TEMA 7: LA PROTECCIÓN DE DATOS PERSONALES. RÉGIMEN JURÍDICO. EL REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL, 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. PRINCIPIOS Y DERECHOS. OBLIGACIONES.

LEGISLACIÓN

- **Reglamento (UE) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016,** relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- **Ley Orgánica 3/2018, de 5 de Diciembre,** de Protección de Datos Personales y garantía de los derechos digitales

1. LA PROTECCIÓN DE DATOS PERSONALES. RÉGIMEN JURÍDICO

Podemos decir que vivimos en la sociedad de la información, teniendo lugar a diario el tratamiento de millones de datos personales. Así, facilitamos nuestros datos personales cuando abrimos una cuenta en el banco, cuando solicitamos participar en un concurso, cuando reservamos un vuelo o un hotel, cada vez que efectuamos un pago con la tarjeta de crédito o cuando navegamos por Internet.

El nombre y los apellidos, la fecha de nacimiento, la dirección postal o de correo electrónico, el número de teléfono, el DNI, la matrícula del coche y muchos otros datos que usamos a diario constituyen información valiosa que podría permitir identificar a una persona, ya sea directa o indirectamente.

El derecho fundamental a la protección de datos es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y en el Derecho Europeo, que ha estado protegido en nuestro país hasta hace poco por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y actualmente se encuentra regulado por el Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2018, y que establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española.

El artículo 18.4 de nuestra Constitución dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Aunque no se hace mención explícita a los datos de carácter personal, estos forman parte de la intimidad de las personas, puesto que pertenecen al ámbito más privado de las mismas y que desean mantener en secreto o al resguardo del conocimiento de terceros.

La protección de las personas en relación con el tratamiento de sus datos personales es un derecho fundamental consagrado en la Carta de los Derechos Fundamentales de la UE (artículo 8) y en el Tratado de Funcionamiento de la Unión Europea (artículo 16).

El pasado mes de mayo de 2016 se publicó en el Diario Oficial de la Unión Europea el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Este reglamento europeo deroga a la Directiva 95/46/CE.

Los reglamentos son normas que tienen efecto directo lo que significa que se aplican directamente a los Estados miembros sin necesidad de que éstos adopten ninguna norma de trasposición al Derecho interno. Es por ello que la Comisión eligió esta vía con el fin de terminar con la dispersión normativa existente entre los países miembros. Así, con el RGPD tenemos una norma jurídica europea que conforma un Derecho único para toda la Unión al reemplazar a las leyes nacionales.

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

El citado Reglamento ha entrado en vigor el 25 de mayo de 2016, pero no comenzó a aplicarse hasta dos años después de su entrada en vigor, el 25 de mayo de 2018.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual.

Como consecuencia de lo anterior se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Se atiende así a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información.

Por otro lado, apuntar que aún sigue vigente el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales.

Debemos tener en cuenta, asimismo, las limitaciones que prevé la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Por otro lado, se encuentra la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La norma trata de alinear el Ordenamiento con el RGPD abordando la materia con distintos objetivos:

a) Adaptar las previsiones generales del RGPD en el ámbito nacional con el límite del margen de apreciación que se concede a los Estados.

b) Regular sectores de actividad que requieren de un marco específico, ya sea por razón de la naturaleza de la actividad del tratamiento, ya sea por razón de los riesgos eventualmente asociados al tratamiento.

c) Integrar en nuestro Ordenamiento un marco de tutela de los derechos digitales, con fundamento en el mandato de desarrollo legal de garantías respecto del uso de la informática del artículo 18.4 de la Constitución Española.

La **LOPDGDD** debe ser leída e interpretada siempre en el marco del RGPD. Ello exige a sus intérpretes, y en particular a los llamados delegados de protección de datos, aproximarse a esta materia con un enfoque global e integrador.

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble.

Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía.

En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Así, establece su artículo 2 que lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables[1]

Por otro lado, destacar la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público.

También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse

[1]Se añade por disposición final 4.1 de la Ley Orgánica 7/2021, de 26 de mayo

fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley.

Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan.

Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia[2]

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene

[2] Apartado 3 artículo 44 Ley Orgánica 3/2018 modificado por disposición final 4.2 LO 7/2021

o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

2. EL REGLAMENTO (UE) 2016/679, DE 27 DE ABRIL, 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.

Continuando con el Reglamento Europeo, los contenidos fundamentales del mismo son los siguientes:

1. Fortalecimiento de la exigencia de consentimiento y protección de los datos especialmente sensibles. Establece el Reglamento, que el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (art. 7). Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines.

Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. A los ya considerados como datos especialmente protegidos (ideología, religión, afiliación sindical, creencias, salud, origen racial y vida sexual) se añaden los datos genéticos y biométricos dirigidos a definición completa de los «datos genéticos», como los «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona»; y de los datos biométricos», que se describen como los «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos».

2. Reforzamiento del principio de transparencia: Derecho al olvido y portabilidad. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad

del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento

El Reglamento introduce nuevos elementos, como el derecho al olvido y el derecho a la portabilidad, que mejoran la capacidad de decisión y control de los ciudadanos sobre los datos personales que confían a terceros.

Según la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que reconoció por primera vez el derecho al olvido recogido ahora en el Reglamento europeo, tiene por objeto garantizar el derecho de los sujetos titulares de los datos a obtener, sin dilación indebida, la supresión de los datos personales que le conciernan del responsable del tratamiento en determinados supuestos, entre otros, cuando los datos no sean necesarios para las finalidades para las que fueron recogidos, cuando los datos personales hayan sido tratados ilícitamente o cuando los datos personales deban suprimirse para cumplir con una obligación legal establecida en la legislación aplicable al responsable del tratamiento.

El responsable que esté obligado a suprimir datos personales deberá adoptar medidas razonables, teniendo en cuenta la tecnología disponible y el coste de su aplicación, así como informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

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

3. La privacidad y la protección de los datos personales en «todo» el ciclo de vida de la tecnología (Privacy by design). El nuevo marco europeo de protección de datos promueve el establecimiento de un «sistema de control de los riesgos» asociados al tratamiento de los datos personales, que, de manera preventiva, considere la necesidad de tener en cuenta la privacidad y la protección de los datos personales en «todo» el ciclo de vida de la tecnología, desde la fase de diseño hasta su fin, tanto de los sistemas de información, como de las arquitecturas y redes

de comunicación, los procesos productivos y de negocio, de tal manera que se entienda siempre la privacidad como una opción «por defecto».

Se impone una obligación de «responsabilidad proactiva» que exige a las organizaciones el establecimiento de medidas que garanticen y permitan demostrar el cumplimiento del Reglamento (esto es, políticas de protección de datos que no solo han de existir, sino que han de estar adaptadas a las circunstancias de la organización, implementadas y funcionar en la práctica). Desarrollando este principio general, el Reglamento establece la obligación de las empresas de tener en cuenta la protección de datos desde el momento del diseño de sus procedimientos, productos y servicios (privacy by design) y a que por defecto solo sean objeto de tratamiento los datos personales mínimos que sean necesarios para alcanzar el fin legítimo perseguido (privacy by default).

Frente al marco normativo vigente que exige la inscripción de ficheros de las organizaciones ante la Agencia Española de Protección de Datos, el Reglamento se centra en obligaciones de registro internas. Así, ahora será cada responsable, encargado y, en su caso, su representante quienes llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, que deberá contener una información de mínimos que se regula en el propio Reglamento. Las obligaciones anteriormente indicadas no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales (datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física), o datos personales relativos a condenas e infracciones penales en los términos contemplados en el art. 10 del Reglamento.

4. La construcción de un modelo institucional de control: Privacy Impact Assessments y Data Protection Officer. Entre las incorporaciones del Reglamento se incorpora la realización de evaluaciones de impacto (Privacy Impact Assessments o PIAs), siempre que sea probable que las operaciones de tratamiento, especialmente cuando se utilicen nuevas tecnologías, entrañen un alto riesgo para los derechos y libertades de las personas físicas. La Agencia Española de Protección de Datos publicará listas de los tipos de operaciones de tratamiento que requieran una evaluación de impacto.

Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de

aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas.

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

En línea con la tendencia actual que se aprecia en otras muchas normas de establecer figuras y roles específicos que aseguren en las empresas el cumplimiento normativo, el Reglamento introduce la figura obligatoria del «delegado de protección de datos». Así, las empresas se verán obligadas a designar un DPO (ya sea internamente o externalizándolo en un tercero) cuando (i) las actividades principales del responsable consistan en operaciones de tratamiento que requieran un seguimiento regular y sistemático de los interesados y se realicen a gran escala; o (ii) las actividades principales del responsable consistan en el tratamiento a gran escala de categorías especiales de datos.

En lo que a las Administraciones Públicas se refiere, el nombramiento de un DPO será obligatorio en todo caso. El Reglamento establece funciones, requisitos y protecciones específicas para esta figura.

El Reglamento llama también a los mecanismos de soft law para dar respuesta nuevas necesidades. Se insta a asociaciones u otros organismos que representen a categorías de responsables o encargados en determinados sectores a que elaboren códigos de conducta para facilitar la aplicación del Reglamento a las microempresas y las pequeñas y medianas empresas. Se fomenta el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos que permitan evaluar el nivel de protección de datos de los productos y servicios y demostrar el cumplimiento del Reglamento.

5. Severidad del régimen sancionador. El régimen sancionador que ahora se establece resulta mucho más severo que el precedente. Se prevén poderes para sancionar con una advertencia, apercibimiento, solicitud de atención de ejercicio de derechos, limitaciones del tratamiento, y multas administrativas para las que se contempla un importante aumento de las cuantías que pueden llegar hasta los 20.000.000 o un 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Se prevé que para el 25 de mayo de 2018 los Estados miembros comuniquen a la Comisión otras sanciones efectivas, proporcionadas y disuasorias que decidan aplicar para las infracciones que no estén sancionadas con multas administrativas en el Reglamento.

-REGLAMENTO EUROPEO: ALCANCE GENERAL Y EFICACIA DIRECTA

Un reglamento europeo es una norma jurídica de Derecho Comunitario con alcance general y eficacia directa. Ello implica que es directamente aplicable en todos los Estados miembros, pudiéndose invocar por cualquier autoridad o particular, sin que sea precisa ninguna norma jurídica de origen interno o nacional que la transponga para completar su eficacia plena. Esta última característica es lo que los diferencia de las directivas europeas, ya que aunque éstas disponen de alcance general no gozan de eficacia directa.

Su eficacia directa comportará que la normativa estatal, autonómica o incluso los reglamentos u ordenanzas locales queden desplazados y sean inaplicables en todo aquello en lo que se opongan al Reglamento europeo.

El RGPD que es aplicable a partir del 25 de mayo de 2018 surge para garantizar un nivel uniforme y elevado de protección del tratamiento de los datos de las personas físicas, y así lo indica el considerando núm. 10 del Reglamento: «debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea».

El RGPD contiene un total de 99 artículos estructurados en once capítulos: Capítulo I : Disposiciones Generales

Capítulo II: Principios
Capítulo III: Derechos del interesado
Capítulo IV: Responsable del tratamiento y encargado del tratamiento
Capítulo V: Transferencias de datos personales a terceros países u organizaciones internacionales
Capítulo VI: Autoridades de control independiente
Capítulo VII: Cooperación y coherencia
Capítulo VIII: Recursos, responsabilidad y sanciones
Capítulo IX: Disposiciones relativas a situaciones específicas de tratamiento
Capítulo X: Actos delegados y actos de ejecución
Capítulo XI: Disposiciones finales

En cuanto al objeto de regulación, el Reglamento:

— establece normas relativas al tratamiento de DP y a la libre circulación de los mismos;

— protege derechos fundamentales de las personas físicas, en particular su derecho a la protección de los DP, mientras que la Directiva hacía una especial mención a la intimidad, que desaparece en el Reglamento, consolidándose así la naturaleza autónoma del DPDP.

El objeto del RGPD es la protección de las personas físicas en lo que respecta al tratamiento, automatizado o no, de sus datos personales y las normas relativas a la libre circulación de dichos

datos (artículo 1). Se excluye del objeto de este reglamento el tratamiento de datos personales relativos a personas jurídicas.

El RGPD no será aplicable en el tratamiento de datos personales en los siguientes supuestos (artículo 2.2):

— Cuando se ejerza una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión

— Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE, es decir las relativas a la política exterior y seguridad común

— Cuando se refiera al tratamiento de datos realizado por una persona física en el ejercicio de una actividad exclusivamente personal o doméstica

— Para las actividades de las autoridades con finalidades de prevención, investigación, detección de ilícitos penales o de protección a la seguridad pública.

Por lo que se refiere al ámbito de aplicación territorial, se indica en el artículo 3 del RGPD que éste será de aplicación al tratamiento de datos personales cuando el establecimiento del responsable o del encargado se encuentre en la Unión, independientemente de que el tratamiento tenga lugar dentro o fuera de ella, así como al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en ella, cuando las actividades del tratamiento estén relacionadas con:

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

— el control de su comportamiento, en la medida en que éste tenga lugar en la Unión.

Se observa la gran ambición de este nuevo reglamento, pues su ámbito territorial de aplicación se extiende y traspasa las «fronteras europeas». Se protege el tratamiento de datos personales de ciudadanos de la Unión con independencia que el tratamiento o el responsable de los mismos esté o no establecido en la Unión.

Añade el apartado tercero del artículo 3 , que también será de aplicación el RGPD cuando en virtud del Derecho Internacional Público deba acudirse al Derecho de uno de los Estados miembros, siendo esta previsión obvia pues, como hemos indicado anteriormente, el reglamento resultará directamente aplicable en los Estados de la Unión.

En las definiciones (art. 4) hay que destacar una ampliación considerable del catálogo (se pasa de 8 a 26), en la que conviene subrayar las siguientes novedades:

— En la definición de datos personales (art. 4.1), la persona física se considera ahora identificable mediante un identificador, no sólo un número, sino también un nombre, datos de localización o identificador en línea. Además se añaden a los elementos propios los de la identidad genética, que se suman a los de la física, fisiológica, psíquica, económica, cultural o social, que contenía la Directiva.

Se considera Dato personal: (art. 4.1): 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.

En la definición de tratamiento (cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción), se mantiene tanto el procedimiento automatizado como el que no lo está; y se añaden al concepto de tratamiento las operaciones de estructuración, adaptación o limitación; con supresión de la elaboración y el bloqueo.

También destacan las nuevas definiciones no contenidas en la Directiva, que ahora contempla el art. 4 del Reglamento : limitación de tratamiento, elaboración de perfiles, seudonimización (el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable), violación de la seguridad de los DP, datos genéticos, datos biométricos, datos relativos a la salud, establecimiento principal, representante, empresa, grupo empresarial, normas corporativas vinculantes, autoridad de control, autoridad de control interesada, tratamiento transfronterizo, objeción pertinente y motivada, servicio de la sociedad de la información y organización internacional.

Por otro lado, salvo alguna modificación de estilo o accesoria, no varía la definición de «fichero», «responsable de tratamiento» (determina los fines y medios del tratamiento), «encargado del tratamiento» (trate datos personales por cuenta del responsable del tratamiento) y «tercero» (el cual está bajo la autoridad directa del responsable o del encargado).

— En la definición de destinatario: de la exclusión de los destinatarios en los supuestos de comunicación de DP en el marco de una investigación, se añade que la misma ha de ser conforme al D. UE o nacional.

— El consentimiento del interesado añade a los requisitos de manifestación de voluntad libre, específica e informada, el de ser inequívoca y que deba hacerse mediante declaración o clara acción afirmativa.