UN NUEVO MODELO DE PRIVACIDAD: EL RETO DE LA TRANSPARENCIA VS. LA ECONOMÍA DEL DATO

A NEW PRIVACY MODEL: THE TRANSPARECY CHALLENGE VS. THE DATA ECONOMY

YOLANDA HERNÁNDEZ VILLALON.- Letrada de la Comunidad de Madrid

SUMARIO.- El presente artículo analiza la evolución en la regulación internacional, europea y nacional del derecho de la protección de datos y el alcance delReglamento 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.

CONTENTS.- The article analyzes the development of international, European and national legislation about the data protection rightand the impact of the General Data Protection Regulation.

PALABRAS CLAVE: Reglamento General de Protección de Datos; derecho internacional, derecho europeo; responsable del tratamiento; encargado del tratamiento; protección de datos; principios; derechos;transferencias de datos; medidas de seguridad; autoridades de control; régimen sancionador; inspecciones; infracciones; sanciones

KEYWORDS: General Data Protection Regulation;treatment responsible; treatment manager; data protection; principles; rights; international law; European law; transfers of personal data; security measures; Data Protection Authorities; remedies; liability; penalties

1. REGULACIÓN DEL DERECHO DE PROTECCIÓN DE DATOS. PRINCIPIOS INSPIRADORES

La configuración del derecho de protección de datos ha experimentado un largo proceso, siendo la evolución tecnológica quien ha marcado la necesaria adaptación legislativa sobre la materia.

Desde 1965, momento en el que L. Roberts y T.Merril conectaron dos ordenadores a través de una línea de teléfono, y comprobaron la posibilidad de transmitir datos, hasta nuestra actualidad, internet y las nuevas tecnologías han generado un nuevo modelo de identidad individual.

Inicialmente, la protección de datos se incluía en el derecho a la intimidad, regulado en el Convenio de Derechos Humanos y Libertades Fundamentales de Roma, de 4 de mayo de 1950[1].

El primer hito normativo internacional sobre la materia fueron dos resoluciones,la Resolución del Comité de Ministros del Consejo de Europa 22, de 26 de septiembre de 1973, sobre protección de la vida privada de las personas físicas respectolos bancos de datos electrónicos en el sector privado, yla Resolución del Comité de Consejo de Ministros del Consejo de Europa 29, de 20 de septiembre de 1974.

Las citadas Resoluciones aunque carecían de carácter jurídico vinculante, recopilaron los principios que han servido de base para el desarrollo legislativo del sector: acceso, cancelación, información sobre la finalidad del tratamiento, calidad de datos o seguridad.

En 1981 el Consejo de Europa emite el primer texto normativo vinculante, el Convenio 108 de 28 de enero de Estrasburgo, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[2] (en adelante, Convenio o Convención 108).

---

[1]Art. 8 del CDHLF.

[2] El artículo 1 delimita su finalidad del siguiente modo: "*el fin del presente convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueran su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente, su derecho a la vida privada, con respeto al tratamiento automatizado de datos de carácter personal correspondiente a dicha persona ("protección de datos")*". España lo firmó el 28 de enero de 1982. El texto entró en vigor el 1 de octubre de 1985.

La denominada “Convención 108” se encuentra en vigor tras la actualización realizada por el propio Consejo de Europa,mediante el Protocolo de 18 de mayo de 2018.El objetivo ha sido adaptarse al Reglamento 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 (en adelante, RGPD).

El Convenio 108 es el único tratado internacional que aborda el derecho de las personas a la protección de sus datos personales, y está abierto a la firma y ratificación de cualquier país. Las partes actuales de la Convención son los 47 Estados miembros del Consejo de Europa, más Mauricio, Senegal, Túnez y Uruguay, mientras que Argentina, Burkina Faso, Cabo Verde, México y Marruecos han sido invitados a adherirse al tratado. Asimismo, es utilizado como modelo para la legislación de protección de datos[3].

El segundo texto internacional relevante sobre la materia, es el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), celebrado en Oviedo el 4 de abril de 1997[4].

En el ámbito internacional, en tercer y último lugarencontramos el Convenio sobre Ciberdelincuencia, suscrito en Budapest, el 23 de noviembre de 2001[5], emitido por el Consejo de Europa.

Desde el punto de vista europeose destaca la siguiente normativa en la materia:

- La Carta de Derechos Fundamentales de la Unión Europea[6].

[3]Esta norma de derecho internacional consagró seis principios fundamentales: el principio finalista, es decir, que la justificación de la base de datos deberá ser accesible en todo momento; el principio de lealtad, licitud; principio de exactitud; principio de publicidad garantizado a través de un registro público de los ficheros automatizados existentes; principio de acceso individual: cada persona tiene derecho a acceder a sus datos y obtener copia de ellos; principio de seguridad, reforzado especialmente respecto los datos sobre el origen racial, la religión, las opiniones políticas, la salud o la orientación sexual, que sólo podrán ser tramitados automáticamente si el estado ofrece garantías suficientes de protección.

[4]Ratificado por España el 23 de julio de 1999. El artículo 5 del Convenio de Derechos Humanos y Biomedicina, consagra el principio general de respetar el consentimiento del paciente para toda actuación que vaya a realizársele en el ámbito sanitario.

[5]En su Capítulo II se regulan las medidas legislativas que deben adoptar los Estados signatarios, para la persecución y control de los delitos informáticos, así como los aspectos procedimentales y de jurisdicción.

[6] Proclamadapor el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza. Actualizada el 12 de diciembre de 2007en Estrasburgo, antes de la firma

- Tratado de Funcionamiento de la Unión Europea[7]
- El RGPD, aplicable en España desde el 25 de mayo de 2018. La adaptación nacional al contenido del RGPD, se encuentra en tramitación parlamentaria[8].

  No obstante, el R.D-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, (en adelante, R.D.-ley 5/2018), ha acomodado al derecho nacional determinados aspectos, que no se han considerado objeto de reserva de ley orgánica:el procedimiento de inspección; el régimen sancionador y el procedimiento en el caso de posible vulneración de la normativa. Ahora bien, se trata de una norma temporal, su vigencia está limitada a la entrada en vigor de la ley orgánica que se encuentra en tramitación (disposición final única del R. D-ley 5/2018).
- El Reglamento 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 el tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de esos datos[9].
- Directiva 58/02/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativo 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)[10]. El considerando 95 del RGPD señala que no se impondrán obligaciones adicionales a las previstas en la Directiva 58/02/CE, en lo concerniente al tratamiento de datos en el ámbito de prestaciones de servicios públicos de comunicación dentro de la Unión Europea.

---

del Tratado de Lisboa; una vez ratificado éste, la Carta devino legalmente vinculante para todos los países, por remisión al artículo 6 del Tratado, a excepción de Polonia y el Reino Unido.

[7] Art. 16

[8] El Consejo de Ministros el 10 de noviembre de 2017 propuso un proyecto de ley orgánica.

[9] El Considerando 17 del RGPD señala que continúa vigente, si bien exige que se adapte a sus principios y normas.

[10] La Directiva 58/2002/CE del Parlamento Europeo y del Consejo fue traspuesta a la normativa española, a través del R.D. 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios y parcialmente en la Ley 32/2003, de 3 de noviembre, de Telecomunicaciones.

Las principales novedades que se derivaron de la Directiva 58/2002/CE fueron: el deber de los Estados de garantizar la confidencialidad de las comunicaciones de los nacionales (art. 5); la obligación de eliminar los datos de tráfico de usuarios y abonados tratados y almacenados por una red pública, cuando no sean necesarios a los efectos de la transmisión de una comunicación (art. 6), y se regularon el uso de las "cookies" (los archivos que llevan la orden de instalación en el disco duro de ordenadores personales).

- Reglamento UE 611/2013, de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, sobre la privacidad y las comunicaciones electrónicas.
- Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[11].
- Directiva 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes, para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales.

A continuación, se examinan los principios consagrados por el RGPD para proteger nuestros datos personales (artículo 5 del RGPD):

1.- Principios de licitud en la obtención de datos y su utilización, así como los principios de lealtad y de transparencia con el interesado.

2.- Principio de limitación de uso a la finalidad correspondiente: los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con los fines. El artículo 89 del RGPD introduce una matización: el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, no se considerará incompatible con los fines iniciales.

3.- Principio de tratamiento minimizado de los datos: se recabarán los adecuados, pertinentes y limitados en relación con los fines perseguidos.

4.- Principio de exactitud y actualización: se deberán adoptar las medidas necesarias para que se supriman o rectifiquen, los datos personales que no sean adecuados para los fines de su tratamiento.

[11]Denominada Directiva NIS (Network and Infomation System) y la Directiva SRI (por seguridad de las redes y de la información). El objetivo es una estrategia de ciberseguridad para impulsar el Mercado Digital Único. Ha sido traspuesta al ordenamiento español, a través del Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad en las redes y sistemas de información, tras iniciar la Comisión un procedimiento formal de infracción contra España por no haberla traspuesto en la fecha límite 9 de mayo de 2018.

5.- Principio de limitación del plazo de conservación.

6.- Principios de seguridad, integridad y confidencialidad.

7. Principio de responsabilidad proactiva: el responsable del tratamiento de datos deberá velar por el cumplimiento de dichos principios y contará con pruebas para justificar su debida diligencia. El objetivo es garantizar la implicación en el resultado final del adecuado tratamiento de los datos.

8.- Garantías de tratamiento para las situaciones específicas.

Las situaciones específicas de tratamiento se regulan en los artículos 85 a 91 del RGPD. La regulación pretende conciliar el derecho de protección de datos, con otros derechos y libertades públicas pilares de una sociedad democrática. Nos detenemos brevemente en alguno de ellos.

En primer lugar, se destaca el necesario equilibrio entre el tratamiento y la libertad de expresión y de información (art. 85 del RGPD). Cada Estado deberá regular por ley la concurrencia del tratamiento de datos personales con estos derechos, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

Respecto el tratamiento y acceso público a documentos oficiales (art. 86 del RGPD), los datos personales obrantes en documentos oficiales en posesión de alguna autoridad pública u organismo público, o una entidad privada, para la realización de una misión en interés público, podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros.

Como se observa el principio de transparencia de tratamiento de datos está conectado con el principio de transparencia de información de las Administraciones Públicas, y en España, éste se regula en el artículo 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno (en adelante Ley

19/2013)[12]. Este principio para el sector público se manifiesta en dos vertientes: el principio de publicidad activa y el principio de publicidad rogada[13].

El principio de publicidad activa se consagra en el artículo 5 de la Ley 19/2013 en los siguientes términos:"*Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública*."

El límite al principio de publicidad activa de la información pública por parte de las administraciones se encuentra en el apartado tercero, del artículo 5, y se compone de dos aspectos: cuando esa publicidad represente perjuicio para aspectos esenciales de la seguridad del Estado (art. 14 de la Ley 19/2013), o afecte a la protección de datos de carácter personal (artículo 15 de la Ley 19/2013).

Por otro lado, la publicidad rogada se regula en los artículos 17 a 22 de la Ley 19/2013.Especial mención merecen las causas de inadmisión del acceso a la información pública[14] previstas en el artículo 18 de la Ley 19/2013: la información esté en curso de elaboración o de publicidad general; se trate de notas, borradores, opiniones, resúmenes, comunicaciones o informes internos; si hay que reelaborar la información; cuando el órgano no cuente con la información que se le solicita; o si la petición es repetitiva o tiene un carácter abusivo no justificado con la finalidad de la transparencia de la Ley.

Regresando al examen de las situaciones especiales de tratamiento en el RGPD, destaca el relativo al ámbito laboral (art. 88 del RGPD).Los Estados a través de normas o de convenios colectivos deberán garantizar la protección de datos, en particular a efectos

[12] El borrador del Real Decreto por el que se desarrolla la Ley 19/2013 se encuentra actualmente en tramitación parlamentaria.
La Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés que entrará en vigor a los tres meses de su publicación, el 24 de diciembre de 2018, regula por un lado las materias que la Ley 19/2013 prevé, e introduce un aspecto novedoso, la regulación de una realidad social importante, los grupos de interés, que han sido abordados por otras Comunidades Autónomas.

[13]La información pública se define en el artículo 13 de la Ley 19/2013: se trata de los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación del Título I de la Ley 19/2013[13], cuando hayan sido adquiridos o elaborados en el ejercicio de sus funciones.

[14] El órgano competente para conocer de la solicitudes de acceso a la información pública es el Consejo de Transparencia y Buen Gobierno (art. 33 a 40 de la Ley 19/2013). Las Comunidades Autónomas contarán con un órgano independiente equivalente (disposición adicional cuarta de la Ley 19/2013), o en su defecto, podrán suscribir convenio con el Estado para que las reclamaciones del artículo 24 de la Ley 19/2013, se resuelvan por el Consejo de Transparencia y Buen Gobierno.

de: contratación de personal; ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo; gestión, planificación y organización del trabajo; igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo; protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

En el mencionado artículo 89.1 del RGPD se regula un supuesto que permite el tratamiento de datos aun cuando no conste consentimiento del interesado, cuando el tratamiento sea con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

A tal fin, se deberá contar con medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Además, siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

Finalmente,se hace mención a la obligación de secreto (art. 90 del RGPD). Los Estados podrán fijar los poderes de las autoridades de control en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado.

2. BASES LEGITIMADORAS DEL TRATAMIENTO DE DATOS

Tras el análisis de los principios inspiradores de la normativa de tratamiento de protección de datos, incluidas sus matizaciones según la concurrencia con otros derechos públicos, pasamos a examinar una novedad sobre la que pivota el RGPD, las bases legitimadoras de la licitud del tratamiento de datos personales:

- El consentimiento del interesado (art. 6 del RGPD).

- El tratamiento necesario para la satisfacción del interés legítimo del responsable del tratamiento (art. 7 del RGPD).

  En primer lugar, se analiza el consentimiento para tratar los datos[15].

  Comenzamos por la definición de consentimiento (artículo 4 del RGPD):

  "*11. 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.''*[16]

En consecuencia, es previsible que el consentimiento tácito, derivado del artículo 14 del R.D. 1720/2007, de 21 de diciembre, por el que se reguló el Reglamento de desarrollo de la L.O. 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, no se mantenga en la normativa española en tramitación.[17].

[15]La STC 292/2000, de 30 de noviembre, delimitó el derecho a consentir el tratamiento de datos del siguiente modo. "(…)*Estos poderes de disposición y control sobre los datos personales que constituyen parte del contenido del derecho fundamental a la protección de datos se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y tratamiento, informático o no, de los datos personales requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro, el poder oponerse a ese uso*".

[16]El Considerando 32 del RGPD señala cómo debe ser el 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 el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos*."

[17] La Agencia Española de Protección de Datos concluyó en su Informe 0195/2017 sobre los efectos del consentimiento: *''Cuando el responsable del tratamiento hubiera recabado el consentimiento de los afectados a través del procedimiento señalado en el artículo 14 del reglamento de desarrollo de la Ley Orgánica 15/1999, dicho responsable deberá a partir del 25 de mayo de 2018, recabar un nuevo consentimiento del afectado, a menos que pueda considerar que el tratamiento viene amparado en la regla de ponderación establecida en el artículo 6.1 f) del reglamento general de protección de datos.''*

No obstante, el Considerando 171 del RGPD indica: *''Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento''*

El artículo 6 del RGPD delimita cuándo se considera que un tratamiento ha sido consentido.

El artículo 6.1 a) del RGPD presume lícito todo tratamiento cuando: "*a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos".*

Ahora bien,el artículo 7 del RGPD regula los requisitos que deben concurrir para considerar válidamente otorgado el consentimiento. El apartado primero señala: "*1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales".*

En relación con lo indicado, el apartado 4, del artículo 7, presume cuándo el consentimiento se prestó libremente: "*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."*

Por otro lado, se considera un aspecto esencial la formalidad del consentimiento (art. 7.2 del RGPD):

> *"2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento".*

El Considerando 42 *in fine,* indica sobre el consentimiento:"*De acuerdo con la Directiva 93/13/CEE del Consejo (10), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los*

fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".

Otro aspecto fundamental de la eficacia del consentimiento es poder retirarlo en cualquier momento. No obstante, la retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada, debiendo tener el interesado conocimiento antes de dar su consentimiento (art. 7.3 del RGPD).

Una novedad del RGPD es la regulación del consentimiento por los menores (art. 8 del RGPD). En este caso, la presunción de licitud del tratamiento concurrirá cuando se haya consentido para uno o varios fines específicos, por un menor de 16 años, y si el menor tiene una edad inferior, será necesaria la autorización de la persona que ejerza la patria potestad o la tutela y en los términos que sea concedida.

Ahora bien, los Estados pueden establecer otra edad, siempre que no sea inferior a los 13 años[18].

La problemática que se deriva de esa previsión recae en el responsable del tratamiento quiendeberá realizar"*esfuerzos razonables*" con la tecnología disponible, para verificar que la autorización procede de la persona que ejerza la patria potestad o tutela (art. 8.3 del RGPD).

En segundo lugar, se examina el interés legítimo, segunda base legitimadora para tratar lícitamente los datos.

El Considerando 47 del RGPD reconoce como base legitimadora el "interés legítimo", limitando su eficacia a que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable.

El interés legítimo podría darse, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que aquél es cliente o está

[18]La "Loi nº 2018-493, du 20 de juin 2018 relative à laprotection des donnéespersonnelles", ha establecido en Francia la edad de consentimiento de los menores en 15 años, si bien esos menores necesitarán también, el consentimiento de los padres. A su vez, la Ley modifica el Código de la Educación, para añadir a la formación sobre los derechos y deberes del uso de Internet y de las redes sociales que se imparte en las escuelas, las reglas sobre la protección de datos personales.

al servicio del segundo. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin.

En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento, cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones.

El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate, y el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse, igualmente, realizado por interés legítimo.

Pues bien, las letras b) a f) del artículo 6.1 del RGPD, enumeran los supuestos en los que se presume que concurre el interés legítimo para el tratamiento:

1.- Sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales*;*

2.- Cuando se requiere para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

3.- Protege intereses vitales del interesado o de otra persona física;

4.- Se cumple una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

5.-Satisface 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.

Asimismo, el apartado segundo del artículo 6 del RGPD se habilita a los Estados a regular con disposiciones nacionales específicas, por un lado, el cumplimiento de la obligación legal del responsable del tratamiento a garantizar el adecuado uso de los datos, y por otro, a respetar el principio de finalidad cuando el tratamiento se realice en el ámbito del interés público, o en el ejercicio de poderes públicos.

Finalmente, hay que tener en cuenta el supuesto en el que no concurra ninguna de las dos bases legitimadoras del tratamiento: no medie consentimiento y se traten los datos para una finalidad distinta a la invocada para su recogida, o no légitima. En este caso, el responsable deberá realizar un juicio de compatibilidad entre los fines originales y los actuales (art. 6.4 del RGPD).

No obstante, el juicio de compatibilidad no será necesario si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros, y constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, de manera que el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines (Considerando 50 del RGPD)[19].

A continuación, se exponen en primer lugar, los derechos del interesado, para controlar sus datos en un escenario comercial transfronterizo e internacional, y en segundo lugar, las correlativas obligaciones para las empresas que tratan los datos.

3. ÁMBITO SUBJETIVO, MATERIAL Y TERRITORIAL DEL RGPD

Con carácter previo al examen del régimen previsto en el RGPD cabe delimitar el ámbito subjetivo, el objetivo y el territorial del RGPD.

[19]El Considerando 50 del RGPD señala: "Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista"

Desde el punto de vista subjetivo, el RGPD persigue la protección de las personas físicas respecto al tratamiento de sus datos y la libre circulación de estos por la Unión Europea (art. 1 del RGPD), por tanto, las garantías se extienden, únicamente, a las personas físicas, con independencia de su nacionalidad y lugar de residencia, y se excluyen a las personas jurídicas y a los fallecidos. Las personas físicas pueden estar identificadas, o ser identificables, destacando al respecto la nueva figura de la seudonimización[20].

La seudonimización se define en el artículo 4 del RGPD como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*". [21]

No obstante, la protección prevista para las personas físicas no es absoluta. Un aspecto esencial en la configuración de los derechos europeos para proteger los datos personales, es el respeto al principio de libre circulación, seña de identidad de la Unión Europea, y que hasta ahora sólo se había aplicado a las personas y a las mercancías.

El apartado 3 del artículo 1 del RGPD señala expresamente:

> *"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*."

El principio de libre circulación de datos se encuentra incorporado en determinadas normas europeas para garantizar la seguridad nacional e internacional, por ejemplo, en la Directiva 2016/681, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR), para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo

[20]Se elimina la posibilidad de los datos anónimos que contemplaba la Directiva 95/46/CE.

[21] El Considerando 29 propone:"Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas."

y de delincuencia grave[22]. Precisamente, en sintonía con esta directiva, el artículo 2.2 d) del RGPD excluye su ámbito de aplicación, al tratamiento de datos por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Por otro lado, el ámbito objetivo de aplicación del RGPD se configura con la definición de datos personales y de su tratamiento.

Los datos personales son definidos en el artículo 4 del RGPD del siguiente modo: "*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*".

Hay que añadir las denominadas "*categorías especiales de datos*" reguladas en el artículo 9 del 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 la orientación sexual de una persona física.

Estos datos no podrán ser tratados con carácter general, salvo en los supuestos previstos en el artículo 9.2 del RGPD: exista consentimiento del interesado; los hizo públicos; son necesarios para el cumplimiento del derecho laboral y protección social; por razones de seguridad sanitaria por movimientos transfronterizos; en el ámbito de procedimientos judiciales y la omnipresente finalidad de archivo para el interés público, para fines de investigación científica o histórica o fines estadísticos, prevista en el artículo 89.1 del RGPD.

---

[22] La Directiva 2016/681 tiene por objeto (art. 1): "a) la transferencia por las compañías aéreas de datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE;b) el tratamiento de los datos a que se refiere la letra a), incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros."

A su vez el artículo 2.1 del RGPD se dedica al tratamiento, considerando como tal: el *"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."*

No obstante, el tratamiento de los datos estará excluido del régimen del RGPD cuando afecten: a la seguridad nacional; la seguridad de la Unión Europea; las actividades de política exterior, nacional o europea, así como las actividades exclusivamente personales o domésticas[23] (art. 2.2. del RGPD).

La premisa que fundamenta todo tratamiento, o actuación relacionada con el mismo es el principio de transparencia (art. 12 del RGPD), cuyas manifestaciones fundamentales son:

- Facilitar al interesado toda información que le solicite en virtud de dos derechos básicos de información (art. 13 del RGPD), y del derecho de acceso (art. 15) que comprende, en esencia, la información sobre el fin al que se destinan sus datos.
- Comunicarse con el interesado dando respuesta a las peticiones de éste según los derechos de olvido, de rectificación, de portabilidad o de oposición al tratamiento (artículos 15 a 22 del RGPD).
- La comunicación concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada con carácter general, por escrito o por otros medios, inclusive, si procede, por medios electrónicos.
- Supuesto excepcional: si el responsable puede demostrar que no está en condiciones de identificar al interesado, no se aplicarán los artículos 15 a 20 del RGPD, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

[23]El Considerando 18 del RGPD define las actividades domésticas:"*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*."

- El plazo para dar respuesta a las solicitudes derivadas de los artículos 15 a 22 del RGPD, será de un mes, prorrogable a dos meses, previo aviso al interesado.

Por último, el ámbito territorial de aplicación del RGPD se contempla en el artículo 3 del RGPD y se delimita del siguiente modo:

1º.- El establecimiento responsable o del encargado del tratamiento se encuentre en un país de la Unión Europea (art. 3.1): "*El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*"

2º.- Cuando el interesado esté en la Unión Europea (art. 3.2): *"El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*

> *a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o*
>
> *b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.*"

3º.- El responsable del tratamiento esté en un tercer país al que le es aplicable el Derecho nacional del país europeo, por las reglas del derecho internacional.

El RGPD ha optado por dos elementos para determinar su ámbito territorial, la ubicación del interesado y la realización del tratamiento, sin tener en cuenta aspectos como el domicilio social de la empresa, o si el tratamiento de datos se realiza por una filial o por la matriz.

A continuación, procede el análisis de los actuales derechos de los ciudadanos para controlar el tratamiento de sus datos, que, básicamente, son similares a los que preveía la Directiva 95/46/CE.

4. LA PROTECCIÓN DE DATOS. DERECHOS DEL INTERESADO. MENCIÓN A LAS OBLIGACIONES DE LAS EMPRESAS/ENTIDADES

La protección de datos inicialmente se consideraba una manifestación del derecho a la intimidad. Sin embargo, el desarrollo tecnológico y el ejercicio de actividades económicas transfronterizas, han impulsado una necesaria adaptación legislativa para dar respuesta a la realidad, y ofrecer mayores garantías sobre la recolección, utilización, tratamiento y control de los datos personales.

El RGPD se erige en modelo normativo en la materia, no sólo para los Estados miembros, sino también para terceros países con los que la Unión Europea mantiene relaciones comerciales. Sin embargo, no siempre sirve de inspiración a legisladores extranjeros. Un ejemplo lo encontramos en los Estados Unidos donde se ha aprobado la denominada "Cloud Act"[24]. Esta norma permite a prácticamente toda autoridad policial estadounidense, acceder a los datos que un proveedor de servicios de los Estados Unidos tenga almacenados en otro país, cuando afecte a un ciudadano estadounidense y el proveedor sea requerido a través de una citación judicial[25].

En el ámbito europeo, los derechos de los ciudadanos para garantizar la protección de sus datos personales se contienen en los artículos 14 a 20 del RGPD[26].

En primer lugar se aborda el derecho del interesado a solicitar información al responsable del tratamiento (art. 13).

El fundamento de este derecho es garantizar la transparencia en el uso de los datos de los particulares,con esa finalidad el responsable del tratamiento debe facilitar una

[24] Clarifying Lawful Overseas Use of Data Act.

[25] Esta norma pretende resolver legislativamente la situación generadapor el Caso Warrant, o "Microsoft Ireland case": Microsoft se negó a entregar los datos que le requería la fiscalía de Nueva York sobre el Sr. Warrant, ciudadano americano
No obstante, el Estado de California ha aprobado la "California Consumer Privacy Act of 2018" (entrará en vigor en 2020.) Su ámbito de aplicación se limita a las personas físicas residentes en el estado californiano, sin embargo, dado que empresas como Google, Facebook, Amazon o Microsoft tienen sede en dicho estado, el conflicto entre los dos ámbitos de protección de la privacidad de los ciudadanos estadounidenses, el que crea su norma estatal y el generado por su ley nacional, está asegurado.

[26]Algunas de las adaptaciones normativas nacionales internas al RGPD se han producido en el Reino Unido, con la "Data Protection Act" de 21 de mayo de 2018 y en Francia, con la citada Loi nº 2018-493, du 20 de juin 2018 relative à laprotection des données personnelles, que además traspone la Directiva 2016/680 del PE y del Consejo, de 27 de abril, relativa a la protección de las personas físicas en los que respecta al tratamiento de datos personales por parte de autoridades componentes para fines de prevención, investigación, detección o enjuiciamiento penales.

información determinada en el momento previo a la recogida de datos, y otra, en el momento de su obtención.

La información previa que se debe facilitar antes de obtener los datos del interesado afecta a los siguientes aspectos:

1.- La identidad y los datos de contacto del responsable y, en su caso, de su representante.

2.- Los datos de contacto del delegado de protección de datos, si se hubiera designado.

3.- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.

4.- Cuando el tratamiento se base en el artículo 6.1 f), los intereses legítimos del responsable o de un tercero, es decir, cuando el tratamiento sea 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.

No obstante, no será de aplicación cuando el tratamiento sea realizado por las autoridades públicas en el ejercicio de sus funciones.

5.- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.

6.- En su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional, y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47, o el artículo 49.1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado

Por otro lado, la información que el responsable ofrecerá tras haber obtenido los datos será:

1.- El plazo para conservar los datos personales, o en su defecto, los criterios para precisar ese plazo.

2.- El derecho de acceso que asiste al sujeto para comprobar los datos, rectificarlos o suprimirlos, la limitación de su tratamiento, oponerse a que sean tratados o su portabilidad.

3.- La posibilidad de retirar el consentimiento en los siguientes supuestos:

- Cuando el interesado dio su consentimiento para el tratamiento de sus datos personales para unos fines específicos (art. 6.1 a) del RGPD).

- Cuando tratándose de datos de categoría especial, el interesado dio su consentimiento explícito para un fin específico (art. 9.2 a) del RGPD).

4.- El derecho a presentar una reclamación ante una autoridad de control.

5.- La comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

6.- La existencia de decisiones automatizas, incluida la elaboración de perfiles, previstos en el artículo 22.1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En virtud de este último apartado, por ejemplo, los bancos pueden articular medios técnicos que permitan la concesión de hipotecas de forma automatizada.

El artículo 13.4 del RGPD exime del deber de información al responsable, cuando el interesado dispusiera de aquélla anteriormente.

En segundo lugar, el RGPD regula el derecho de acceso (art. 15 del RGPD). Esta facultad incluye tanto conocer si los datos están siendo utilizados para los fines que fueron recabados, como:

- Las categorías de datos personales de que se trate;

- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- 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, a que se refiere el artículo 22,.1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

El acceso a esa información se realiza mediante copia en formato electrónico de uso común, y podrá cobrarse un precio por obtenerla siempre que sea razonable y estén justificados los costes administrativos.

En tercer lugar, el interesado dispone del derecho de rectificación de datos inexactos o que se completen aquéllos que no lo estén (art. 16 del RGPD).

En cuarto lugar, se analiza el llamado derecho al olvido (art. 17 del RGPD). El derecho de supresión representa la posibilidad para el interesado de solicitar al responsable del tratamiento, que elimine sus datos cuando estos:

a) No son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) El interesado retira el consentimiento en que se basa el tratamiento, de conformidad con el artículo 6.1 a), o el artículo 9. 2 a), y éste no se base en otro fundamento jurídico;

c) El interesado se oponga al tratamiento con arreglo al artículo 21.1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21.2 del RGPD;

d) Hayan sido tratados ilícitamente;

e) Deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable;

f) Se hayan obtenido en relación con la oferta de servicios de la sociedad de la información, mencionados en el artículo 8.1 del RGPD.[27]

El derecho al olvido presenta dificultades burocráticas para el interesado exigiéndole identificar el responsable del borrado. El artículo 17 del RGPD atribuye esa obligación con carácter general, al responsable del tratamiento, por ser quien publica los datos. El cumplimiento de ese deber conlleva adoptar las medidas razonables dentro de la tecnología disponible y los costes, para que los responsables que en ese momento estén tratando esos datos, conozcan la solicitud del interesado de supresión de cualquier enlace a esos datos personales.

En España, la Agencia Española de Protección de Datos (en adelante, AEPD) ha defendido que el cumplimiento corresponde a los buscadores informáticos, por ser quienes posibilitan el acceso a las webs master. Esta postura fue refrendada por la STJUE de 13 de mayo de 2014, Sr. Costeja contra Google[28].

Sin embargo, la STC 58/2018, de 4 de junio, extiende el derecho de olvido a los "buscadores internos" de las páginas integrantes de la hemeroteca digital, que declara inalterable.

A su vez, el TJUE ha decidido que a partir del 1 de julio de 2018, se sustituya en todas las cuestiones prejudiciales, el nombre de las personas físicas implicadas por sus iniciales y se suprimirá cualquier dato adicional que permitiera identificarlas[29].

[27]El artículo 8 se dedica a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.
[28] Asunto C- 131/2012.
[29]https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180096es.pdf

No obstante, el derecho al olvido no es un derecho absoluto. Por un lado, la Sentencia del TEDH de 28 de junio de 2018[30], concluye que, en todo caso, debe ser ponderado según las circunstancias: la Sentencia niega a dos ciudadanos alemanes condenados en 1993 por el asesinato de una persona conocida, a desvincular su nombre de ciertas noticias en tres medios germanos.[31]

Por otro, el apartado tercero del artículo 17 del RGPD regula las excepciones que limitan su ejercicio fundadas, esencialmente, en considerar que el tratamiento sea necesario[32].

Los tres últimos derechos de los interesados son :la limitación del tratamiento (art. 18); la portabilidad de datos (art. 20), y el derecho de oposición (art. 21).

El interesado puede solicitar al responsable del tratamiento que limite éste cuando (art. 18): el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; 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; 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 y, finalmente, si el interesado se ha opuesto al tratamiento en virtud del artículo 21.1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

[30] Affaire M.L. et W.W. vs. Alemania.

[31] La negativa de la STEDH se funda en los siguientes hechos: los solicitantes volvieron a hacer público su caso y reclamaron atención en 2004, de forma que se considera que son personas conocidas y públicas en parte por voluntad propia; la información periodística es parcialmente de pago, no siendo directo el acceso a la misma; la reclamación se dirigió contra el medio, no contra el buscador. La sentencia distingue- como lo hizo la STJUE de 13 de mayo de 2014, Asunto Costeja-, entre el efecto multiplicador del buscador frente al del medio. Previsiblemente la STEDH hubiera sido diferente si se hubiera reclamado contra los motores de búsqueda.

[32]No se suprimirán los datos personales en los siguientes casos (art. 17.3 del RGPD):a) para ejercer el derecho a la libertad de expresión e información;b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89.1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento; e) para la formulación, el ejercicio o la defensa de reclamaciones.

En este supuesto relativo a la limitación del tratamiento, los datos sólo podrán ser objeto de conservación cuando exista consentimiento del interesado, se vayan a formular reclamaciones, sean necesarios para 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.

El derecho de portabilidad de los datos[33] (art. 20) se configura como la posibilidad que tiene un interesado de solicitar al responsable del tratamiento, que le sean "entregados" sus datos personales, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado inicialmente, cuando:a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6.1 a), o el artículo 9. 2 a), o en un contrato con arreglo al artículo 6.1, b), y el tratamiento se efectúe por medios automatizados.

Por último, el derecho de oposición (art. 21 del RGPD) merece especial mención. El interesado puede oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6.1, e) o f)[34], incluida la elaboración de perfiles.

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento, que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Asimismo, cuando el tratamiento de datos se dirija a la mercadotecnia directa, el interesado podrá oponerse en cualquier momento, incluida la elaboración de perfiles en la medida en que esté relacionada con aquélla[35]. Una especialidad del derecho de

[33]Considerando 68 del RGPD: se incentiva a los responsables del tratamiento a crear formatos interoperables que permitan la portabilidad de datos.

[34]El art. 6.1 indica que el tratamiento es necesario cuando: e) para cumplir una misión de interés público o para el ejercicio de poderes públicos del responsable del tratamiento,o f) para la satisfacción de intereses legítimos del responsable del tratamiento o de un tercero.

[35]Los perfiles son definidos en el artículo 4 del RGPD: "*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,*

oposición relacionada con el ámbito de los perfiles es objeto de previsión en el artículo 22 del RGPD, donde se reconoce al interesado, el 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.[36]

A su vez, cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos previstos en el artículo 89.1 del RGPD, el interesado también 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 por razones de interés público.

No obstante, el ejercicio de los derechos de los interesados examinados puede ser limitado por el responsable del tratamiento, cuando la base jurídica esté prevista en la normativa europea o nacional, y concurra alguno de los motivos del artículo 23 del RGPD, que podrían agruparse del siguiente modo:

1º.- Causas relativas a la seguridad y defensa del Estado, la seguridad pública; la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

2º.- Causas fundadas en el interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

3º.- Causas relacionas con el ámbito judicial y su independencia, o la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas, o la ejecución de demandas civiles.

---

situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

[36]No obstante, una vez más vía excepciones, se limita el derecho de oposición al tratamiento automatizado de los datos cuando se considere necesario para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; 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 se base en el consentimiento explícito del interesado (art. 22.2 del RGPD)

4º.- Otras causas: la inspección, supervisión o reglamentación en el ejercicio de autoridades públicas, en alguno de los supuestos anteriormente mencionado o la protección de los derechos de otro.

A lo indicado hay que añadir las excepciones para la obligación del responsable del tratamiento, de comunicar las violaciones de la seguridad de los datos personales al interesado (art. 34 del 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;*
>
> *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."*

En definitiva, el RGPD si bien articula un amplio número de derechos para facilitar a los interesados la protección del uso de sus datos, la realidad es que a través de la vía de las excepciones, son objeto de relevantes matizaciones con el fin de congeniar la protección de datos personales y su libre circulación.

Examinados los derechos de los ciudadanos y las restricciones de su ejercicio, procede abordar las obligaciones de las empresas o entidades para adaptarse a las exigencias normativas europeas.

A pesar de todas las obligaciones previstas para garantizar en la medida de lo posible, la privacidad de los datos de los ciudadanos, la gestión de las bases de datos (los "Big Data"), se ha convertido en una relevante materia prima de la economía actual.

La premisa fundamental es que deben tratar los datos de manera lícita: el tratamiento debe estar fundado con carácter general en el consentimiento del interesado, o en el interés legítimo (art. 6 del RGPD).

Asimismo, deben responder a las solicitudes de los particulares sin dilación indebida, y en todo caso, en el plazo de un mes a partir de la recepción de la solicitud, salvo que se trate de solicitudes complejas que tiene hasta dos meses, informando de la prórroga al interesado. Las peticiones se tramitarán de forma gratuita con carácter general, si bien cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o negarse a actuar respecto de la solicitud. En el caso de rechazar la solicitud, debe ser de forma motivada e informar de su derecho a presentar reclamación ante la AEPD (art. 12.3 y 5 del RGPD).

Además, están obligados a informar al interesado del tratamiento de datos y sus fines (art. 13 y 15 del RGPD).

La consecuencia directa de la adaptación es que conforme señala el Considerando 59, la entidad debe contar con medios adecuados para que los interesados puedan ejercitar, en su caso, los derechos de rectificación, supresión, limitación del tratamiento, portabilidad o de oposición del tratamiento regulados respectivamente, en los artículos 16, 17, 18, 20 y 21 del RGPD.

Otro aspecto esencial en la configuración del tratamiento es su protección, entendiendo ésta desde un punto de vista integral, desde el diseño, es decir, desde la planificación del tratamiento, y que a su vez, contemple la protección por defecto, de manera que la empresa u organización siempre configure los parámetros por defecto de la forma más respetuosa con la privacidad (art. 25 del RGPD).

Como respuesta a la posibilidad de que sobre los mismos datos intervengan responsables y encargados del tratamiento, se prevé el instrumento jurídico para regular sus respectivas responsabilidades, el contrato del tratamiento (art. 28.3 del RGPD), donde se estipularán las obligaciones respectivas para la protección de los datos.

Una cuestión fundamental en el RGPD es la adopción de medidas adecuadas por las empresas u organizaciones que permitan demostrar el cumplimiento de la normativa (considerando 77 del RGPD). Al efecto, se habilitan opciones que les faciliten esa obligación: la adhesión, bien, a códigos de conducta aprobados a tenor del artículo 40, o

bien, a un mecanismo de certificación aprobado a tenor del artículo 42 que podrán ser utilizados como elementos para demostrar el cumplimiento (art. 24.3 del RGPD).

A todo lo indicado se añade que los responsables del tratamiento o sus representantes, deben llevar el registro de actividad (art. 30 del RGPD), donde existirá un control de las actividades de tratamiento efectuadas bajo su responsabilidad.

Para finalizar la referencia a las obligaciones empresariales en materia de protección de datos, es necesario reseñar los sistemas de seguridad para garantizar el adecuado tratamiento de los datos (art. 32 a 43 del RGDP), que serán objeto de examen detenido en el punto sexto del artículo:

- La evaluación de impacto de la protección de datos (art. 35 del RGPD).

- La consulta previa a la autoridad de control antes de proceder al tratamiento, siempre y cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo, sin haber tomado el responsable las medidas para mitigarlo (art. 36 del RGD).

- La designación de un delegado de protección de datos (art. 37 del RGPD).

5. TRANSFERENCIAS DEDATOS

La transferencia de datos se ha convertido en un elemento fundamental de la economía de libre comercio. La normativa europea ha pretendido aunar los intereses comerciales, generadores de riqueza y empleo, con la mayor exposición de la intimidad personal que el nuevo sistema económico conlleva.

La Directiva 95/46 se limitaba a prohibir la transferencia de datos a países que no garantizaran el mismo nivel de protección que se establecía en la Unión Europea.

El RGPD perfila de forma más detallada todo lo concerniente a la transferencia de datos. En primer lugar, el artículo 4 circunscribe la "transferencia transfronteriza", al tratamiento de datos realizado sólo entre Estados miembros de la Unión Europea y la define como:

"a) El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un

encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) El tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro".

Por otro lado, la posibilidad de realizar transferencias a terceros países u organizaciones internacionales, se condiciona a que el responsable y el encargado del tratamiento cumplan las obligaciones de seguridad, así como respeten los códigos de conducta, y realicen las evaluaciones de impacto y consulta previa, contenidas en el Capítulo IV del RGPD, incluyendo las obligaciones que afecten a las transferencias ulteriores de datos personales desde el tercer país u organización internacional, a otro tercer país u organización internacional(art. 44 del RGPD).

Las transferencias a terceros países se dividen en dos grupos: transferencias basadas en una decisión adecuada (art. 45), y transferencias mediante garantías adecuadas (art. 46).

En el primer tipo de tratamiento de datos, -transferencias basadas en una decisión adecuada-, la Comisión Europea decide que el destinatario (tercer país, territorio, o sector del mismo u organización internacional), cumple con los estándares de protección adecuados, y por tanto, no es necesaria autorización previa para la transferencia[37].

Anualmente, la Comisión publica la lista de países que cumplen los requisitos, entre los que en ocasiones, no se encuentran todos los países occidentales.[38]

[37]Los criterios que tendrá en cuenta la Comisión para tomar la decisión serán: el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales; la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional; los compromisos internacionales asumidos por el tercer país u organización internacional (art. 45.2 del RGPD).

[38]https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

El acto decisorio de la Comisión respecto el tercer país será revisable cada cuatro años (art. 45.3 del RPD), y aquélla supervisará de forma continuada los actos de aplicación de su decisión (art. 45.4 del RGPD).

El segundo tipo de transferencia – transferencia mediante garantías adecuadas-, opera de forma subsidiaria a la anterior, sólo cuando la Comisión no haya adoptado la decisión favorable, el tratamiento de los datos podrá realizarse cuando el tercer país o la organización internacional, observen dos aspectos: ofrecer garantías adecuadas del tratamiento, y los interesados cuenten con derechos exigibles y acciones legales efectivas (art. 46.1 del RGPD).[39]

El RGPD ha recogido un mecanismo que permite mantener las actividades comerciales con los terceros países que no alcanzan el nivel de protección adecuado, se trata de las llamadas normas vinculantes (art. 47 del RGPD). Son aprobadas por la autoridad de control y deben contener como mínimo los siguientes aspectos:

> *"a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;*
>
> *b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;*
>
> *c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;*
>
> *d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;*

[39] La enumeración de posibles instrumentos donde ofrecer esas garantías se encuentra en los apartados segundo y tercero del artículo 46 del RGPD.

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta;

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, y

n) la formación en protección de datos pertinente para el personal.

A lo indicado se añade una particularidad. Cuando se trate de transferencias no autorizadas por el derecho europeo, que son reclamadas por sentencias o decisiones de autoridades administrativas de un tercer país. En este caso, el responsable o el encargado, transferirá los datos cuando aquéllas sean reconocidas o ejecutables en virtud de un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro(art. 48 del RGPD).

A pesar de todo lo regulado, una vez más hay que hacerse eco de las excepciones para realizar este tipo de transferencias reguladas en el artículo 49 del RGPD, se trata de las denominadas "excepciones por cuestiones específicas", y permiten la transferencia de datos a terceros países aunque no se cumpla lo indicado anteriormente.

Las excepciones concurren en los siguientes supuestos:

1.- 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;

2.- 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;

3.- 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;

4.- La transferencia sea necesaria por razones importantes de interés público;

5.- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

6.- 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;

7.-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.

A su vez, el artículo 49 del RGPD prevé una cláusula residual que habilita una transferencia de datos, aun cuando no pueda basarse en las disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y además, no sea aplicable ninguna de las excepciones mencionadas.

Los requisitos para permitir ese tipo de transferencias son las siguientes: no debe ser repetitiva, afectar solo a un número limitado de interesados, ser 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 (art. 49.1 *in fine*).

Por último,el funcionamiento de la transferencia de datos, en todo caso, se llevará a cabo fundada en el principio de cooperación internacional (artículo 50 del RGPD).

6. RESPONSABILIDAD DE LOS DATOS. SEGURIDAD.

Las obligaciones en materia de seguridad por las entidades u organizaciones se articulan inspiradas en el principio de responsabilidad activa.

Las figuras de responsable y de encargado del tratamiento son definidas en el artículo 4 del RGPD:

- El 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;
- El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas y proporcionadas, como pueden ser la seudonimización, o la minimización de datos para garantizar y demostrar que, tanto en el momento de determinar los medios del tratamiento de datos, la denominada protección de datos desde el diseño, como durante el tratamiento en sí, aquéllas son ajustadas al Reglamento (art. 24 y 25 del RGPD).[40] A su vez, deberá realizar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad y deberá contener toda la información necesaria para identificarlos (art. 30 del RGPD).

Además, el responsable será quien informe tanto a la autoridad de control (art. 33), como al interesado cuando se haya producido una violación de sus datos personales (art. 34), y es el competente para llevar a cabo dos actuaciones novedosas incorporadas en el artículo 35 del Reglamento: la evaluación de impacto de datos personales y la consulta previa.

La evaluación de impacto se trata de un análisis previo al tratamiento de ciertos datos personales cuando se considere 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. En el caso de que exista delegado

[40]Los responsables del tratamiento deben llevar un registro de actividad del tratamiento (art. 30 del RGPD).

de protección, podrá colaborar en la realización de la evaluación.[41] La Evaluación deberá contener:

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 que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Por otro lado, la consulta previa será realizada en su caso, por el responsable 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 (art. 36 del RGPD).

Respecto las obligaciones del encargado del tratamiento, que será elegido por el responsable, se centran en la aplicación de medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con el RGPD. El tratamiento por el encargado se regirá por un contrato u otro negocio jurídico previsto en el derecho europeo y contendrá el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del

[41] Los supuestos para los que será necesario la Evaluación de Impacto son: 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; tratamiento a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales y observación sistemática a gran escala de una zona de acceso público (art. 35.3 del RGPD). En todo caso, la autoridad de control publicará una lista de las actuaciones que requerirán evaluación de impacto (art. 35.4 del RGPD).

responsable (art. 28 del RGPD). El acceso a los datos estará supeditado, en todo caso, a las instrucciones del responsable (art. 29 del RGPD).

Se presumirá que el responsable y el encargado realizan un tratamiento adecuado de los datos cuando se hayan adherido a códigos de conducta, aprobados siguiendo lo previsto en el artículo 40 del RGPD, o estén vinculados a un mecanismo de certificación aprobado conforme regula el artículo 42 del RGPD (art. 24.3 y 28.5 del RGPD).

En todo caso, será obligación tanto del responsable como del encargado, y en su caso de sus representantes[42], cooperar con la autoridad de control cuando se les solicite (art. 31 del RGPD).

Asimismo, ambas figuras deben garantizar la seguridad del tratamiento fomentando la adhesión a los códigos de conducta, (artículos 40), y a los mecanismos de certificaciones (42 del RGPD)[43].

Finalmente, destaca en el RGPD la figura del Delegado de Protección de Datos (art. 37 a 39) designado por el responsable o el encargado del tratamiento cuando:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de

[42] Una novedad del RGPD es la creación de los representantes de los responsables o encargados. Es una figura que se define en el art. 4, apartado 17 del RGPD: "*persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento*." El artículo 27 del RGPD exige que el nombramiento sea por escrito por parte del responsable o del encargado, salvo que el tratamiento sea ocasional o se trate de autoridades públicas. No obstante, es imprescindible que el representante se encuentre en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado, y en todo caso, la existencia de representante no afecta a las acciones que los afectados puedan dirigir contra los responsables o encargados.

[43] El Reglamento 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio, regula los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos.

datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Las funciones mínimas de esta figura se delimitan en el artículo 39 del RGPD:

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.

7.-AUTORIDADES Y ÓRGANOS DE CONTROL

La relevancia otorgada a las autoridades de control en la normativa europea vigente, conlleva un examen detenido de estas figuras.

Hay que distinguir entre los órganos del Consejo de Europa, y los de la Unión Europea.

Respecto los órganos derivados del Consejo de Europa, hay dos órganos que se dedican a la protección de derechos fundamentales en general, son el Tribunal Europeo de Derechos Humanos (TEDH)[44] y el Comisario de Derechos Humanos[45], y otros dos órganos especializados en la materia de protección de datos: el Comité de Expertos y el Comité Consultivo.

El Comité de Expertos en Protección de Datos fue creado en 1976 y se dedica a la elaboración de recomendaciones e informes en aspectos concretos en el sector. Por su parte, el Comité Consultivo creado por el Convenio 108 (1981) está formado por un representante de cada Estado que ha ratificado el citado Convenio. Su objeto es mejorar la aplicación de la Convención 108, en especial en el ámbito de la protección de datos. No obstante, hay que señalar que la proliferación de instituciones europeas en la materia han desplazado en cierto modo a estos dos órganos, si bien hay que tener en cuenta que el encontrarse ajenos a la dinámica institucional europea, les dota de mayor objetividad, sobre todo, en la adopción de iniciativas de actuaciones o de regulación.

En la Unión Europea existe a su vez una variedad de órganos legitimados para pronunciarse en materia de protección de datos:

- El Tribunal de Justicia de la Unión Europea (TJUE)[46].
- Agencia de los Derechos Fundamentales de la Unión Europea[47].
- El Comité Europeo de Protección de Datos.
- Supervisor Europeo de Protección de Datos.
- Las Autoridades de control para cada Estado miembro.

Nos centramos en los tres últimos órganos, por la especialidad en el sector.

El Comité Europeo de Protección de Datos es creado por el RGPD (art. 70)[48], siendo destacable que puede actuar por iniciativa propia, o por solicitud de la Comisión. El ámbito de actuación es muy amplio y fundamentalmente estará legitimado para supervisar y garantizar la aplicación del RGPD, cuando las autoridades de control hayan informado de su intención de adoptar determinadas medidas en materia de protección de

[44] Se creó en el Convenio Europeo de Derechos Humanos (1950)
[45]Se creó por Resolución (99) 50 del Comité de Ministros, aprobada el 7 de mayo de 1999.
[46]Formado por 27 jueces y 8 Abogado Generales, designados de mutuo acuerdo por los Estados miembros.
[47] Creada por Reglamento nº 168/2007 del Consejo, de 15 de febrero de 2007.
[48]El CEPD sustituye a los órganos previstos por la derogada Directiva 95/46/CE

datos, propuestas por autoridades de control (artículos 64 y 65 del RGPD), como por ejemplo, determinar las cláusulas contractuales para una transferencia mediante las garantías adecuadas a terceros países.

Asimismo, tiene reconocidas amplias facultades en materia de asesoramiento a la Comisión sobre los aspectos de la protección de datos, incluidas las propuestas para la aplicación adecuada del RGPD, o su modificación; emitirá directrices y recomendaciones en relación con los procedimientos para garantizar las distintas transferencias de datos, protocolos de actuación en el caso de violación de la seguridad de los datos; fomentará la creación de los códigos de conducta y establecimientos de certificación, así como de los criterios que deben seguir, para la protección de datos, sellos y marcas al respecto.

Además, tiene asignadas facultades relacionales con autoridades de control, formativas, de asesoramiento sobre los códigos de conducta, de promoción dela cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control; y llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

Por su parte, el Supervisor Europeo de Protección de Datos [49] forma parte del Comité Europeo de Protección de Datos, junto con los representantes de las autoridades de control de los Estados miembros, y en concreto, ejerce las funciones de la Secretaría del Comité.

A continuación, se examinan las autoridades de control, se consideran tales las autoridades públicas independientes creadas por los Estados miembros (artículo 4, apartado 21 del RGPD).[50]

[49]Previsto en el art. 286 del TCE incluido por el Tratado de Ámsterdam (1997). Lo regulan el Reglamento nº 45/2001, 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 organismos comunitarios y a la libre circulación de datos, y la Decisión nº 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio.

[50]El artículo 51 del RGPD señala: Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante, autoridad de control), supervisar la aplicación del Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

Sus funciones se regulan en el artículo 57 del RGPD, y entre otras, destacan: a) controlar la aplicación del Reglamento y hacerlo aplicar; b) promover la sensibilización de los responsables y encargados del tratamiento y del público y su comprensión de los riesgos, normas, garantías y derechos con especial

Por otro lado, las autoridades de control se consideran "interesadas" (artículo 4, apartado 22 del RGPD) cuando le 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 España opera la AEPD y sus facultades, como para el resto de autoridades de control en la Unión Europea, están definidas en el artículo 58 del RGPD:

"*a) Ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;*

b) Llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) Llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) Notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) Obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

atención a los niños; c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; d) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros; f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control.

f) Obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros."

En el caso de concurrencia de autoridades de control sobre un tratamiento de datos, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento, será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado (art. 56 del RGPD). No obstante, una vez la excepcionalidad opera, el artículo 56.2 habilita a que cada autoridad de control conozca de una reclamación que le sea presentada o una posible infracción del Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro, o únicamente afecte de manera sustancial a interesados en su Estado miembro.

En todo caso, las autoridades de control de los Estados miembros, quedan sujetas a actuar respetando los principios de asistencia mutua, cooperación y de coordinación (art. 61, 63 y 64.2 del RGPD).

8. RÉGIMEN DE INFRACCIONES Y SANCIONES

Los recursos en materia de protección de datos, la exigencia de responsabilidad y las posibles sanciones se regulan en el Capítulo VIII del RGPD (art. 77 a 84).

Las acciones fundamentales reconocidas a los interesados son tres:

1.- Presentar una reclamación ante una autoridad de control (art. 77 del RGPD): sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales vulnera la normativa europea.

2.- Ejercicio de la tutela judicial efectiva contra una autoridad de control (art. 78 del RGPD): sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica, tendrá derecho a la tutela judicial efectiva contra decisiones jurídicamente vinculantes de autoridades de control que le conciernan.

3.- Ejercer acciones legales contra un responsable o encargado del tratamiento (art. 79 del RGPD): sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

Una novedad relevante en el ejercicio de las acciones previstas a favor de los interesados para la defensa del tratamiento de sus datos, es la figura del representante. El artículo 80 del RGPD contempla la posibilidad de conceder un mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82, si así lo establece el derecho del Estado miembro.

Si bien el RGPD, a diferencia de la normativa estadounidense, no contempla expresamente la opción para las empresas a prestar un servicio "bajo coste" para eliminar o rectificar los datos de los interesados previa su solicitud, pero sí admite la intervención de las entidades u organizaciones sin ánimo de lucro, para reclamar indemnizaciones por vulneraciones del derecho europeo, lo que representa otra vertiente de la economía del dato.

El derecho de indemnización se regula en el artículo 82 del RGPD donde se indica: si un interesado considera que el incumplimiento del RGPD le ha ocasionado un daño material o inmaterial, podrá reclamar una compensación al responsable, o en su caso al encargado del tratamiento.

La responsabilidad por el daño derivado del incumplimiento de las previsiones del Reglamento, se atribuye al responsable del tratamiento (art. 82.2 del RGPD). El encargado, únicamente, responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones previstas específicamente a los encargados, o haya actuado al margen o en contra de las instrucciones legales del responsable.

Para cerrar el aspecto de respuesta en caso de daño, los artículos 83 y 84 del RGPD regulan las circunstancias para imponer multas y sanciones. No obstante, y sin perjuicio de la temporalidad del R.D- ley 5/2018 que regula algunos aspectos de esa materia, se menciona su contenido, en relación a los correlativos preceptos del proyecto de ley orgánica que se dedican a esas cuestiones.

En el ámbito nacional la materia de infracciones y sanciones y el procedimiento en caso de posible vulneración de la normativa de protección de datos, ha sido objeto de desarrollo como se adelantó en el punto primero, a través del R.D- ley 5/2018, que estará vigente hasta la entrada en vigor de la nueva ley orgánica que adapte el ordenamiento jurídico español al RGPD (disposición final única del R. Decreto-ley 5/2018).

Este texto nacional regula algunos aspectos de la materia sancionadora en materia de protección de datos:

- El artículo 3 determina el ámbito subjetivo al que se aplicará la regulación de protección de datos, (correspondecon el artículo 70 del proyecto de ley orgánica) y destacar que se excluye al delegado de protección de datos del régimen sancionador.
- El artículo 4 remite al artículo 83.4, 5 y 6 del RGPD para la materia de infracciones, (en los mismos términos se pronuncia el artículo 71 del Proyecto);
- La prescripción de las sanciones se contiene en el artículo 6 del R. Decreto –ley 5/2018, (similar el artículo 78 del proyecto de ley orgánica): a) las sanciones por importe igual o inferior a 40.000.-€, prescriben en el plazo de un año; b) las sanciones por importe superior a 40.000.-€ e inferior a 300.000.-€ prescriben a los 2 años, y c) las sanciones con importe superior a 300.000.-€ prescriben a los tres años.

El *dies a quo* del cómputo de los plazos señalados será el día siguiente aquél en que se ejecutable la resolución por la que se impone la sanción o si ha transcurrido el plazo para recurrirla, y sin perjuicio de que se interrumpirá el plazo de prescripción, cuando se inicie el procedimiento de ejecución con conocimiento del interesado, reanudándose el plazo si está paralizado durante más de seis meses por causa no imputable al infractor.

En relación con el procedimiento en caso de posible vulneración de la normativa en la materia, los artículos 7 a 12 del texto normativo vigente, ylos artículos 63 a 69 del

proyecto de ley orgánica, se dedican a este ámbito. El objeto es regular los procedimientos tramitados por la AEPD, cuando un afectado reclame que no ha sido atendida una solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD, así como cuando la Agencia investigue la existencia de una posible infracción contemplada en el RGPD, y en la normativa nacional en el sector.

La AEPD examinará el carácter nacional o transfronterizo del tratamiento a fin de determinar la autoridad de control principal. Si es competente, llevará a cabo actuaciones previas al inicio del procedimiento para realizar la investigación que determine los hechos y circunstancias que justifican la tramitación del aquél, en su caso.

Para finalizar una particularidad temporal destaca eneste régimen transitorio previsto por el R.D.-ley 5/2018.La disposición transitoria segunda indica que el plazo de los contratos del encargado del tratamiento anteriores a la entrada en vigor del RGPD (25 de mayo de 2018), mantendrán su vigencia al amparo del artículo 12 de la L.O. 15/1999, de 13 de diciembre, de Protección de Datos, hasta la fecha de vencimiento y si se estipuló que fuera indefinida hasta el 25 de mayo de 2022.

BIBLIOGRAFÍA

- "El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea". Autores: José Luis Piñar Mañas y Miguel Recio Gayo. Editorial La Ley. Edición, 2018.

- "Protección de datos en Europa. Origen, evolución y regulación actual". Autor: D. Lucrecio Rebollo. EditorialDykinson. Edición 2018.

- “El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal”. Autor: D. Alfonso Ortega Giménez. Editorial Thomson Reuters. Aranzadi. Edición 2017.

- “Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo”, Claves Prácticas.Autor: D. Luis Felipe López Álvarez. Editorial Francis Lefebvre. Edición 2016.

- “Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad”, Director, D. José Luis Piñar Mañas. Editorial Reus, S.A. Edición 2016.