autoridades policiales, debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

10º) EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS (ARTÍCULO 35 RGPD)

Se prevé que el responsable del tratamiento en determinadas condiciones (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)[24], realice una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales junto con el asesoramiento del delegado de protección de datos, si ha sido nombrado.

11º) CONSULTA PREVIA A LA AUTORIDAD DE CONTROL EN CASO DE IDENTIFICARSE RIESGOS EN EL TRATAMIENTO (ARTÍCULO 36 RGPD)

Se regula una consulta previa a la autoridad de control, por parte del responsable del tratamiento que deberá facilitar una concreta información que se detalla, antes de proceder al tratamiento en aquellos supuestos en los que una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

[24] La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos, que será comunicada al Comité Europeo de Protección de Datos.

Si la autoridad de control considera que el tratamiento puede infringir la normativa prevista en el RGPD, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control tiene que asesorar por escrito al responsable, y en su caso al encargado, en un plazo de ocho semanas desde la solicitud de la consulta, aunque este plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto, y suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

También se contempla que los Estados miembros garanticen que se consulte a la autoridad de control durante la elaboración cualquier propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento de datos.

12º) INTRODUCCIÓN DE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS (ARTÍCULOS 37-39 RGPD)

El Reglamento Europeo ha introducido la figura del Delegado de Protección de Datos (DPO), imponiendo su designación al responsable y al encargado del tratamiento, exigiendo la obligatoriedad de su nombramiento a todos los organismos públicos, con la excepción de tribunales que actúen en el ejercicio de la función judicial, y a las entidades privadas, sean éstas consideradas responsables o encargados del tratamiento, cuyas actividades principales conlleven la "observación habitual y sistemática de interesados a gran escala" o el "tratamiento a gran escala de categorías especiales de datos personales" y "de datos relativos a condenas e infracciones penales".

El DPO deberá ser designado atendiendo a sus cualidades profesionales, sus conocimientos sobre las normas de protección de datos personales, su práctica en materia de protección de datos, y su capacidad para realizar las funciones encomendadas en el RGPD. El DPO puede ser un empleado de la plantilla del responsable o del encargado del tratamiento, o actuar mediante un contrato de prestación de servicios. El responsable y al encargado del tratamiento están obligados a apoyar al DPO en la realización de sus funciones, sin que esté sometido a las instrucciones de ningún estamento de la propia compañía, respondiendo y rindiendo cuentas únicamente ante "el más alto nivel jerárquico" de la misma, y se prevé la prohibición expresa de destitución o sanción del DPO con causa en el desempeño de sus funciones.

El DPO desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento, y está obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros. También se contempla que podrá desempeñar otras funciones y cometidos siempre que no den lugar a conflicto de intereses.

En cuanto a las funciones que tendrá el DPO, destacan el asesoramiento general dentro de la compañía en todo lo relativo a protección de datos personales, la supervisión del cumplimiento de la legislación y políticas de privacidad con especial atención a los riesgos asociados a las actividades que llevara a cabo la empresa, la elaboración de informes de evaluación de impacto

de ciertos tratamientos de datos personales y la cooperación con las autoridades de control nacionales.[25]

13º) REGULACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS (ARTÍCULOS 44 a 50 RGPD)

En la normativa de protección de datos en España actualmente vigente, una transferencia internacional de datos es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español[26].

En el ámbito de la transferencia internacional de datos hay que tener en cuenta recientes pronunciamientos del Tribunal de Justicia de la Unión Europea de especial trascendencia en este ámbito y que han tenido una importante incidencia en el texto aprobado[27]. Como destacan

[25] En concreto, el artículo 39 del 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) atribuye, como mínimo, al DPO las siguientes funciones: *«a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento 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; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto».*

[26] En el ordenamiento jurídico español, las transferencias internacionales de datos, se regulan en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, (RLOPD). Más información al respecto se puede encontrar en la página institucional de la AEPD: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado en fecha 6 de junio de 2016].

[27] Véase la Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 (petición de decisión prejudicial planteada por la High Court -Irlanda-Maximillian Schrems/Data Protection Commissioner), Asunto C-362/14. En esta sentencia judicial, el Tribunal de Justicia de la Unión Europea estima que la existencia de una Decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y de la Directiva. En este sentido, el Tribunal de Justicia destaca el derecho a la protección de los datos personales garantizado por la Carta y la función que ésta atribuye a las autoridades nacionales de control, y declara inválida la Decisión de la Comisión de 26 de julio de 2000 [Decisión 2000/520/CE de la

algunos autores, *"la sentencia del TJUE ha marcado un punto de inflexión respecto a cómo se venían realizando las transferencias internacionales de datos de empresas de la Unión Europea a EE.UU., además de determinar las obligaciones que tienen las autoridades de control europeas de atender aquellas denuncias que pueda presentar un ciudadano respecto a un tratamiento de sus datos que implique una transferencia de datos a EE.UU. según el acuerdo de Puerto Seguro*."[28]

Así, si los datos personales se transfieren de la Unión Europea a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión Europea por el nuevo reglamento de protección de datos, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional

Con esta finalidad se encomienda a la Comisión la evaluación del nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país, y en el supuesto que la Comisión no haya adoptado una decisión de adecuación sobre un territorio o sector, la transferencia de datos personales se puede seguir realizando en casos especiales o cuando existan garantías apropiadas (cláusulas tipo de protección de datos, normas corporativas vinculantes, cláusulas contractuales…).

En definitiva, en ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado.

Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, p. 7)]. Como consecuencia de esta sentencia judicial, la autoridad irlandesa de control está obligada a examinar la reclamación del Sr. Schrems con toda la diligencia exigible y, al término de su investigación, deberá decidir si, en virtud de la Directiva, debe suspenderse la transferencia de los datos de los usuarios europeos de Facebook a Estados Unidos porque ese país no ofrece un nivel de protección adecuado de los datos personales.

La referida sentencia judicial pueda consultarse en el siguiente enlace: http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=312534 (fecha de consulta: 6 de junio de 2016).

Hay que tener en cuenta que tras la disolución del acuerdo Safe Harbor, se abrió un período de negociación en el marco del cual, la Comisión Europea y el Departamento de Comercio de EEUU, han alcanzado un acuerdo que permitirá llevar a cabo transferencias internacionales de datos con garantías suficientes, a través del denominado acuerdo Privacy Shield.

[28] García Romero, S: *Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas.* Diario La Ley, Nº 8691, Sección Documento on-line, 28 de enero de 2016, Editorial LA LEY.

14º) INTRODUCCIÓN DEL SISTEMA DE VENTANILLA ÚNICA (ARTÍCULOS 60-67 RGPD)

La introducción de este sistema "One stop shop" permite que los responsables que estén establecidos en varios Estados miembros o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE tengan a una única autoridad de protección de datos como interlocutora.

Asimismo, supone que cada autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, a partir de la entrada en vigor del RGPD valorará si el supuesto tiene carácter transfronterizo, y en caso afirmativo habrá de proceder a iniciar un procedimiento de cooperación entre todas las autoridades afectadas buscando una solución aceptable para todas ellas. En el supuesto que hubiera discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos para que resuelva la controversia mediante decisiones vinculantes para las autoridades implicadas.

En todo caso, ello seguirá permitiendo que los interesados pueden continuar planteando sus reclamaciones o denuncias ante su propia autoridad nacional (en España la AEPD), sin perjuicio de que la gestión será realizada por esa autoridad, que será también responsable de informar al interesado del resultado final de su reclamación o denuncia. La ventanilla única no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado.

15º) CREACIÓN DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (ARTÍCULOS 68-70 RGPD)

El RGPD promueve la creación de un órgano independiente, Comité Europeo de Protección de Datos, que estará formado por representantes de las autoridades de control de cada uno de los estados miembros, así como por el Supervisor Europeo de Protección de Datos y será responsable, entre otras cosas, de garantizar la aplicación coherente del reglamento, asesorar a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, emitir directrices y recomendaciones de buenas prácticas, o ser responsable de la acreditación de los organismos de certificación así como de su revisión periódica.

16º) NUEVA NORMATIVA EN RELACIÓN A LAS SANCIONES Y MULTAS (ARTÍCULOS 82-84 RGPD)

El RGPD contempla la posibilidad de que el interesado que considere vulnerados los derechos, pueda conferir mandato a una entidad, organización o asociación sin ánimo de lucro para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados e incluso y el derecho a ser indemnizado, si así lo establece el Derecho del Estado miembro.

El RGPD declara que el responsable o el encargado del tratamiento tiene que indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de una infracción del Reglamento (artículo 82.1 RGPD), aunque aquellos quedarán exentos de

responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios (artículo 82.3 RGPD).

El régimen sancionador se agrava y se vuelve mucho más exigente que el actual[29], y así una de las novedades que se contemplan en el RGPD en materia sancionadora es la posibilidad de llegar a imponer sanciones, multas administrativas, que pueden alcanzar los 20.000.000 de euros o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. (artículo 83.5 RGPD).

4.- CONCLUSIONES

Como hemos podido comprobar, la aprobación del RGPD supone la introducción de importantes novedades en materia de protección de datos personales, y así, presenta aspectos muy relevantes y positivos, como es el hecho que supone implantar, por vez primera, una regulación jurídica homogénea y uniforme en materia de protección de datos para todos los Estados miembros de la Unión Europea lo que beneficia tanto los consumidores como a las propias empresas, que disponen de una norma única que implantar en todos los países miembros, con la consiguiente seguridad jurídica y transparencia.

Además, el ámbito de protección en materia de protección de datos, para los ciudadanos que forman parte de los Estados miembros de la Unión Europea, se amplía de forma considerable desde un punto de vista subjetivo y territorial puesto que ahora con el RGPD se regula no solamente la protección de los datos personales de las personas físicas, sino también la circulación de esos datos, y ello no solo en el ámbito territorial de la propia Unión Europea, ya que se extiende también al tratamiento de los datos de los ciudadanos europeos fuera del ámbito de la Unión.

Por otra parte, se trata de una norma muy técnica, extensa y minuciosa, resultado de una larga y compleja tramitación, que contiene numerosos conceptos jurídicos indeterminados en su articulado que dificultan su comprensión y que pueden generar problemas interpretativos en el futuro. También ha sido cuestionado por expertos en la materia (Javier Puyol Montero, Paula Ortiz López…) si nos encontramos ante un Reglamento que ya ha nacido desfasado, en la medida que, sorprendentemente, no contempla la regulación jurídica de cuestiones tecnológicas actualmente operativas y de uso masivo por los ciudadanos, que tienen una incidencia directa en los datos personales: Big Data, el Cloud Computing, la Internet de las cosas o BiTech.

La sensación que transmite la lectura del RGPD es que la normativa en materia de cumplimiento, aunque afecta a todos los entornos de la actividad, está concebida fundamentalmente pensando en grandes corporaciones, cuando la pequeña y mediana empresa es la mayoritaria tanto a nivel nacional como europeo.

[29] Véase que en el artículo 45.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), las infracciones muy graves son sancionadas con multas de hasta 600.000 euros.

La entrada en vigor del RGPD y su posterior aplicabilidad plantea igualmente el debate jurídico no resuelto de su compatibilidad y coexistencia con nuestra ley nacional en materia de protección de datos (LOPD), por lo que resultará importante ver la posición al respecto que se mantiene por la AEPD.

En este sentido, resultará también de interés comprobar si la circunstancia que los datos biométricos sean considerados ahora de especial protección va a suponer alguna modificación sustancial en el tratamiento de los datos biométricos en el entorno laboral, y su encaje con la excepción que se prevé en el artículo 9.2 b) RGPD[30] sobre la base del principio de proporcionalidad.

Como ya ha recomendado la AEPD, las empresas deberían comenzar a revisar la forma en la que obtienen y registran el consentimiento, ya que actuaciones que se encuadran en el denominado consentimiento tácito y que son aceptadas bajo la actual normativa nacional de protección de datos dejarán de serlo cuando el Reglamento sea de aplicación.

Además, y como ya hemos expuesto, hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento, por lo que también resultará importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

Finalmente, indicar que resulta bastante previsible que la entrada en vigor del nuevo régimen sancionador implique un considerable incremento de las denuncias que se interponen actualmente en materia de protección de datos puesto que actualmente, en la LOPD, no se prevé ninguna indemnización para los damnificados, solo sanción administrativa para los responsables, situación que cambiará con la entrada en vigor.

BIBLIOGRAFÍA

ÁLVAREZ CARO, M: *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Editorial Reus, 2015. ISBN 978-84-290-1836-3.

GUASCH PORTAS, V: *Las transferencias internacionales de datos en la normativa española y comunitaria.* AEPD y BOE. Madrid 2014.

RALLO LOMBARTE, A: *El derecho al olvido en internet: Google versus España,* Centro de Estudios Políticos y Constitucionales, 2014. ISBN 978-84-259-1593-2.

[30] Este precepto se refiere a que: *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".*

REBOLLO DELGADO, L y SERRANO PÉREZ, Mª: *Manual de protección de Datos.* Dikynson. Madrid 2014.

REBOLLO DELGADO, L Y SERRANO PÉREZ, Mª: *Introducción a la protección de datos.* Dykinson. Madrid 2008.

SIMÓN CASTELLANO, P: *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, 2015. ISBN 978-84-9090-021-5.

TRONCOSO REIGADA, A: *Hacia un nuevo marco jurídico europeo de protección de datos personales*. Revista Española de Derecho Europeo nº 43 de 2012, páginas 25 a 184.