uc3m | Universidad Carlos III de Madrid

OpenCourseWare

DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

***Coordinadora Curso:* -Profª (PhD) María Nieves de la Serna Bilbao**

Titular de Derecho Administrativo UC3M// Departamento de Derecho Público

Co-directora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz

LECCIÓN 2: PROTECCIÓN DE DATOS: RÉGIMEN GENERAL

III ANÁLISIS DEL ACTUAL MARCO REGULADOR EN MATERIA DE PROTECCIÓN DE DATOS

Elaborado por PhD. Mª NIEVES DE LA SERNA BILBAO
Profesora Titular de Derecho Administrativo// Departamento de Derecho Público
Codirectora del Máster Universitario en Derecho Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información// Instituto Pascual Madoz
Universidad Carlos III de Madrid

SUMARIO:

7.- Principios fundamentales aplicables en materia de protección de datos

8.- Bases de legitimación del tratamiento

9.- Derechos de los interesados

10. Restricciones a los principios y derechos de los interesados

11.- Responsabilidad proactiva –*Accountability*-

12. Régimen sancionador

.

III ANALISIS DEL ACTUAL MARCO REGULADOR EN MATERIA DE PROTECCIÓN DE DATOS

uc3m | Universidad Carlos III de Madrid

Normas que regulan el derecho a la protección de datos

- 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 sus datos personales y a la libre circulación de estos datos (en adelante RGPD).
- Directiva (UE) 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 o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se derogó la Decisión Marco 2008/977/JAI del Consejo.

1.- Introducción: la Protección de Datos como Derecho Fundamental. Reconocimiento constitucional y consideraciones jurisprudenciales

Como ya hemos dicho, la proliferación de los medios digitales y la interconexión globalizada han transformado la vida en todos sus aspectos gracias a los múltiples avances que han generado. No son pocos, sin embargo, los retos que este inmenso desarrollo tecnológico ha traído consigo; retos que, inevitablemente, han sacudido el ámbito jurídico. Así, en los últimos años la regulación jurídica ha puesto especial atención en la necesidad de responder a las exigencias de un entorno inédito y en continua evolución en

aras de maximizar las ventajas que la transformación digital esconde. Ciertamente, en este nuevo contexto digital, los derechos de los ciudadanos han quedado expuestos a una mayor vulnerabilidad, y de ahí, precisamente, la necesidad de implantar un marco regulatorio firme y sólido que asegure su salvaguarda.

Especial mención requiere, a los efectos que aquí interesan, el impacto de este desarrollo tecnológico respecto del exponencial crecimiento que han sufrido la magnitud de la recogida y el intercambio de datos personales en los últimos tiempos: de un lado, ha aumentado el tratamiento de datos por parte de las empresas privadas y por las autoridades públicas; de otro, las propias personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. Así, se plantea la importancia de regular el uso y el control de las Nuevas Tecnologías para proteger, fundamentalmente, el Derecho a la protección de los datos personales de los ciudadanos en el medio digital.

En España, la necesidad de enfrentar los efectos de la transformación digital desde el plano jurídico se puso de manifiesto ya en 1978. En efecto, la propia Constitución Española previó en su artículo 18.4 el desarrollo de una ley para la limitación de*l uso de la informática en aras de «garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*, precepto en el que, aún a falta de mención expresa, el Tribunal Constitucional ha identificado el derecho de los ciudadanos a la Protección de Datos Personales. En efecto, el alto Tribunal, en su STC 254/1993, de 20 de julio[2], otorga al precepto 18.4 de la Constitución una doble naturaleza: por un lado, lo consolida como una garantía indispensable para la dignidad y los derechos de la persona, particularmente los derechos fundamentales a la intimidad y al honor recogidos en el primer párrafo de ese mismo artículo, frente a los riesgos que entrañan las nuevas tecnologías; segundo, lo

reconoce en sí mismo como un derecho o libertad fundamental en cuanto asegura un núcleo inalienable de la dignidad y libertad de la persona frente a potenciales agresiones generadas por un uso ilegítimo en el tratamiento mecanizado de datos por la «informática». En esta misma línea se mantiene en su STC 11/1998, de 13 de enero[3], en la que asienta la existencia de un derecho a la «libertad informática» cuyo núcleo esencial contiene el derecho a controlar el uso de todos los datos insertos en los programas informáticos, y que abarca también el derecho de oposición del ciudadano al uso de sus datos personales para fines distintos de aquel para los que se otorgaron.

Quizá la sentencia más notable a este respecto sea la Sentencia 292/2000[4], de 30 de noviembre, relativa al recurso de inconstitucionalidad nº 1463-2000 interpuesto por el Defensor del Pueblo contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en la que establece con claridad que el Derecho a la Protección de Datos, que ha de entenderse recogido en el artículo 18.4 de la Constitución, es un derecho fundamental que otorga a sus titulares un poder de disposición y control respecto de sus datos personales que permite a los individuos la libre decisión de los datos que desea proporcionar a un tercero, ya sea este el Estado o un particular, así como los datos que este tercero puede recabar. Igualmente, integra el derecho a saber quién posee dichos datos y con qué finalidad, pudiendo oponerse el particular a esa posesión, salvo supuestos en los que esté obligado por norma legal. Pues bien, jurídicamente, estos poderes de disposición y control se concretan en la facultad de consentir y conocer de la recogida, la obtención, el acceso, el almacenamiento, el tratamiento, sea o no informático, el uso y las cesiones de estos datos personales, que se constituyen como elementos esenciales de la definición constitucional del derecho fundamental que nos ocupa.

En cualquier caso, si algo parece claro es que se trata de un derecho que tiene por objetivo la protección constitucional de la intimidad personal, así como los bienes de la personalidad que pertenecen al ámbito de la vida privada, y que quedan inextricablemente ligados al respeto de la dignidad de la persona por cuanto salvaguardan un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas, tal como reconoció tempranamente el alto Tribunal en su STC 170/1987, de 30 de octubre[5]. Por consiguiente, el derecho a la protección de datos ha de entenderse aplicable a los datos de carácter personal, y de ahí que su aplicación no se limite exclusivamente a los datos íntimos de la persona, sino que protege cualquier dato personal cuyo conocimiento o empleo por terceros pueda afectar a otros derechos, aun no fundamentales. En palabras del Tribunal, los datos amparados son todos aquellos que *«identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico, o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo».*

En el ámbito supranacional, la sala segunda del Tribunal de Justicia de la Unión Europea –en adelante TJUE- consideraba en su Sentencia de 20 de diciembre de 1997 relativa al caso Peter Nowak c. Data Protection Commissioner[6] (Asunto C-434/16) inoportuna la noción de datos personales que recogía la Directiva 95/46, objeto de análisis de la sentencia citada, precisamente por su reducción a datos confidenciales o íntimos, pues debía entenderse que abarcaba todo género de información, tanto objetiva como subjetiva que «*versen sobre la persona en cuestión», consideración que, sin duda, ha de tenerse en cuenta para la interpretación del artículo 18.4 CE.*

La importancia de este derecho es tal que, como hemos visto, la Carta de Derechos Fundamentales de la UE lo reconoce en su artículo 8, junto con el

derecho de acceso y rectificación y los principios de lealtad, finalidad y consentimiento. Además, en su párrafo segundo preceptúa la necesidad de un control respecto a la protección de datos, ejercido por «*una autoridad independiente*», exigencia contenida también en la Directiva 95/ derogada y, que el RGPD refuerza. Para cumplir con dicho objetivo se configuró en España la Agencia Española de Protección de Datos, en adelante AEPD-, en el año 1992, cuyo papel resulta esencial para asegurar el cumplimiento de la normativa de protección de datos que se analiza en el apartado que sigue. Finalmente, como también quedó expuesto, el artículo 16 del Tratado de Funcionamiento de la Unión Europea lo recoge en su articulado, atribuyendo al Parlamento Europeo y al Consejo la facultad para establecer las normas relativas el tratamiento de datos de carácter personal, tanto por las propias instituciones europeas como por parte de los Estados Miembros. Así, por ejemplo, en materia política exterior y seguridad común, el Consejo deberá adoptar una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en este ámbito, tal como prevé el artículo 39 del Tratado de la Unión Europea.

En definitiva, la revolución digital ha acentuado la necesidad de amparar el Derecho a la Protección de los Datos personales frente a todo tipo de intromisiones ilegítimas que puedan producirse, Derecho que también es recogido en la Declaración Europea de Protección de Datos y en todas las Cartas de Derechos Digitales aprobadas en Europa. El desarrollo de este derecho responde a la necesidad de configurar el Derecho a la Protección de Datos como un derecho autónomo, en línea con las exigencias derivadas de la transformación digital. Así, se ha dejado atrás su tradicional consideración como mero mecanismo de garantía del Derecho a la intimidad, para pasar a constituir un derecho en sí mismo e independiente de otros -como el derecho a la intimidad o a la imagen- al que, además, como ya se ha señalado, no ha

tardado en reconocérsele carácter de fundamental por su importancia en la sociedad actual. Sea como sea, se trata de un elemento esencial para la protección de la intimidad en sentido amplio (privacidad) de las personas y, en consecuencia, para el desarrollo de su vida personal, profesional, económica o social; de ahí, precisamente, su reconocimiento constitucional.

2. Marco normativo vigente para la Regulación del Derecho a la Protección de datos

Establecida la importancia del Derecho a la Protección de Datos en la actualidad como Derecho Fundamental de los ciudadanos, procede desarrollar una breve caracterización del marco normativo para asegurar su protección. Se trata de una regulación que se ha desarrollado desde dos niveles territoriales diferentes: el europeo y el nacional, y que, fundamentalmente, puede reducirse a la vigencia de dos cuerpos normativos: el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPDGDD. A esta normativa básica cabría añadir otras disposiciones que resultan igualmente esenciales en relación con determinados aspectos de la materia – así, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales; o la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, entre otras -. No obstante, no siendo este el lugar para el estudio exhaustivo y detallado de todos y cada uno de ellos, a nuestros efectos resulta suficiente con efectuar un análisis de los aspectos esenciales de las dos primeras disposiciones.

El RGPD ha supuesto un antes y un después en la regulación del Derecho Fundamental a la Protección de Datos en todos los Estados Miembros. Como se ha señalado, se trata de una norma obligatoria en todos sus elementos y directamente aplicable en todos los Estados miembros por lo que no necesita ser transpuesta al ordenamiento jurídico de los Estados para su aplicación[1].

No obstante, el propio RGPD deja algunos ámbitos con diverso alcance -aproximadamente 56 habilitaciones- que los Estados miembros pueden desarrollar o completar a través de normativa nacional, situación que en España se completa con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD). Como bien ha señalado la jurisprudencia europea existe el derecho y la obligación de los Estados de hacer cuanto sea necesario para asegurar el efecto útil del conjunto de las disposiciones del Reglamento[2].

La aplicabilidad directa de los Reglamentos exige que su entrada en vigor y su aplicación, en favor o en contra de los sujetos de Derecho, se produzcan sin necesidad de ninguna medida de incorporación al Derecho nacional. Es más, los Estados miembros están obligados a no obstaculizar el efecto directo propio de los Reglamentos, siendo "*el respeto escrupuloso de este deber"* una condición indispensable *"para la aplicación simultánea y uniforme"* de las reglas contenidas en los Reglamentos de la Unión en el conjunto de ésta[3]. De esta

[1] Hay que recordar que, de acuerdo con el artículo 288 del TFUE, el Reglamento es un acto legislativo vinculante que tiene la peculiaridad de que se debe aplicar, directa y completamente, en toda la Unión Europea. Por tanto, los Estados miembros están obligados a no obstaculizar el efecto directo propio de los Reglamentos, siendo "el respeto escrupuloso de este deber" una condición indispensable "para la aplicación simultánea y uniforme" de las reglas contenidas en los Reglamentos de la Unión en el conjunto de ésta. De ahí que, las normas nacionales vigentes deban ser modificadas para evitar controversias –principio de prevalencia- por lo que corresponde al legislador de cada Estado realizar una tarea de depuración del ordenamiento jurídico.

[2] STJCE caso Scheer, asunto 30/70, apartados 7 y 8

[3] Véase al respecto el Dictamen del Consejo de Estado núm.757/2017, de 26 de septiembre con cita, entre otras, de las SSTJCE de 10 de octubre de 1973, Variola, apartado 10; de 2 de febrero de 1977, 50/76, Amsterdam Bulb, apartados 5 y 6; de 31 de enero de 1978, Zerbone, 94/77, apartados 24 y 25; de 28 de marzo de 1985, Comisión/Italia, 272/83, apartado 26; y SSTJUE de 14 de julio de 2011, Bureau national interprofessionnel du Carnac, C4/10 y C27/10, apartado 66; y de 15 de noviembre de 2012, Al-Aqsa/Consejo, C- 539/10 P, apartado 87.

forma, el derecho a la protección de datos en España, protegido por el artículo 18.4 de la CE, pasa a estar directa y principalmente regulado en una norma europea, en donde la norma nacional, es decir, la LOPDGDD, pasa a tener un papel únicamente de desarrollo o complemento del RGPD. Ello implica, por tanto, un traslado parcial del canon constitucional de protección el derecho fundamental que, en cuanto se refiere a actividades regidas por el Derecho de la Unión, se debe regir por la Carta de Derechos Fundamentales de la Unión Europea y por la interpretación que el Tribunal de Justicia de la Unión lleve a cabo.

A partir de la vigencia del RGPD tanto las empresas, los organismos y las administraciones que se han visto obligadas en Europa, y en particular en nuestro país a la adopción de cambios estructurales y organizativos para adaptarse a las previsiones del RGPD, que aspira a garantizar «un nivel uniforme y elevado de protección de las personas físicas» en todo el continente; y ello, con el fin de garantizar el pleno control de los datos personales por parte de sus titulares. Igualmente, se persigue la supresión de los obstáculos que impidan o dificulten la circulación de datos personales entre los Estados Miembros, al tiempo que se garantizan en todo momento elevados niveles de protección en su tratamiento.

De acuerdo con lo anterior, es preciso indicar que, la LOPDGDD no puede confundirse con una norma de transposición del RGPD. Muy al contrario, la misma persigue adaptar el ordenamiento jurídico español el RGPD, pero sólo en aquellos ámbitos que permite. Por tanto, el derecho fundamental de las personas físicas a la protección de datos personales amparado por el artículo 18.4 de la CE, se ejercerá con arreglo a lo establecido en el RGPD y en LOPDGDD. Recordemos que el artículo 18.4 CE señala:

"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."

Por último, baste señalar que la LOPDGDD no sólo desarrolla o complementa las disposiciones del RGPD, sino que también garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 de la CE contenidos en el Título X de la LOPDGDD que se clasifican de la siguiente forma:

1) Derechos generales de los ciudadanos en internet: este bloque incluye los arts. 79 a 82, 96 y 97.
2) Derechos específicos relacionados con los menores: arts. 83, 84, 92 y 97.2 (en parte).
3) Derechos relacionados con el ámbito laboral: arts. 87 a 91.
4) Derechos relacionados con los medios de comunicación digitales: arts. 85 y 86.
5) Derecho al olvido en internet: arts. 93 y 94.
6) Derecho a la portabilidad en las redes sociales: art. 95.

A partir de la vigencia del RGPD y la LOPDGDD tanto las empresas, los organismos y las administraciones que se han visto obligadas en nuestro país a la adopción de cambios estructurales y organizativos para adaptarse a las previsiones de aquella normativa que aspira a garantizar *«un nivel uniforme y elevado de protección de las personas físicas»*; y ello, con el fin de garantizar el pleno control de los datos personales por parte de sus titulares. Igualmente, se persigue la supresión de los obstáculos que impidan o dificulten la circulación de datos personales entre los Estados Miembros, al tiempo que se garantizan en todo momento elevados niveles de protección en su tratamiento.

2. El RGPD; objetivo y ámbito de aplicación

Como señala el RGPD, el mismo persigue *"contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas"*[4]. Su aplicabilidad directa reduce la fragmentación normativa y brinda una homogeneización y aumento de la seguridad, por lo que consigue *"garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior"*[5]. También proporciona *"seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofreciendo a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros"*[6].

El RGPD diferencia dos ámbitos de aplicación, el ámbito material y el ámbito territorial. Respecto del primero, es decir el ámbito material, el artículo 2.1, señala que la aplicación del RGPD recae sobre 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»,* y el artículo 4.1 RGPD define *«fichero»* como *«todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica».*

[4] Considerando 2 RGPD
[5] Considerando 13 RGPD
[6] Considerando 13 RGPD

De acuerdo con el artículo 2 del RGPD, el mismo se aplica a:

1) Todos los tratamientos de actividades comprendidas en el ámbito de aplicación del derecho europeo.

2) Todos los tratamientos de datos automatizados o no, y a la libre circulación de tales datos

3) A los datos de las personas físicas, independientemente de su nacionalidad o residencia, de la Unión Europea.

4) A las actividades de los tribunales y autoridades judiciales[7].

Por el contrario, **no resulta aplicable:**

1) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; como la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional[8].

2) Cuando los Estados miembros lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; como ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión[9].

3) Todo tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Se considera tal a aquella que no tienen conexión con actividad profesional o comercial (sin lucro) entre las que 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[10]. Pero en todo caso, sí se resulta aplicable a los responsables o encargados del tratamiento que proporcionen los

[7] Considerando 20 y artículo 55 RGPD
[8] Considerando 15
[9] Considerando 16
[10] Considerando 18

medios para tratar datos personales relacionados con tales actividades personales o domésticas[11].

4) Tampoco resulta aplicable a las autoridades competentes que realicen tratamientos de datos personales 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. En este caso se aplica un régimen específico contenido en la Directiva (UE) 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 o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[12].

5) Igualmente, no se aplica, como ya vimos, a los datos de las personas fallecidas**.** No obstante, el RGPD permite que los Estados miembros puedan establecer normas relativas a este tipo de datos[13], de ahí que la LOPDGDD dedique el artículo 3 a estos datos[14].

6) Se encuentran también excluidos del RGPD los datos de las personas jurídicas y, en particular, el nombre y la forma de la persona jurídica así como sus datos de contacto[15].

---

[11] Artículo 2.2 RGPD
[12] Considerando 23
[13] Considerando 27
[14] LOPDGDD, en el artículo citado extiende sus efectos al tratamiento de datos de personas fallecidas al establecer en su artículo tercero la posibilidad de que las personas vinculadas al fallecido por razones familiares o de hecho, a sus herederos, las personas o instituciones a las que el fallecido hubiese designado expresamente, así como los representantes menores, el Ministerio fiscal o las personas de apoyo, en caso de que el fallecido sea menor o discapacitados, soliciten al responsable o encargado del tratamiento el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley
[15] Considerando 17

7) No entran dentro del ámbito de aplicación del RGPD los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, como por ejemplo los un e-mail contiene información como la hora de envío, la persona a quien se envía, el remitente, etc, pero en lo que respecta al contenido del mensaje no se divide ni se categoriza fácilmente lo que puede ser un problema de compatibilidad con la estructura de un sistema de base de datos relacional[16]. Sin embargo, se debe tener presente que ya se están desarrollando tecnologías y servicios para ayudar a solventar y estructurar sus contenidos conocida como «datafication».

8) El RGPD no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión[17].

Brevemente descrito el ámbito material de aplicación del RGPD, es necesario referirnos al ámbito territorial que el RGPD concreta. El artículo 3 del RGPD y las Directrices 3/2018 relativas al ámbito territorial del RGPD de 12 de noviembre de 2019 aprobadas por el Comité Europeo de Protección de Datos, el RGPD se aplica tanto a los responsables y a los encargados de tratamiento de datos que estén establecidos en la Unión Europea en el contexto de actividades de un establecimiento[18]. Se entiende por ”establecimiento” el ejercicio y la manera efectiva y real de una actividad y la forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no resulta ser un factor determinante al respecto[19].

[16] Considerando 15 RGPD
[17] Considerando 16
[18] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf
[19] Considerando 21 y art. 4. 16

La aplicación del RGPD se amplía a los responsables y encargados no establecidos en la UE siempre que éstos realicen tratamientos derivados de:

A) Una oferta de bienes o servicios destinados a ciudadanos de la Unión independientemente de que medie pago o no. Como señala el RGPD "*Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión*"[20].

B) Como consecuencia de un control del comportamiento - monitorización y seguimiento-. El propio RGPD señala que "*Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.*

Para que esta ampliación del ámbito de aplicación sea efectiva aquellas organizaciones deben nombrar un Representante en la Unión Europea, sujeto éste que actúa como punto de contacto de las autoridades de supervisión y los

[20] Considerando 23

ciudadanos. Los datos de contacto de los representantes en la Unión se deben proporcionar obligatoriamente a los interesados en la información relativa a los tratamientos de sus datos personales.

Como señala el RGPD corresponde al representante actuar por cuenta del responsable o del encargado y puede ser contactado por cualquier autoridad de control. *El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado*[21].

Finalmente cabe señalar que el RGPD también se aplica al tratamiento de datos personales de un responsable no establecido en el territorio de la Unión el RGPD en virtud del Derecho Internacional Público. En efecto, como señala el RGPD

"*Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro*"[22].

3. Datos de carácter personal; concepto

3.1.- Concepto

[21] Considerando 80 RGPD
[22] Considerando 25 RGPD

Como se suele señalar, en el desarrollo de nuestra vida, tanto en el mundo real como digital, utilizamos datos de carácter personal, es decir, datos en los que la persona física es identificada o puede resultar identificable. Es así que, cualquier dato que se identifique con una persona, en la que su identidad resulte clara o se pueda determinar a partir de información adicional, el mismo es dato de carácter personal y, por tanto, encuentra protección en el RGPD.

El RGPD define el concepto de «datos personales» como comprensivo de "*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.*

La persona titular de los datos recibe la denominación de "interesado" y los datos protegidos no se limitan exclusivamente a los relacionados con la vida privada o íntima de la persona sino que, también, comprende todos los datos que permitan identificar a la persona en cualquier ámbitos de su vida, como los datos del ámbito laboral, profesional, educativo, personal, social, deportivos, sanitarios, etc.. Es así que la normativa de protección de datos reconoce un control, titularidad y disposición de todos los datos a la persona física que contenga información sobre ella.

Como señala el RGPD *"Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación,*

teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos"[23].

3.2. Anonimización y seudonimización de datos

Es importante destacar que los datos que no se puedan relacionar con un sujeto concreto, bien desde su origen, bien por haber sido sometido a un proceso de anonimización, no se consideran datos de carácter personal. Un dato es sometido a un proceso de anonimización cuando el dato se disocia del titular de tal forma que no resulte posible relacionarlo con un interesado (por ejemplo, xx de personas están afectadas por SIDA)[24]. Es por ello que el RGPD señala que *"…los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación*.[25]"

Los datos anónimos, en todo caso, se deben diferenciar de los "datos seudonimizados". En estos últimos, a diferencia del anterior, permiten identificar al titular, pero siempre que se utilice información adicional. Por tanto, la seudonimización determina que un dato personal, en un determinado momento del tratamiento, se sustituyen los atributos que contienen los datos personales por un seudónimo (por ejemplo, un código de barras), manteniéndose los datos personales separados de aquellos atributos. De acuerdo con el RGPD un proceso de seudonimización» se produce cuando "e*l tratamiento de datos personales ….ya no puedan atribuirse a un interesado sin utilizar información*

[23] Considerando 26 RGPD
[24] Véase al respecto el documento AEPD "LA K-ANONIMIDAD COMO MEDIDA DE LA PRIVACIDAD", de 14 de mayo de 2019; o las Orientaciones y garantías en los procedimientos de anonimización de datos personales, de 16 de julio de 2018.
[25] Considerando 26 RGPD

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"[26]. Como también señala el propio RGPD, "*La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.*[27]. Por esta razón resulta importante destacar que a los datos personales seudonimizados se les debe aplicar medidas técnicas y organizativas adecuadas para evitar que se produzca la conexión del dato seudonimizado con los datos personales del titular.

4. Categorías especiales de datos personales

4.1 Aspectos generales

Con carácter general, todos los datos personales que cumplan los requisitos antes mencionados, es decir, que pueda identificar con una persona directa o indirectamente, encuentran protección tanto por el RGPD como por la LOPDGDD, salvo que los mismos tengan un uso doméstico. Dentro de los datos personales, el RGPD presta una atención particular a aquellos datos personales que, por su naturaleza, pueden considerarse particularmente sensibles por entrañar su tratamiento importantes riesgos para los derechos y las libertades fundamentales. Se trata de una "categoría especial de datos" que cuentan con una protección reforzada. Dentro de ellos se comprende a los

[26] Artículo 4 RGPD y Considerando 29 RGPD
[27] Considerando 28 RGPD

datos que revelan el origen étnico o racial -entendiéndose que el uso del término «origen racial» en el RGPD no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas-, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos o datos relativos a la saludo o vida sexual u orientaciones sexuales de las personas físicas que puedan generar discriminación[28].

No se consideran dentro de esta clasificación a las fotografías *"pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física."*[29].

Como señala el RGPD, estos "datos especiales" merecen una atención específica dado 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".* La citada norma europea adopta, por regla general, la prohibición de su tratamiento, salvo en aquellos casos específicos contemplados por el propio Reglamento y, aun en ellos, con sometimiento pleno a las condiciones y límites en él previstos[30]. En efecto, el RGPD admite la posibilidad de establecer excepciones a dicha prohibición de tratamiento de estas categorías especiales de datos personales; así, por ejemplo, cuando el interesado preste su consentimiento explícito o si su uso se desarrolla en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales[31]. Fuera

[28] Véase al respecto el artículo 9 RGPD y las definiciones del artículo 4 RGPD
[29] Considerando 51 RGPD
[30] Art 9.1 RGPD *"1. Quedan prohibidos el tratamiento de 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 orientaciones sexuales de una persona física."*
[31] Considerando 51

de tales casos, su tratamiento sólo puede responder a razones de interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud, siempre que se asegure en todo momento las garantías pertinentes[32]. Finalmente, destacar que el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública, si bien ha de estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas y sin que en ningún caso pueda implicar la intervención de terceros con fines ajenos a los expuestos[33].

El artículo 9 de la LOPDGDD completa las previsiones del RGPD al disponer que, con el fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no resulta suficiente para legitimar el tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico, salvo en los supuestos expresamente previstos en el artículo 9.2. del Reglamento de la UE, ya citados. Además, este precepto exige que el tratamiento de datos que se efectúe por razones de un interés público esencial, para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas, servicios de asistencia sanitaria y social, o para fines de interés público en el ámbito de la salud pública, habrá de hacerse mediante una norma con rango le ley.

4.2 Datos de salud

[32] Considerando 52
[33] Considerando 54 y art. 9.2 RGPD

Respecto de los datos de Salud el RGPD señala que *"Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos"*[34].

[34] Considerandos 52 y 53 RGPD