EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Módulo 1: Marco general para el tratamiento de datos personales

Contenido

1.1. PRINCIPALES NOVEDADES DEL REGLAMENTO GENERAL DEL PROTECCIÓN DE DATOS (RGPD).

1.1.1. INTRODUCCIÓN.

El **Reglamento General de Protección de Datos[1] (RGPD)** es la más importante de las normas a través de las que se ha producido la revisión del marco legal de la protección de datos en la Unión Europea. Ello se debe a su alcance general y a que, como dispone su artículo 1, su objeto es fijar las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y también las normas sobre la libre circulación de datos en la Unión.

Junto al RGPD se aprobó también una Directiva sobre protección de datos en el ámbito policial y judicial penal (Directiva de Policía)[2]. Esta norma tiene carácter sectorial y, si bien se basa en los principios, derechos y garantías establecidos en el RGPD, contiene especialidades adecuadas a las peculiaridades de los tratamientos de datos que se desarrollan en la prevención y persecución de delitos.

Actualmente está en fase de tramitación legislativa una reforma de la conocida como Directiva ePrivacy[3]. La norma que se está debatiendo es un reglamento. Pese a ser también una norma limitada a un sector concreto, sus efectos son transversales, ya que una parte significativa de los tratamientos de datos que hoy día se realizan se apoya de una u otra forma en comunicaciones electrónicas, al menos tal y como el proyecto de reglamento las define.

En todo caso, la propuesta de nuevo reglamento ePrivacy presentada por la Comisión se remite en todo lo relativo a protección de datos al RGPD, incluyendo el hecho de que prevé que las autoridades de control de la aplicación de este reglamento serán las mismas que supervisen la aplicación del RGPD.

Las tres normas mencionadas son el núcleo central del régimen europeo de protección de datos. Hay también previsiones sobre protección de datos en otras normas de la Unión, como pueden ser las relativas a prevención del blanqueo de capitales o las que regulan agencias como Europol o Eurojust. Pero en todos estos casos las regulaciones son muy específicas para las actividades propias de cada uno de estos ámbitos y siempre se remiten a alguna de las tres normas citadas.

---

[1] 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).

[2] 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.

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

1.1.2. EL RGPD COMO ACTO JURÍDICO DE LA UNIÓN EUROPEA.

Una primera e importante novedad del RGPD tiene que ver con su naturaleza jurídica.

Los reglamentos son normas que tienen efecto directo y se aplican directamente en los Estados Miembro sin necesidad de que éstos adopten ninguna norma de introducción en el derecho interno. No sucede como en el caso de las Directivas, que requieren de normas nacionales de trasposición.

La Comisión eligió este instrumento porque uno de los problemas que la revisión del marco legal europeo pretendía resolver era la dispersión normativa derivada de las trasposiciones llevadas a cabo por los Estados Miembro.

Las Directivas son normas que fijan los fines y dejan a los Estados Miembro un amplio margen de libertad para elegir los medios para conseguirlos. Hay que señalar, sin embargo, que en los últimos años se está asistiendo a una generalización de directivas muy precisas y detalladas, en las que la capacidad de actuación de los Estados se ve muy limitada.

En el caso de la Directiva 95/46, sus objetivos han sido interpretados de maneras muy distintas por los Estados, lo que ha dado lugar a soluciones diferentes que, en último extremo, suponen niveles de protección también heterogéneos.

Un buen ejemplo podría ser el de la posición de las autoridades de protección de datos. La Directiva se limitaba a señalar que debían existir y ser independientes, asignándoles unas funciones mínimas que todos los Estados deberían respetar. En la práctica, ello ha conducido a que mientras en algunos Estados Miembro, como España, la autoridad de control tiene potestades de investigación y sanción, en otros carece del poder de imponer sanciones económicas y, en algunos casos, sólo puede emitir recomendaciones o iniciar un proceso judicial si detecta una infracción de la normativa.

Algo similar ocurre en otras materias, entre las que pueden citarse la lista de datos objeto de especial protección, los datos sensibles, el valor relativo de las bases jurídicas que legitiman los tratamientos de datos o la presencia de figuras como el delegado de protección de datos.

La Comisión optó por enfrentar esta situación proponiendo como nueva norma un reglamento, acto jurídico europeo que pretende lograr un derecho único para toda la Unión al reemplazar a las leyes nacionales existentes y no necesitar de trasposición mediante nuevas normas.

Los propósitos de la Comisión se han alcanzado, pero de forma relativa.

El carácter directamente aplicable de los reglamentos ha dado lugar a un fenómeno completamente opuesto al que antes se describía para las directivas. Los negociadores en el Consejo o el Parlamento Europeo son conscientes de que lo que se decida en un reglamento se convierte en la norma que se aplica directamente en los Estados. No existe el margen de maniobra que permite la trasposición de las directivas. Por ello, empieza a ser habitual que cuando un reglamento trata sobre materias sensibles para los Estados en los que es difícil llegar a entendimientos comunes los textos finales dejen márgenes razonablemente amplios de desarrollo o aplicación a nivel nacional.

Este fenómeno se ha dado también en el RGPD. **Los Estados Miembro pueden actuar normativamente en relación con una lista extensa de materias, valiéndose de distintos tipos de habilitación que el RGPD les ofrece**. Se ha llegado a decir que se trata de una norma con cuerpo de reglamento y alma de directiva.

Ante todo, hay disposiciones del RGPD que expresamente mandatan a los Estados Miembro para que adopten normas de aplicación que las completen o detallen. El ejemplo más claro de este tipo de disposiciones es el que tiene que ver con las autoridades de supervisión. El RGPD define sus características generales, pero pide a los Estados que adopten normas en las que se precise cuál de las posibles opciones que ofrece eligen. Por ejemplo, el RGPD señala que la autoridad de supervisión podrá ser designada por el gobierno, el parlamento, el jefe del estado o un organismo independiente encargado de esa tarea. Cada Estado Miembro tendrá que decidir en su norma de aplicación, y siguiendo su tradición jurídica o práctica establecida, por cuál de esas alternativas opta.

En segundo término, hay disposiciones en que la regulación estatal es prácticamente condición indispensable para que el RGPD pueda aplicarse. Es el caso, entre otros, de algunas de las excepciones que permiten el tratamiento de los datos sensibles. El RGPD prevé que esos datos puedan tratarse para determinadas finalidades (por ejemplo, con fines de asistencia sanitaria, o de investigación científica) en los términos que establezca la legislación nacional. Aunque no hay una obligación de que los Estados adopten esta legislación, es obvio que si no lo hacen no será posible el tratamiento de esos datos para esas finalidades.

Una tercera posibilidad es la de que los Estados Miembro hagan uso de las autorizaciones para regular determinadas materias en el plano nacional que ofrece el RGPD.

El ejemplo más llamativo puede ser el de la edad mínima a partir de la cual los menores pueden otorgar consentimiento para que sus datos sean tratados sin necesitar la autorización de sus padres o tutores. El RGPD fija esa edad en 16 años. Sin embargo, permite a los Estados Miembro que la reduzcan hasta un límite mínimo de 13. Los Estados pueden acogerse o no a esa habilitación, pero lo cierto es que el Reglamento abre una puerta a la diferenciación a nivel nacional en este punto.

Otro caso es el que se refiere a los tratamientos necesarios para atender a obligaciones legales del responsable, la consecución de intereses públicos o el ejercicio de poderes públicos. En todos estos supuestos, el RGPD prevé que los Estados Miembro podrán establecer condiciones específicas para esos tratamientos. Estos tratamientos son los que habitualmente realizan las autoridades públicas y también los que llevan a cabo empresas cuando la legislación les obligue a ello, lo que puede dar una idea del alcance de esta previsión.

En resumen, aunque el RGPD contiene numerosas disposiciones que sí producirán sus efectos y, como tales, serán aplicables directamente por los operadores jurídicos en los Estados Miembro, también incluye otras en que su regulación se verá precisada o complementada por normativa nacional.

En España, algunos de estos desarrollos normativos se han incorporado al Anteproyecto de Ley Orgánica de Protección de Datos (APLOPD) que actualmente se tramita y que reemplazará a la vigente Ley Orgánica 15/99 (LOPD). Otros se incluirán en normas sectoriales.

La sustitución de la todavía vigente LOPD por una nueva norma general de protección de datos es consecuencia de que el derecho europeo exige que los Estados Miembro, por razones de seguridad jurídica, deroguen las disposiciones internas que contradigan lo previsto en un reglamento. Una derogación caso por caso de las disposiciones de la actual LOPD habría constituido un ejercicio complejo, que, en todo caso, habría supuesto también modificar parcialmente algunas de ellas. Por eso se ha optado, como en general han hecho todos los Estados Miembro, por preparar un nuevo texto que derogue íntegramente el vigente.

1.1.3. ÁMBITO DE APLICACIÓN.

El RGPD distingue entre ámbito de aplicación material y territorial.

- **Ámbito material**.

El ámbito material del RGPD es sustancialmente coincidente con el de la Directiva 95/46.

El RGPD se aplica a todos los tratamientos total o parcialmente automatizados de datos y también a los tratamientos no automatizados de datos contenidos o destinados a ser incluidos en un fichero. Esta descripción del ámbito de aplicación es exactamente igual que la de la Directiva del 95. No obstante, en nuestros días los tratamientos que tienen un mayor impacto sobre los derechos de los ciudadanos son los realizados por medios automáticos, mientras que los totalmente manuales son relativamente raros. El hecho de que se haya mantenido la referencia a estos últimos puede considerarse casi como una cláusula de estilo destinada a evitar que algún tratamiento pueda eventualmente escapar de la cobertura del RGPD.

El RGPD no distingue entre tratamientos llevados a cabo por empresas privadas o por autoridades u organismos públicos en lo que a su aplicabilidad se refiere, aunque sí que contiene algunas disposiciones específicas para estos últimos.

Desde otro punto de vista, el RGPD en su Considerando 27 señala expresamente que no será de aplicación a las personas fallecidas, sin perjuicio de que los Estados Miembro puedan establecer normas aplicables a los tratamientos de sus datos personales. Esa posibilidad ha sido tenida en cuenta por el APLOPD, que contiene varios artículos destinados a regular cómo los herederos de la persona fallecida o las personas que ésta haya designado podrán acceder y disponer tanto sobre sus datos personales como sobre sus contenidos digitales.

Quedan excluidos del ámbito de aplicación del RGPD los siguientes tratamientos:

- En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión. Un ejemplo de este tipo de tratamientos sería el de los tratamientos de datos relacionados con la seguridad nacional.

- Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea. Son tratamientos relacionados con la Política Exterior y de Seguridad Común de la UE.

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

  En este punto, el RGPD también retoma la definición de la Directiva 95/46. Esta excepción se refiere a los tratamientos de datos que las personas realizan en el marco de su vida personal y familiar y con fines que podrían describirse como particulares. Ejemplos de este tipo de tratamientos serían las agendas personales o el uso de algún servicio de almacenamiento de fotografías "on line", siempre que ese uso no implique el acceso público a las fotografías almacenadas.

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

Esta excepción se corresponde exactamente con la definición del ámbito de aplicación de la Directiva de Policía que se mencionaba al principio de este capítulo. Dicho en otros términos, el ámbito de aplicación del RGPD finaliza donde comienza el de la Directiva y viceversa.

La interpretación del alcance de esta excepción está dando ya lugar a algunas dudas entre los Estados Miembro.

Como regla general, los tratamientos cubiertos por la excepción son los que llevan a cabo las autoridades policiales en la prevención y persecución de delitos, así como los que se desarrollan en el ámbito judicial penal. Pero hay conductas que son consideradas como un ilícito penal en algunos Estados Miembro mientras que tienen solo la consideración de infracción administrativa en otros. Determinadas conductas relacionadas con la inmigración irregular podrían ser un ejemplo.

Asimismo, en ocasiones puede resultar difícil determinar hasta dónde se aplica cada una de las dos normas cuando un tratamiento puede incluir cuestiones administrativas y faltas o delitos penales. Por ejemplo, las infracciones de tráfico tienen en general la consideración de falta administrativa, pero hay conductas de especial gravedad tipificadas como delitos.

En último extremo, puede haber diferentes interpretaciones sobre qué norma resulta aplicable a determinados tratamientos que pueden ser desarrollados por las autoridades policiales pero cuya incidencia en la prevención o persecución de los delitos es más cuestionable. Ejemplos en este sentido serían los de los tratamientos de datos necesarios para expedir documentos de identidad, o pasaportes, o permisos de armas.

Es de esperar que algunas de estas cuestiones sean resueltas en las normas nacionales que traspongan la Directiva 680/2016. Pero en cualquier caso queda abierta la posibilidad de que el perfil del ámbito de aplicación de la Directiva varíe según los Estados Miembro y, por tanto, que haya también diferencias en los límites del ámbito de aplicación del RGPD.

- **Ámbito territorial.**

El RGPD mantiene uno de los criterios usados por la Directiva para establecer su ámbito territorial de aplicación.

Se trata del criterio del establecimiento en la UE.

Según el artículo 3.1, el RGPD será aplicable 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.

Como se ha dicho, la definición sigue a grandes rasgos la que da la Directiva, aunque con salvedades.

La Directiva, como norma que debía ser traspuesta en cada Estado Miembro, aludía a la aplicabilidad de las normas de cada Estado y las relacionaba con la existencia de un establecimiento en ese Estado. El Reglamento, como norma única para toda la Unión, regula su propia aplicabilidad y lo hace por referencia a todo el territorio de la UE.

Expuesto otro modo, el Reglamento es aplicable siempre que exista un establecimiento en la Unión, con independencia del país en que ese establecimiento esté localizado.

Por otro lado, la definición del RGPD incluye no sólo a los responsables, sino también a los encargados. Algo que no hacía la Directiva. Esta inclusión refleja la diferente aproximación que el RGPD tiene respecto a la posición y obligaciones de los encargados de tratamiento. En la Directiva, el único destinatario de sus disposiciones, con alguna excepción, era el responsable. Se consideraba que el encargado, que en principio actúa solo siguiendo instrucciones del responsable, respondía solo ante él por posibles irregularidades. El RGPD reconoce la evolución de la figura del encargado, que en la actualidad tiene una influencia mucho mayor en la forma en que se desarrollan los tratamientos, por lo que le atribuye expresamente determinadas obligaciones y prevé que posibles incumplimientos, más allá de la responsabilidad que pueda sustanciarse ante el responsable en el marco de la relación contractual que les une, dan lugar también a responsabilidades administrativas.

El Considerando 22 del RGPD repite lo que también decía otro considerando de la Directiva respecto a que la noción de establecimiento implica el ejercicio de manera real y efectiva de una actividad de a través de "modalidades estables". La forma jurídica de esas modalidades, ya sea como sucursal o como filial con personalidad jurídica propia, no son determinantes para valorar la existencia de establecimiento.

Hay que entender que la jurisprudencia del TJUE sobre el ámbito de aplicación de la Directiva sigue siendo válida para el RGPD a la hora de interpretar algunos otros de los conceptos o expresiones que el artículo 3.1 utiliza.

En particular, parece que el Reglamento confirma la posición del TJUE en el caso Google Spain[4]. En esa decisión, el Tribunal concluyó que la expresión "tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable en (el territorio del Estado Miembro)" no exige que ese establecimiento participe en el tratamiento. Para considerar que existe un establecimiento a los efectos de aplicación de la Directiva (y ahora del RGPD) sería suficiente con que la actividad

[4] Sentencia "Google Spain y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González" C-131/12.

que lleva a cabo ese establecimiento esté "indisolublemente asociada" con las actividades de tratamiento. En el caso Google Spain, esa actividad llevada a cabo en España es la de promoción y venta de publicidad del motor de búsqueda, que se considera que es indispensable para que el motor obtenga los beneficios económicos que le permiten seguir en funcionamiento.

Como se ha indicado más arriba, el RGPD parece querer corroborar esta posición, ya que ha añadido la frase "independientemente de que el tratamiento tenga lugar en la Unión o no". Es obvio que si, en contra de la posición del TJUE, fuera necesario que el establecimiento en la Unión tomara parte en el tratamiento, esta última frase no tendría sentido.

Junto con el criterio territorial, el RGPD contiene una importante novedad, que sustituye al criterio de uso de medios situados en un Estado Miembro contenido en la Directiva.

El Reglamento establece su aplicabilidad a responsables o encargados que no estén situados en territorio de la Unión pero que realicen actividades de tratamiento 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 este tenga lugar en la Unión de datos de personas en la Unión.

Con esta disposición, el RGPD pretende asegurar la protección que ofrece a los datos de ciudadanos en la Unión sea cual sea el lugar desde el que el tratamiento de esos datos se lleve a cabo. Una previsión de este tipo es apropiada a las características de los tratamientos de datos en el mundo actual. Hoy no es necesaria la presencia física en un lugar para recoger o procesar los datos de las personas. En el mundo de internet, esas operaciones pueden realizarse a distancia y, en la práctica, muchos servicios de la sociedad de la información están organizados de tal manera que se prestan a todo el mundo desde la sede central de la compañía.

El punto de conexión para esa aplicabilidad es que el tratamiento sea consecuencia de una conducta consciente del responsable o encargado. Esto es evidente en el segundo de los supuestos, donde es el responsable o encargado el que hace un seguimiento del interesado en la Unión a partir, por ejemplo, de su navegación "on line". Es menos claro en lo relativo a la oferta de bienes y servicios. En este caso, la oferta tiene que estar específicamente dirigida a personas en la Unión. No entraría en esta categoría, por ejemplo, una página web de comercio electrónico diseñada para ciudadanos en EEUU y a la que, eventualmente, accede una persona desde la Unión y realiza alguna transacción que da lugar a tratamiento de sus datos.

En esta materia es presumible que sean de aplicación las interpretaciones del Tribunal de Justicia de la UE sobre ley aplicable en contratos transfronterizos. En varias sentencias, el Tribunal ha identificado varios elementos como indicios para establecer si la oferta se dirige a un país concreto. Entre esos elementos estaría el idioma en que se presenta la página web, la moneda en que se pueden retribuir, en su caso, los productos y servicios ofrecidos o el que se dé un teléfono de contacto correspondiente al país en cuestión. En otro terreno, en la ya citada Sentencia Google Spain el Tribunal concedió importancia al hecho de que la publicidad que el motor de búsqueda ofrecía en España estaba dirigida a usuarios españoles.

No es éste el lugar para profundizar en el modo en que se aplicará este nuevo criterio, pero sí puede añadirse que el Reglamento pide a los responsables y encargados que se encuentren en esta situación que designen un representante en la Unión, que será el punto de contacto con interesados y autoridades de supervisión y al que, sin perjuicio de las acciones contra los representados, podrán dirigirse las medidas correctivas que prevé el RGPD en casos de incumplimiento.

1.1.4. DEFINICIONES.

El RGPD también da continuidad a la Directiva en la definición de los conceptos que utiliza.

El artículo 4 del RGPD está dedicado en su totalidad a estas definiciones. Se trata de un artículo largo, con veintiséis definiciones, entre las que se contienen varias ya presentes en la Directiva y otras que son propias de las novedades que se introducen en el RGPD.

Entre las primeras pueden mencionarse las definiciones de dato personal, tratamiento, fichero, responsable, encargado, destinatario, tercero, o consentimiento del interesado.

Con todo, y a pesar de esta continuidad, algunas de estas definiciones presentan matices respecto a la Directiva.

Así, **se define dato personal** como toda información sobre una persona física identificada o identificable («el interesado»), pero el resto de la definición de la Directiva se vincula en el Reglamento a ese interesado, al establecerse que *"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"*.

Es relevante también que el Considerando 30 considera que los identificadores en línea que se proporcionan a los usuarios pueden ser bajo ciertas condiciones considerados datos personales.

El responsable es descrito como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"*, es decir, como quien decide que el tratamiento se lleve a cabo y la forma en que se desarrollará. De nuevo se sigue la definición clásica contenida en la Directiva.

La misma línea se sigue respecto al encargado de tratamiento, *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

En el caso del consentimiento, la definición del RGPD es también idéntica a la Directiva en sus primeras frases. Sin embargo, el Reglamento incorpora un elemento adicional, al señalar que la manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de sus datos personales debe prestarse *"mediante una declaración o una clara acción afirmativa"*. **Esta precisión**

tiene gran calado, ya que excluye que el consentimiento pueda otorgarse mediante la inacción, como puede suceder con algunas modalidades en que el responsable informa al interesado de que procederá a tratar sus datos si éste no manifiesta su disconformidad en un plazo determinado.

Junto a estas definiciones, ya clásicas en el derecho europeo, el RGPD contiene, como se ha señalado, otras que reflejan las novedades que en él se incluyen, **y que son:**

- **Seudonimización:**

"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").

- **Elaboración de perfiles:**

"toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".

En ambos casos, el RGPD utiliza estos conceptos a lo largo del texto. La seudonimización se considera fundamentalmente una medida de seguridad en el tratamiento de datos personales, pero los Considerandos 26, 28 y 29, se refieren también a que su uso puede ayudar a los responsables a cumplir con sus obligaciones.

Es importante destacar que el RGPD considera explícitamente que los datos seudonimizados son datos personales y que por tanto están sujetos a sus disposiciones.

La noción de perfilado se utiliza también en el RGPD en relación con el derecho de oposición, el derecho a no ser objeto de decisiones automatizadas y la información que debe proporcionarse a los interesados. Se trata de un concepto que, aunque antiguo, ha cobrado enorme relevancia en la medida en que cada vez son más numerosos, y con mayores efectos sobre los ciudadanos, los tratamientos basados en la elaboración de perfiles. Por citar solo algunos ejemplos podría hablarse de la publicidad conductual (basada en perfiles de navegación on line), los perfiles de solvencia crediticia, o los perfiles que pueden realizarse con el uso de tecnologías de "big data" o análisis masivo de información.

El RGPD incluye también definiciones de las dos nuevas categorías de datos sensibles que añade a la lista de la Directiva del 95: datos genéticos y datos biométricos.

- **Datos genéticos:**

"*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*".

Los datos genéticos ya tenían la consideración de datos especialmente protegidos en el marco de la Directiva, pero solo como parte de los datos relacionados con la salud. El RGPD los separa como categoría con entidad propia, al margen de su implicación en el terreno de la salud, con lo que extiende la protección especial a tratamientos relacionados, por ejemplo, con la filiación.

- **Datos biométricos**.

"*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*".

Respecto a esta definición hay que señalar que los datos biométricos tendrán la condición de datos sensibles solo cuando sean utilizados para identificar unívocamente a una persona. Una fotografía, por ejemplo, contiene datos biométricos, pero su tratamiento no está sometido a especiales condiciones salvo que se utilice para individualizar o identificar a alguien dentro de un colectivo más amplio.

También hay que indicar que la noción de dato biométrico es muy amplia e incluye aspectos cada vez más innovadores. Se consideran datos biométricos en la medida en que permiten identificar a una persona aspectos como la huella de la oreja, el patrón venoso de una mano o la forma de caminar de una persona.

Es también novedad la definición de "violación de seguridad de los datos personales". Este concepto hace alusión a incidentes relacionados con la seguridad de los datos objeto de tratamiento e incluye cualquier evento que *"ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos"*.

La definición está tomada de la Directiva 2002/58, citada al principio de este capítulo, ya que hasta ahora la notificación a autoridades de control e interesados de las violaciones, o quiebras de seguridad, como se denominan frecuentemente, sólo era obligatoria en el sector de las comunicaciones electrónicas. El Reglamento hace esta obligación aplicable a todo tipo de tratamientos.

Algunas de las nuevas definiciones del RGPD están directamente vinculadas con el mecanismo de cooperación o "ventanilla única", se desarrollarán con más detalle en el módulo 5. Son definiciones de conceptos como "tratamiento transfronterizo", "establecimiento principal", "autoridad de control interesada" u "objeción pertinente y motivada".

1.1.5. PRINCIPIOS.

Los principios del tratamiento constituyen el fundamento del sistema europeo de protección de datos, tal y como se formulan, y son lo que le diferencia de otros modelos de protección de datos o privacidad.

Los principios que el RGPD enuncia son en esencia los mismos que ya enumera la Directiva 95/46, pero presenta, igual que sucedía con el ámbito de aplicación o las definiciones, algunas novedades frente a esta última. Es también una característica nueva en el RGPD que "pone nombre" a los principios. La Directiva se limitaba a exponerlos, mientras que en el RGPD cada principio tiene asignada una denominación propia que, en general, se corresponde con el modo en que se han identificado comúnmente en la doctrina, la jurisprudencia y la actuación de los operadores y de las autoridades de protección.

Un primer principio es el de "licitud, transparencia y lealtad", que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.

La licitud en el tratamiento se relaciona con la necesidad de que esté amparado en una de las bases jurídicas que establece el Reglamento. Los datos no pueden ser tratados simplemente porque estén disponibles o porque el responsable entienda que recopilándolos y procesándolos podrá encontrarles alguna utilidad presente o futura. El principio reconoce que el derecho a la protección de datos implica que los datos solo pueden ser tratados con el consentimiento del interesado o cuando la ley lo permita porque existan motivos que justifiquen que esa voluntad del interesado deba ceder ante otros derechos o intereses.

Es preciso identificar un propósito para el tratamiento (esa identificación se integra en el principio de "limitación de la finalidad" del que luego se hablará) y que ese tratamiento, con esa finalidad, sea necesario para conseguir alguno de los objetivos que el artículo 6.1 del Reglamento considera que permiten legitimar un tratamiento o que el interesado consienta en que éste se lleve a cabo. Por ejemplo, el tratamiento de datos puede resultar necesario para la ejecución de un contrato, o para que un organismo público pueda ejercer sus poderes o satisfacer un interés público.

Al mismo tiempo, el principio excluye el que los datos sean tratados de forma desleal para con el interesado o sin proporcionarle la información necesaria para que entienda el objeto y fines del tratamiento, sus consecuencias y posibles riesgos, y pueda, en su caso, decidir sobre él. El principio impide, por ejemplo, que se oculte alguna finalidad del tratamiento, o que esa finalidad se exprese de forma vaga y confusa. También tiene una dimensión positiva, que obliga a los responsables a buscar la mayor transparencia en sus relaciones con los interesados.

Este aspecto del principio de "licitud, lealtad y transparencia" tiene su correlato en las disposiciones del RGPD que determinan qué información debe proporcionarse al interesado, en qué forma y en qué momentos, así como en las que regulan el modo en que debe responderse a las solicitudes de ejercicio de derechos.

El segundo de los principios que formula el RGPD es el de "limitación de la finalidad". En realidad, este principio tiene dos partes.

Por un lado, obliga a que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas. Este principio se relaciona estrechamente con el anterior. La finalidad del tratamiento ha de estar claramente definida. En ocasiones se encuentran finalidades del tipo "sus datos serán tratados para mejorar su experiencia como usuario". Estas definiciones no se ajustan al principio de finalidad. Es posible que las finalidades sean descritas de un modo amplio, pero siempre que una descripción de ese tipo permita al interesado o a las autoridades de control conocer qué tipo de actividades se incluyen en ella.

Dentro de esta primera parte del principio se encuentra también el hecho de que las finalidades han de ser legítimas, entendiéndose como tales todas las que están permitidas por el ordenamiento jurídico. En ese sentido, finalidades que resulten ilegales, como sería por ejemplo discriminar en el acceso a un puesto de trabajo a personas solteras, o casadas, o a personas de una determinada confesión religiosa, nunca pueden servir como base para el tratamiento de los datos.

La segunda parte del principio es la que le da nombre, ya que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines. En la interpretación que se hace de esta parte del principio, se entiende que lo que no es posible es tratar los datos recogidos para una finalidad con fines que no sean compatibles con ella.

El RGPD no impide que los datos sean tratados con finalidades distintas de la que justificó el tratamiento originario, lo que prohíbe es tratamientos para fines no compatibles.

El RGPD, en su artículo 6.4 ofrece una serie de criterios a tener en cuenta para determinar la compatibilidad de esos fines ulteriores, si bien no da una definición precisa de cuáles son los rasgos que los caracterizarían. Sin embargo, y siguiendo lo que ya dispone la Directiva 95/46, sí menciona cuatro casos de finalidades que se consideran siempre compatibles. Son los de archivística en interés público, investigación científica e histórica y fines estadísticos.

El principio de "minimización de datos" es también heredero de las previsiones de la Directiva, aunque mientras que en ésta se describía diciendo que sólo serán tratados los datos "adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados", el Reglamento sustituye la expresión "no excesivos" por la de "limitados a lo necesario". Se trata de un matiz que precisa y refuerza el contenido del principio. No es posible, según este principio, recabar y tratar datos simplemente por si pudieran resultar útiles o "por tenerlos". Si para una finalidad determinada no es necesario que el responsable conozca las pautas de navegación de un usuario, no podrá hacer ese seguimiento.

Los datos, según el "principio de exactitud", deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.

Este principio tiene importancia por el hecho de que de muchos tratamientos de datos se derivan decisiones que pueden afectar, en ocasiones de forma significativa, a los derechos o intereses de los titulares de los datos. Un ejemplo muy simple sería el de que la compañía suministradora de electricidad o gas mantenga datos erróneos sobre sus clientes. Las consecuencias podrían ir desde no proporcionar el servicio que se ha contratado hasta emitir facturas a los clientes equivocados.

El principio de "limitación del plazo de conservación" está relacionado con el de minimización. En cierto modo, podría describirse como un principio de minimización temporal en el tratamiento de datos. Igual que solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

No obstante, hay casos en que es posible mantener los datos por más tiempo del necesario para la consecución de la finalidad originariamente perseguida. El RGPD menciona los casos de tratamientos ulteriores con fines de archivística en interés público, investigación científica e histórica y fines estadísticos. También es posible que los datos sean conservados para el cumplimiento de una obligación legal del responsable, o para que el responsable pueda ejercer acciones legales. Esas excepciones están recogidas en el artículo 17.3 del Reglamento.

Un último principio es el de "integridad y confidencialidad". Este principio es nuevo en el RGPD y no se mencionaba en la Directiva. Básicamente, impone a quienes tratan datos la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

Fuera del listado de principios que se recogen en el artículo 5 del RGPD se encuentra un principio denominado de "responsabilidad proactiva", expresión que pretende traducir el término inglés "accountability".

Este principio se describe no en el propio artículo 5, sino en el artículo 24, según el cual *"teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento"*.

El principio tiene una doble lectura. Por un lado, confirma algo que también estaba presente en la Directiva, como es que **la responsabilidad última por la forma en que se traten los datos atañe al responsable**. Es el responsable el que decide que se inicie un tratamiento, su finalidad, los datos que van a ser tratados y cuáles son las actividades de tratamiento que se van a realizar. Es, por tanto, el responsable, que toma las decisiones que determinan la existencia del tratamiento, el que debe ocuparse de que se lleve a cabo adecuadamente y asumir las responsabilidades correspondientes en caso de que ello no suceda.

Aunque el RGPD, como se ha indicado, prevé también obligaciones y responsabilidades para los encargados, esas previsiones no afectan a este principio general, ya que se refieren a aspectos concretos dentro del contexto general del tratamiento y no a su consideración como un todo.

La segunda interpretación del artículo se refiere al modo en que el responsable ha de afrontar su papel. El RGPD no se limita a situar la responsabilidad sobre un responsable pasivo, que deberá hacer frente a las consecuencias de posibles infracciones.

El RGPD adopta un enfoque proactivo, exigiendo que el responsable adopte medidas preventivas dirigidas a reducir los riesgos de incumplimiento y, además, que esté en condiciones de demostrar que ha implantado esas medidas y que las mismas son las adecuadas para lograr la finalidad perseguida.

1.2. LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.

1.2.1. INTRODUCCIÓN.

El punto de partida para el tratamiento de datos personales es determinar la base jurídica que permite realizar lícitamente las distintas operaciones de tratamiento definidas en el artículo 4.2 del Reglamento (UE) 2016/679, General de Protección de Datos (RGPD) que recoge las siguientes:

- "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.

Base jurídica que puede ser común o distinta para cada una de ellas.

En este punto la sistemática de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) ha inducido a una cierta distorsión al establecer como base jurídica general el consentimiento de los afectados, configurando las restantes bases jurídicas como excepciones a este principio general.

El RGPD parte de una sistemática distinta al enumerar en su artículo 6 las diversas bases jurídicas que legitiman el tratamiento de datos personales en términos de igualdad. Su redacción es la siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del

interesado que requieran la protección de datos personales, en particular cuando el interesado sea"

Si bien el propio RGPD establece modulaciones sobre algunas de ellas, como posteriormente se indicará.

A continuación se analiza cada una de ellas conforme a la sistemática del precepto, si bien debe atenderse de forma específica a las letras c) y e) que se tratarán conjuntamente por ser la base jurídica más habitual para el tratamiento de datos por parte de las Administraciones públicas.

1.2.2. EL CONSENTIMIENTO.

El RGPD define el consentimiento como una manifestación de voluntad libre, específica, informada e inequívoca (art.7).

Manifestación de voluntad por la que el afectado acepta el tratamiento mediante una declaración o una clara acción afirmativa.

Los considerandos del RGPD ofrecen algunas aclaraciones sobre la prestación válida del consentimiento que se describen a continuación:

- Se considera que puede existir un acto afirmativo claro en supuestos como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (Considerando 32).

- También puede considerarse un acto afirmativo 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 (Considerando 32).

- Por tanto, el silencio, las casillas premarcadas o la inacción del afectado no constituyen un consentimiento válido (Cdo.32).

- En el caso de que el tratamiento tenga varios fines deberá prestarse para cada uno de ellos (Cdo.32).

- No obstante, sería posible agrupar varias finalidades en virtud de su vinculación (por ejemplo, consentimiento para la recepción de publicidad propia o de terceros).

- Pero deberían desagregarse cuando los tratamientos impliquen conductas distintas (por ejemplo, tratamiento por quien recaba los datos y cesión a terceros).

- En el caso de que en el marco de un contrato se solicite el consentimiento para una finalidad que no guarde relación con su objeto, el Anteproyecto de LOPD establece que deberá garantizarse que el afectado pueda manifestar

específicamente su voluntad mediante un procedimiento sencillo y gratuito (p.ej. una casilla específica no premarcada).

Mención especial requiere la exigencia de que el consentimiento sea libre ya que el RGPD recoge algunas aclaraciones sobre supuestos en los que puede considerarse que no se cumple esta condición.

En este sentido el Considerando 42 señala que:

"*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*".

Por su parte, el Considerando 43 añade que:

"*Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular".*

Y presume que:

"el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento".

No obstante, el RGPD no implica necesariamente una obligación de recabar un nuevo consentimiento si el que se hubiera obtenido antes de su aplicación fuese conforme a los requisitos que establece.

En ningún caso hay aplicación retroactiva, dado que las normas del RGPD no se aplican a tratamientos anteriores al momento en que produce plenos efectos.

Siguen siendo válidos los consentimientos expresos y los consistentes en una manifestación o clara acción afirmativa.

El todavía vigente Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), admite la posibilidad de obtener un consentimiento basado en la inactividad del afectado. Se trata de aquellos casos en que el responsable del tratamiento ha obtenido lícitamente los datos personales y quiere obtener el consentimiento para otra finalidad, normalmente la de realizar publicidad. Para ello puede dirigirse al afectado informándole en los términos recogidos en el artículo 5 de la LOPD, concediéndole un plazo de treinta días para manifestar su negativa al tratamiento y advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente (art. 14 RLOPD).

Los consentimientos obtenidos por este procedimiento con anterioridad a la aplicación efectiva del RGPD, el 25 de mayo de 2018, no serán válidos al señalar el Considerando 171, a sensu contrario, que únicamente mantendrán su validez los consentimientos anteriores que se ajusten a las previsiones

del Reglamento que, como se ha señalado, exige una declaración positiva o una clara acción afirmativa.

Por tanto, para que el tratamiento de estos datos personales sea lícito deberá obtenerse un nuevo consentimiento conforme con las previsiones del RGPD o acudir a alguna otra base jurídica para el tratamiento de los mismos, como puede ser el interés legítimo del responsable en los términos que se indican posteriormente.

Respecto del consentimiento de los menores de edad el RGPD prevé que el consentimiento sólo se considerará lícito si el menor fuera mayor de 16 años o si, siendo menor de esa edad, el consentimiento es prestado por los titulares de la patria potestad o la tutela.

Esta regla general puede modificarse por el derecho de los Estados miembro rebajando la edad hasta un mínimo de 13 años. Esta opción ha sido la recogida en el Anteproyecto de Ley Orgánica de Protección de Datos que sustituya a la vigente LOPD, si bien puede tener excepciones en los casos en que se establezca otra edad para la celebración de actos o negocios jurídicos en cuyo contexto se recaba el consentimiento o en normativas sectoriales como puede ser la sanitaria.

En todo caso, recae en el responsable del tratamiento de los datos la prueba de que cuenta con el consentimiento del afectado y de que ha sido prestado a través de medios que resulten pertinentes.

En el caso del consentimiento prestado por menores el responsable está obligado a realizar esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

El consentimiento es esencialmente revocable debiendo informarse al afectado de esta posibilidad. La revocación del consentimiento debe poder realizarse por procedimientos tan sencillos como los utilizados para obtenerlo, pero no tiene efectos retroactivos, no afectando a la licitud de los tratamientos realizados hasta ese momento.

1.2.3. LA RELACIÓN CONTRACTUAL.

En relación con esta base jurídica como legitimadora del tratamiento de los datos personales el RGPD es particularmente escueto tanto en el articulado como en los considerandos limitándose a establecer en su artículo 6.1.b) que será lícito el tratamiento *"necesario para la ejecución de un contrato en el que el interesados es parte o para la aplicación a petición de éste de medidas precontractuales"*.

1.2.4. TRATAMIENTOS NECESARIOS PARA EL CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL O PARA EL CUMPLIMIENTO DE UNA MISIÓN REALIZADA EN INTERÉS PÚBLICO O EN EL EJERCICIO DE PODERES PÚBLICOS.

La base jurídica del tratamiento de datos personales por parte de las administraciones públicas será, como regla general, la contemplada en el artículo 6.1.c) y e) del RGPD.

Respecto de estas bases jurídicas el RGPD prevé que deben ser establecidas por el derecho de la Unión o de los Estados miembro.

Adicionalmente señala que la finalidad del tratamiento para el cumplimiento de una obligación legal debe quedar determinada en la norma que la establezca. Y que la finalidad del tratamiento para el cumplimiento de una misión de interés público o para el ejercicio de poderes debe ser necesaria para el cumplimiento o ejercicio de los mismos.

El Considerando 45 aclara que una misma norma puede ser suficiente como base para varias operaciones de tratamiento.

Con el fin de garantizar adecuadamente el derecho a la protección de datos conforme al RGPD la norma puede incluir disposiciones específicas tales como las condiciones generales que rigen la licitud del tratamiento, los tipos de datos objeto de tratamiento, los afectados, las entidades a las que se pueden comunicar los datos y la finalidad de la cesión, la limitación de la finalidad, los plazos de conservación de los datos o las operaciones y procedimientos del tratamiento. En todo caso, el tratamiento deberá ser proporcional a los objetivos de interés público perseguidos.

Respecto de la norma que incorpora estas bases jurídicas, el Anteproyecto de LOPD establece que deberá ser una ley.

Cuando el tratamiento se realice en el ejercicio de poderes públicos el responsable del mismo debe ser una autoridad pública u otra persona física o jurídica de interés público.

Y si se realiza para el cumplimiento de misiones de interés público el responsable podrá ser también una persona de derecho privado (Considerando 45).

El artículo 5.1.b) del Reglamento establece la regla general de que el tratamiento de datos se realice para fines determinados, explícitos y legítimos. No obstante, admite que puedan tratarse con fines que no sean incompatibles con los iniciales y cita expresamente entre ellos tratamientos que pueden ser propios de las administraciones públicas como son los fines de archivo de interés público, así como los de investigación científica e histórica o los estadísticos.

Ahora bien, el tratamiento de datos para estas finalidades deberá estar sujeto a garantías adecuadas para garantizar los derechos y libertades de los afectados conforme al Reglamento. Entre ellas deberán adoptarse medidas técnicas y organizativas para respetar el principio de minimización de los datos.

Entre estas medidas el artículo 89.1 del RGPD cita específicamente la pseudonimización de los datos y, también, su anonimización siempre que permita la consecución de estos fines.

En el caso de los tratamientos con fines de investigación científica o histórica el RGPD prevé que una norma europea o nacional pueda establecer excepciones a los derechos de acceso, rectificación, limitación del tratamiento y oposición, cuando sea probable que imposibiliten u obstaculicen gravemente el logro de los fines mencionados y se establezcan garantías adecuadas en los términos señalados anteriormente.

En cuanto al tratamiento con fines estadísticos podrán establecerse, además de las mencionadas anteriormente, excepciones al derecho de que el responsable del tratamiento comunique a los cesionarios de los datos las rectificaciones o supresiones que haya realizado o la limitación del tratamiento de los datos. Y al derecho a la portabilidad.

Sin embargo, cuando el tratamiento para los fines indicados pueda servir también para otras finalidades, las excepciones a los derechos sólo serán aplicables respecto de aquellos.

1.2.5. EL INTERÉS VITAL.

El tratamiento de datos personales es lícito cuando sea necesario para proteger intereses vitales del interesado o de otra persona física (art. 6.1.d).

El RGPD no recoge una definición de interés vital, si bien el Considerando 46 parece apuntar a una interpretación restrictiva al señalar que debe tratarse de "un interés esencial para la vida del interesados o de otra persona".

El mismo considerando atribuye, además, a esta base jurídica para el tratamiento un carácter que podría calificarse como subsidiario, al indicar que la misma únicamente debe aplicarse cuando el tratamiento no puede basarse en otra base jurídica distinta. En este sentido cita como ejemplos el tratamiento con fines humanitarios, incluido el control de epidemias y su propagación o las situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

1.2.6. EL INTERÉS LEGÍTIMO.

El RGPD, en términos similares a la Directiva 95/46/CE incluye el interés legítimo del responsable o de un tercero como base jurídica para el tratamiento de datos personales (art.6.1.f).

No obstante, para ello no basta con la concurrencia de un interés legítimo sino que es necesario que prevalezca sobre los intereses, derechos o libertades fundamentales del interesado.

Por tanto, será necesario realizar en cada caso concreto una ponderación para poder determinar la prevalencia o no del interés legítimo. Ponderación que deberá tener en cuenta no sólo la incidencia del tratamiento en los derechos y libertades del afectado, sino también en sus propios intereses. El RGPD exige que esa ponderación sea especialmente cualificada cuando el afectado sea un menor.

El RGPD refuerza algunas de las garantías para el tratamiento de datos personales cuando su base jurídica sea el interés legítimo. Así, en relación con el deber de informar al interesado sobre el tratamiento de los datos, exige no sólo que se indique el interés legítimo como base jurídica del tratamiento de la que debe informarse en todo caso, sino además que se especifiquen los intereses legítimos concretos del responsable o del tercero que lo realizaran, tanto si los datos se han obtenido del afectado como si no ha sido así (arts. 13.1.d y 14.2.b).

Adicionalmente, el RGPD refuerza el derecho a oponerse en cualquier momento al tratamiento de datos personales por motivos relacionados con su situación personal, cuando su base jurídica sea el interés legítimo, estableciendo que el responsable dejará de tratar los datos personales salvo que acredite "motivos legítimos imperiosos" que prevalezcan sobre los intereses, derechos y libertades del afectado (art. 21.1).

Los considerandos 47 a 49 recogen algunas aclaraciones sobre esta base jurídica.

El Considerando 47 aclara que el interés legítimo puede ser una base jurídica no sólo del responsable que trata los datos sino también de un responsable del tratamiento al que se puedan comunicar los datos personales.

Asimismo, establece un punto de partida sobre la ponderación, a la que anteriormente se hizo referencia, al relacionarla con las expectativas razonables de los afectados basadas en su relación con el responsable del tratamiento, citando como ejemplos las situaciones en las que el afectado es cliente o está al servicio del responsable.

No obstante, exige que se realice una evaluación meticulosa de la ponderación, incluso si el afectado puede prever de forma razonable, en el momento y en el contexto de la recogida de los datos personales, que puede producirse un tratamiento para una determinada finalidad.

En particular, el Reglamento señala que cabe apreciar la prevalencia de los intereses y derechos del afectado cuando se proceda al tratamiento de sus datos en circunstancias en que no espere razonablemente que vaya a realizarse un tratamiento ulterior (p.ej. cesiones ulteriores de los datos).

Los citados considerandos recogen algunos ejemplos de intereses legítimos, aunque sin considerarlos por sí mismos como prevalentes.

Entre ellos se citan los siguientes:

- La prevención del fraude, siempre que se cumpla el principio de minimización (Considerando 47);
- El marketing directo (Considerando 47);
- Las transmisiones de datos en grupos de empresas para fines administrativos internos como puede ser la centralización de datos de clientes o empleados (Considerando 48);
- Las transmisiones de datos para garantizar la seguridad de las redes (p.ej. a los equipos de respuesta a emergencias informáticas – CERT – o de respuesta a incidentes de seguridad informática – CSIRT–), para impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas (Considerando 49).

El Anteproyecto de LOPD recoge una previsión de gran importancia al establecer que una ley puede considerar que un tratamiento fundado en el interés legítimo del responsable o de un tercero prevalece sobre los derechos del afectado. En cuyo caso, no sería necesario que los responsables que tratan los datos tengan que realizar una ponderación adicional.

Finalmente, el Reglamento establece que el interés legítimo no puede ser una base jurídica aplicable a los tratamientos realizados por las autoridades públicas en el ejercicio de sus funciones, al señalar que es el propio legislador el que debe establecer por ley la base jurídica para el tratamiento de datos por parte de las autoridades públicas, por lo que el interés legítimo no debe aplicarse al tratamiento realizado por ellos en el ejercicio de sus funciones.

1.3. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS (DATOS ESPECIALMENTE PROTEGIDOS).

El RGPD incluye en el concepto de categorías especiales de datos los denominados datos especialmente protegidos en la LOPD como son las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los que revelen el origen racial o étnico, y los relativos a la salud o a la vida u orientación sexual de una persona.

Pero incorpora **nuevas categorías de datos como son los datos genéticos y los datos biométricos**. El RGPD, como ya hemos visto al principio de este módulo al referirnos a las definiciones, considera como **datos genéticos**, *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, como **datos biométricos**, *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*.

Respecto de estos últimos el Considerando 51 recoge una aclaración sobre el tratamiento de datos de fotografías señalando que no debe considerarse sistemáticamente un tratamiento de categorías especiales de datos personales, 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.

Asimismo el RGPD prevé especialidades para el tratamiento de datos de condenas, medidas de seguridad e infracciones penales, que no son considerados estrictamente datos sensibles, pero respecto de los cuales se establecen limitaciones para su tratamiento.

Estas categorías de datos sólo podrán tratarse bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembro que establezca garantías adecuadas para los derechos y libertades de los interesados.

Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

A este respecto, el artículo 20 del Anteproyecto de LOPD reconoce la competencia exclusiva del Ministerio de Justicia para la llevanza de un registro que recoja la totalidad de los datos relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas.

La regla general contemplada en el Reglamento es la prohibición del tratamiento de categorías especiales de datos (art. 9).

No obstante, se recoge un amplio abanico de excepciones a esta regla general como son las siguientes:

"*a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Como motivos de interés público amparado en habilitaciones legales que exceptúan la prohibición, el propio RGPD recoge expresamente los siguientes supuestos:

- *"El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social"*.

Sobre los tratamientos realizados con las finalidades citadas se prevé que el tratamiento se realice por un profesional sujeto a deber de secreto o bajo su responsabilidad, así como por cualquier otra persona sujeta a la obligación de secreto:

- *"El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios"*.

- *"El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos".*

Finalmente, se admite que los Estados miembro puedan mantener o introducir condiciones adicionales, incluidas limitaciones, sobre los tratamientos de datos genéticos, biométricos o de salud.

El Anteproyecto de LOPD incorpora algunas previsiones sobre las categorías especiales de datos.

Partiendo de la posibilidad admitida por el RGPD de que el derecho de los Estados miembro puedan establecer que el consentimiento del afectado no permita excepcionar la prohibición de tratar datos sensibles (art. 10.2.a in fine), el Anteproyecto establece que no bastará para levantar la prohibición cuando la finalidad principal del tratamiento de los datos sea identificar la ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico de los afectados (art. 10.1). Con esta previsión se pretende establecer una regla equivalente a la prevista en el artículo 7.4 de la vigente LOPD que prohíbe los ficheros creados con la finalidad exclusiva de almacenar las categorías de datos que se han citado ni siquiera contando con el consentimiento de los afectados.

Por su parte, el artículo 10.2 del Anteproyecto incluye una referencia específica sobre el tratamiento de datos de salud estableciendo que *"la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada y de los seguros de asistencia sanitaria".*

Por último, el artículo 20 reitera el principio de reserva de ley o de una norma de derecho comunitario para los datos de naturaleza penal.

La vigente LOPD establece un régimen reforzado de protección para los datos relativos a las infracciones y sanciones administrativas al calificarlas como datos especialmente protegidos.

El RGPD no contempla una previsión similar. Sin embargo, el Anteproyecto de LOPD, en aplicación del principio de minimización de datos regulado en el artículo 5.1.c) del RGPD y, en congruencia con las garantías contempladas en el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, establece que el tratamiento de los citados datos sean realizados por los órganos competentes para la declaración de infracciones y la imposición de sanciones, limitándose su tratamiento a los estrictamente necesarios para la finalidad perseguida por ellos.

En cualquier otro supuesto el tratamiento deberá estar autorizado por una ley en la que se incluyan, en su caso, garantías adicionales para los derechos y libertades de los afectados.