

DESARROLLO DE COMPETENCIAS AVANZADAS PARA LA APLICACIÓN DE LA PROTECCIÓN DE DATOS EN LA JUNTA DE ANDALUCÍA

UNIDAD 1

Aspectos introductorios de la regulación del derecho fundamental a la protección de datos en el ámbito europeo y nacional. Principios en la protección de datos. Legitimidad. Protección de datos desde el diseño y por defecto. Derechos en materia de protección de datos.

CONTENIDOS

1. INTRODUCCIÓN	3
2. CONCEPTOS BÁSICOS	4
3. PRINCIPIOS EN LA PROTECCIÓN DE DATOS.....	10
3.1. PRINCIPIOS RELATIVOS AL TRATAMIENTO	10
3.2. LEGITIMIDAD	12
4. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO.....	15
5. DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS	17
5.1. DERECHO DE ACCESO DEL INTERESADO (ARTÍCULO 15).....	17
5.2. DERECHO DE RECTIFICACIÓN (ARTÍCULO 16).....	19
5.3. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO») (ARTÍCULO 17).....	20
5.4. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ARTÍCULO 18).....	21
5.5. DERECHO A LA PORTABILIDAD (ARTÍCULO 20)	21
5.6. DERECHO DE OPOSICIÓN (ARTÍCULO 21)	21
5.7. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES (ARTÍCULO 22).....	22
6. CONCLUSIONES DE LA UNIDAD 1	24



Este curso ha sido cedido por la Agencia Española de Protección de Datos por medio de una licencia Creative Commons Reconocimiento-No comercial-Compartir igual, en los términos que se describen en <http://creativecommons.org/licenses/by-nc-sa/3.0/es> o texto oficial que, para esta modalidad de licencia, sustituya al indicado.

1. INTRODUCCIÓN

En este curso vamos a encontrar una profundización en algunos de los temas que se abordan desde el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, así como tratar algunas cuestiones que no han sido abordadas en acciones formativas anteriores, en concreto en el curso en modalidad de formación abierta denominado "Protección de datos en la práctica"¹ así como el curso en modalidad tutorizada denominado "Aplicación práctica en materia de protección de datos en la Junta de Andalucía" (sujeto a convocatoria).

Los dos cursos citados pueden considerarse como anteriores al que ahora se inicia, siendo recomendable haberlos realizado, lo que no impide el aprendizaje y la participación en esta actividad formativa, ya que este primer bloque de contenido pretende dar una visión general de la protección de datos personales, a través de distintos conceptos básicos definitorios que deben conocerse y son fundamentales para entender así como aplicar esta materia, pero también otros aspectos que deben tenerse siempre en cuenta cada vez que se haga el análisis de una cuestión desde la protección de los datos personales.

En todo caso, se recomienda tener al alcance para su consulta tanto el Reglamento General de Protección de Datos², como la Ley Orgánica 3/2018, de 5 de diciembre³, de tal modo que pueda hacerse la lectura completa de aquellos artículos a los que se vaya haciendo referencia a lo largo de la unidad.

¹ Curso de formación abierta "Protección de datos en la práctica". Instituto Andaluz de Administración Pública.

<https://moodle.iaap.junta-andalucia.es/mod/page/view.php?id=154270#tab-62d00c09d50991>

² 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).

<https://boe.es/doue/2016/119/L00001-00088.pdf>

³ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

<https://boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf>

[illegible]

DATOS PERSONALES

Como puede verse en la propia definición, podemos encontrar una serie de tipos de datos que serán los más habituales (nombre y apellidos, por ejemplo) y que son esos que nos permiten identificar con facilidad a una persona, pero habrá que prestar especial atención a aquella otra información, que por ser muy específica en un contexto o aplicable a una persona también nos permita identificarla, como

puede ser un apodo, por ejemplo. Por ello, saber si un dato puede considerarse como dato personal requiere en todos los casos un análisis que nos ayude a entender sobre su naturaleza.

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;

Esta definición nos muestra que prácticamente cualquier acción que se haga con los datos personales, incluso su destrucción, supone un tratamiento, por lo que deberá tenerse en cuenta lo que se hace con los datos personales cuando se definan los encargos de tratamiento, los ciclos de vida de los datos y cualquier procedimiento que se establezca en su gestión.

LIMITACIÓN DEL TRATAMIENTO

El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

Este concepto nos recuerda la necesidad de reflexionar sobre los datos y la “vida” de los mismos, cuestión muy relacionada con la protección de datos desde el diseño (que veremos en el punto 4). Una vez determinada la necesidad de desarrollar una actividad de tratamiento debemos tener conciencia que ello también supone definir qué se hará con esos datos personales en un futuro una vez que hayan cumplido su finalidad principal, como por ejemplo en el caso de las subvenciones, que una vez se haya concedido una ayuda y finalizado el trámite de justificación, así como transcurridos todos los plazos para posibles recursos (administrativos o judiciales), debemos actuar sobre esos datos personales, explicado de un modo general.

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 este caso el concepto, más allá de su propia definición, tiene como destacables dos aspectos: el primero de ellos es que el tratamiento debe realizarse de manera automatizada, es decir, a través de sistemas informáticos preparados para ellos; y por otra parte que sirve para tener una “imagen” de la persona sobre una cuestión concreta que podrá tendrá consecuencias posteriores.

SEUDONIMIZACIÓN

el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;”

Esta cuestión, que se incorpora como nuevo concepto, se considera fundamentalmente una medida de seguridad en el tratamiento de datos personales, pero en los Considerandos 26, 28 y 29 también se recogen como un elemento que puede ayudar a los responsables de tratamiento a cumplir con sus obligaciones. Un claro ejemplo de ello es cuando se acude a una visita médica y una vez identificada la persona pendiente de ser atendida se le asigna un código que suele ser aleatorio (habitualmente de números y letras), de tal modo que solamente es posible saber de quien se trata si tenemos ese código a través del sistema que lo ha generado, es decir, es necesaria esa información adicional para poder identificar a la persona.

FICHERO

Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;”

Este concepto, que ya procede de normativa anterior, hace referencia a la organización de los datos personales según unos criterios específicos. Un ejemplo de reparto funcional o geográfico lo encontramos cuando en una línea de ayudas definida desde la Dirección General competente en la materia (que actuaría como responsable) y desarrollada una aplicación para su gestión en los Servicios Centrales, se determina que las solicitudes y su gestión se hará de manera provincializada. En este caso encontramos que el “fichero” afectaría a los datos personales de quienes participen de la subvención, de quienes soliciten, pudiendo ser tratados los mismos tanto en los Servicios Centrales como a través de las Delegaciones Territoriales.

RESPONSABLE DEL TRATAMIENTO O RESPONSABLE

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;”

Siguiendo la definición que podemos encontrar en la normativa anterior al RGPD, la determinación del responsable es un elemento importante dado que le corresponde determinar los fines y los medios, es decir, definir la actividad de tratamiento, decidir cuáles serán los datos a tratar, qué medios deberán utilizarse para su gestión, las medidas de seguridad que deben adoptarse, ... Es decir, es en el responsable donde recae prácticamente toda la decisión sobre el tratamiento de los datos. Y es destacable que aunque suele ser habitual en la administración que el responsable es una figura centrada en una única persona (alto cargo que debe desarrollar las funciones que se le atribuyen a través de una norma específica o mediante un decreto de estructura) también es posible que para una actividad de tratamiento exista más de un responsable, en cuyo caso hablamos de “corresponsable del tratamiento”, de tal modo que cada responsable lo será de la parte que le corresponda pero de manera conjunta sobre una misma actividad de tratamiento.

ENCARGADO DEL TRATAMIENTO O ENCARGADO

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;”

Parece que la definición es clara, se trata de aquél que hace un tratamiento de datos para el responsable. Es fundamental saber diferenciar entre responsable y encargado de tratamiento, cuya

relación deberá estar determinada de algún modo admitido desde el ámbito jurídico y/o administrativo -admitido en derecho- (un contrato, una resolución, un encargo a medio propio,...) pero también entender cuando no existe esa relación, ya que cuando el personal vinculado de manera directa o indirecta con un responsable de tratamiento actúa sobre una actividad no lo hace en calidad de encargado, sino simplemente como parte de la estructura del mismo. Un ejemplo habitual que suele llevar a confusión es cuando en una Dirección General se desarrolla una actividad de tratamiento tanto por el personal de la misma como por otro personal en una Delegación Territorial, en cuyo caso ninguna de esas personas actúa como encargado ya que pertenecen a la estructura de funcionamiento de la Dirección General. Caso distinto es cuando desde una Dirección General se hace un contrato o se encarga a una entidad instrumental de la propia administración⁴, en cuyo caso el personal de esa entidad instrumental actuará bajo las órdenes de su dirección que desarrolla el papel de encargado de tratamiento. Conocer la estructura funcional y orgánica en la administración y su relación nos suele ayudar a entender esta cuestión.

DESTINATARIO

La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;”

Por tanto, entendemos que destinatario será todo aquél a quien se remitan los datos, con una única excepción que suele entenderse que se aplica al ámbito policial y judicial, es decir, en el marco de una investigación concreta. Pero al estar sujeto al Derecho de la Unión o de los Estados miembros podemos encontrar otros -siempre autoridades públicas- a los que se pueden comunicar datos personales sin que sean considerados como destinatarios, como pudiera ser en actuaciones de tipo tributario o fiscal, por ejemplo, que cuentan con normativa sectorial específica que regula esta cuestión.

TERCERO

Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;”

Este concepto, que entendemos es suficientemente claro y conciso en su definición y no requiere comentario, es importante, junto con el de “destinatario” a la hora de abordar la cuestión de la cesión de los datos y la transferencia internacional de los mismos.

⁴ Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía. Artículo 50.1: “Tienen la consideración de entidades instrumentales de la Administración de la Junta de Andalucía, a los efectos de esta Ley, las entidades dotadas de personalidad jurídica propia, creadas, participadas mayoritariamente o controladas efectivamente por la Administración de la Junta de Andalucía o por sus entes públicos, con independencia de su naturaleza y régimen jurídico, que tengan por objeto la realización de actividades cuyas características por razones de eficacia justifiquen su organización y desarrollo en régimen de autonomía de gestión y de mayor proximidad a la ciudadanía, en los términos previstos en esta Ley.” <https://www.boe.es/buscar/act.php?id=BOE-A-2007-19819&p=20201231&tn=1#a50>

CONSENTIMIENTO DEL INTERESADO

Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;”

Si esta cuestión ya era relevante anteriormente, con la nueva regulación adquiere una importancia fundamental ya que si bien no es la única forma de legitimidad de la actividad de tratamiento (cuestión que recordaremos más adelante), sí se produce un avance fundamental al exigirse para entender que se produce el consentimiento que sea de manera fehaciente, es decir, que se produzca como tal ese consentimiento de manera libre y consciente, excluyendo el llamado consentimiento tácito, que se solía ver con casilleros premarcados que no daban la opción a la persona a no estar de acuerdo con el consentimiento; o incluso si fuera posible, tenía que desmarcar el casillero de manera expresa para que quedase claro que no consentía. Dicho de otro modo, la persona debe expresamente marcar o indicar de alguna manera ese consentimiento. Y es destacable que además es una “manifestación de voluntad libre” de tal modo que si una persona decide no consentir en ningún caso deben verse afectadas sus opciones o derechos por ello, ya que de ser así entenderíamos que el consentimiento no es “libre” bajo la “amenaza” del posible perjuicio que se pueda sufrir; por tanto, para que pueda existir el consentimiento la relación entre el responsable y el interesado debe ser de igualdad a estos efectos. Las condiciones para el consentimiento se recogen en el artículo 7 del RGPD, incluido que en caso de que se requiera el consentimiento éste deberá ser independiente para cada uno de los aspectos, no siendo posible un consentimiento genérico.

VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES

toda violación de la seguridad 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;”

Si bien hasta la aprobación del RGPD solo se aplicaba esta cuestión a las comunicaciones electrónicas⁵, con la entrada en vigor de esta nueva norma ya debe considerarse en todos los tratamientos de datos, sea cual será su origen. Ello es de especial relevancia por cuanto supone una mayor garantía para las personas cuyos datos se tratan, pero también respecto de los responsables y encargados de tratamiento que adquieren una obligación ante los órganos de control en materia de protección de datos en todo caso.

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;”

En este caso podemos destacar de este concepto que no es suficiente que se pueda identificar información sobre una persona, como puede ser el grupo sanguíneo o el color de los ojos, para

⁵ 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). <https://www.boe.es/boe/2002/201/L00037-00047.pdf>

considerar que se trata de un dato genético, si no que se exige que debe proporcionar una información única, como sí podría ser el caso de la detección de una enfermedad genética poco común, por ejemplo.

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;”

Este concepto no siempre es fácil de entender y aplicar, ya que es habitual asumir que la obtención de la huella dactilar por si misma es un dato biométrico; sin embargo, se requiere para que así sea hacer un tratamiento técnico específico para poder identificar a una única persona. Caso distinto sería la imagen facial de una persona, ya que con su sola consulta es posible conocer la identidad de la misma. Unido a lo anterior este concepto incluye una cuestión importante como son las características “conductuales”, por lo que un tic nervioso específico o la manera de firmar de manera escrita podrían permitirnos identificar a una persona. Tanto los datos genéticos como los biométricos son, entre otros, aquellos que se recogen en el artículo 9 como “categorías especiales de datos personales”⁶, por las especiales consecuencias que puede tener su tratamiento en caso de uso indebido o de acceso a los mismos por ante una violación de seguridad.

Comentados los conceptos que entendemos se han abordado con mayor o menor profundidad con anterioridad, insistimos en que el artículo 4 recoge hasta un total de 26 conceptos diferentes, algunos de ellos se abordarán más adelante como “autoridad de control” o “normas corporativas vinculantes”.

⁶ Reglamento General de Protección de Datos. Artículo 9. Tratamiento de categorías especiales de datos personales. “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.”

3. PRINCIPIOS EN LA PROTECCIÓN DE DATOS

El Capítulo II del RGPD recoge los principios por los que deben tenerse en cuenta en la protección de datos personales, en concreto aborda lo siguiente: principios relativos al tratamiento, licitud del tratamiento, condiciones para el consentimiento, condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, tratamiento de categorías especiales de datos personales, tratamiento de datos personales relativos a condenas e infracciones penales, y tratamiento que no requieren identificación. De todo ello vamos a centrarnos, por el carácter introductorio de esta unidad, en las dos primeras cuestiones.

3.1. PRINCIPIOS RELATIVOS AL TRATAMIENTO

Éstos se recogen en el artículo 5 del RGPD, de tal manera que los datos personales deberán ser tratados atendiendo a los siguientes principios:



Licitud, lealtad y
Transparencia



Limitación de la
Finalidad



Minimización de
Datos



Exactitud



Limitación del
Plazo de
Conservación



Integridad y
Confidencialidad



Responsabilidad
Proactiva

a) LICITUD, LEALTAD Y TRANSPARENCIA

Ello supone que los tratamientos solamente podrán realizarse porque tengamos la capacidad, porque sea lícito, es decir, que sea “justo, permitido, según justicia y razón” según lo define la Real Academia Española, siendo el criterio aplicable para ello lo que analizaremos a continuación sobre el artículo 6 del RGPD. Además, se debe realizar con lealtad hacia el interesado, es decir, sin ánimo de que pueda sentirse engañado o traicionado, así como con transparencia, lo que supone que en todo momento deben tener conocimiento claro sobre lo que ocurre con sus datos personales.

b) LIMITACIÓN DE LA FINALIDAD

Este principio hace referencia que, aplicando el principio anterior, una vez hagamos el tratamiento de los datos no podremos utilizarlos para una cuestión diferente para aquello que se obtuvieron, es decir, no se podrán utilizar de manera incompatible con los fines para los que se obtuvieron. No se entenderá que ello es aplicable cuando se trate de fines de archivo en interés público, fines de investigación

científica e histórica o fines estadísticos, ya que ello no se considerará incompatible con los fines iniciales.

c) MINIMIZACIÓN DE DATOS

Considerando los fines para los que se obtuvieron los datos personales, solamente se podrá hacer tratamiento de aquellos que sean los estrictamente necesarios para el cumplimiento de esa finalidad, de tal manera que en ningún caso se podrán recabar y tratar datos bajo la idea de “por si acaso me hicieran falta más adelante”; dicho de otro modo, deberá velarse porque solamente se recogen los datos estrictamente necesarios y para ello es preciso que cuando se diseñe la actividad de tratamiento a desarrollar se reflexione sobre los datos que harán falta en la misma, justificando en todo momento que efectivamente son esos y ninguno más los estrictamente necesarios.

d) EXACTITUD

Los datos personales que se recaben, pero también a lo largo de todo el tratamiento de datos y no solamente en el momento inicial de su recogida deberán ser exactos y siempre que sea necesario se deberán actualizar, pudiendo ello hacerse directamente por parte del interesado o cuando el responsable entienda que debe hacerlo, siendo recomendable en este último caso garantizar con el interesado que efectivamente esos son los datos actualizables en aras a evitar perjuicio posterior. Para ello el responsable adoptará todas las medidas razonables para que se supriman o rectifiquen sin dilación o retraso los datos personales que sean inexactos con respecto a los fines para los que se tratan. La aplicación de este principio estará relacionada también con los principios anteriores por lo que solamente se actualizarán los datos imprescindibles cuando sea necesario, para los que tengamos legitimidad y relacionados con la finalidad.

e) LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

Este principio nos indica que los datos personales que permitan identificar a un interesado no se mantendrán más allá del tiempo necesario para el cumplimiento de la finalidad para los que se obtuvieron, salvo que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (artículo 89, apartado 1), pero en todo caso aplicando las medidas técnicas y organizativas necesarias para su conservación. Es habitual en el caso de la administración que una vez que se inicia el tratamiento de datos los mismos queden con carácter indefinido sin que se establezca una limitación en el plazo de conservación, salvo en aquellas situaciones excepcionales donde existe una norma específica que lo regula, como pueden ser los datos sobre salud. Solemos encontrar en los registros de actividades de tratamiento en la administración de la Junta de Andalucía que el periodo de conservación será “durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Asimismo, se respetarán los plazos de archivo y custodia de documentación establecidos en la normativa vigente en cada momento”, lo que al final se traduce de manera práctica en un periodo indeterminado que no da garantías a los interesados sobre cuándo se producirá la finalización sobre la conservación de sus datos. Esta cuestión está igualmente relacionada con los avances en administración electrónica, así como con el conocimiento general y la percepción sobre el archivo y custodia de documentación administrativa, pero que requiere de una revisión que nos permita avanzar en esta cuestión.

f) INTEGRIDAD Y CONFIDENCIALIDAD

Este principio nos recuerda la necesidad de adoptar medidas tanto técnicas como organizativas que garantice que los datos personales no sufrirán ningún tipo de daño voluntario o involuntario pero que tampoco se hará un tratamiento no autorizado o ilícito de los mismos. Para ello es fundamental a la hora de definir y mantener el tratamiento de los datos personales que el responsable de tratamiento tenga una óptima relación con el Responsable de Seguridad TIC⁷ que le corresponda según el organismo donde se encuentre.

Es importante destacar que este artículo 5 atribuye en su punto 2 al responsable del tratamiento la obligación del cumplimiento de los principios anteriores, ya que al ser quien determina los fines y los medios es quien toma las decisiones para el cumplimiento de todos esos principios. Pero además y de manera expresa recoge que debe ser capaz de demostrarlo, es decir, en caso de que se produzca algún incidente de seguridad que afecte a los datos personales o que se realice una auditoría o control de protección de datos, debe poder acreditar el cumplimiento de esos principios, en línea con lo que el RGPD define como «**responsabilidad proactiva**».

3.2. LEGITIMIDAD

Como hemos comentado con anterioridad es aquello que permite al responsable de tratamiento realizarlo, es parte del marco jurídico y conceptual que viene a indicar el por qué se puede hacer ese tratamiento de datos. El RGPD lo desarrolla en el artículo 6 estableciendo distintas opciones para que pueda entenderse que existe esa legitimidad. Cuando analizamos un tratamiento de datos de las primeras cuestiones que tenemos que observar es que efectivamente existe esta cuestión y está suficientemente motivada porque de no tener legitimidad para el tratamiento de datos supondría que se está haciendo un tratamiento ilícito, y por lo tanto además de tomar medidas propias como la paralización de la actividad de tratamiento, por poner un ejemplo, sería susceptible de sanción por parte de la autoridad de control, como que en nuestro caso podría ser la Agencia Española de Protección de Datos o el Consejo de Transparencia y Protección de Datos de Andalucía, sobre los que se conocerá más adelante. Como decíamos el tratamiento solamente será lícito si se cumple alguna de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos”. Ya hemos tratado con anterioridad la cuestión del consentimiento y sus condiciones; en el caso de la administración pública es posible su uso como base de legitimidad si bien no suele ser el más habitual como comentaremos más adelante. Incluso es posible que en una misma actividad de tratamiento para parte de su ejecución la base de legitimidad sea el consentimiento y para otra parte de la actividad sea otra de las que vemos a continuación. Un ejemplo sería la creación de un registro público que recoja datos personales de docentes, que podía entenderse como una obligación legal si su creación viene determinada en una norma con rango de ley, y al mismo tiempo que esa información se pueda ceder a terceras personas que tengan interés legítimo en contratar a ese personal docente para lo que necesitan poder acceder a

⁷ Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía. <https://juntadeandalucia.es/boja/2011/11/d2.pdf>

Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía. https://juntadeandalucia.es/boja/2017/110/BOJA17-110-00009-10321-01_00115562.pdf

los mismos, por lo que facilitar los datos de contacto de quienes se encuentren en ese registro a terceros que puedan estar interesados requeriría de consentimiento previo bajo las condiciones comentadas.



- 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”. En el caso de la administración es habitual que se firmen contratos con distintas empresas para multitud de servicios. Los datos personales relacionados con la empresa, cómo por ejemplo los de quien la representa o del personal de la empresa que vaya a ejecutar el contrato, podrían enmarcarse dentro de esta base de licitud para la administración; mientras que el tratamiento de los datos de quien ejecuta el contrato en nombre de la administración, actuando en calidad de encargado de tratamiento, también se basaría en esta base de legitimidad, ya que la empresa contratada lo hace porque tiene un contrato con la administración.
- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento”. En el caso de la administración, ha de regir su funcionamiento en base a normas de carácter administrativo, por lo que es muy habitual encontrar que esta sea la base de legitimidad para su actuación, porque hay numerosas normas con rango de ley en todos los ámbitos de actuación y competenciales que establecen qué debe realizar la administración. Por tanto, es habitual encontrar en los registros de actividades de tratamiento que la legitimidad es tanto el artículo 6.1.c del RGPD cómo una norma con rango de ley que viene a explicar por qué se aplica este artículo. Es destacable que la norma debe entenderse como una obligación, es decir, que la administración deberá actuar en cierto modo y no deja libertad a que pueda o no actuar; ahí radica en la diferencia entre la obligación legal y el interés público que es otra base de licitud.
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física”. Entendemos que en este caso no hay duda sobre su aplicación ya que queda claro lo que aquí hace

referencia, sin menoscabo que la casuística del día a día puede generar en alguna ocasión dudas sobre su aplicación pero que requiere de un análisis individual de la situación.

- 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.” En relación con lo comentado en el apartado c), puede entenderse que la administración actúa en interés público cuando hay alguna norma que le habilita para actuar, pero no se lo establece como una obligación, siendo usual encontrar afirmaciones del tipo “podrá desarrollar ...”.
- 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 un niño.” Si bien recogemos esta opción como base de licitud del tratamiento porque así se establece en el RGPD, hay que recordar, porque lo dice el propio artículo, que no será de aplicación en el caso de las administraciones públicas por qué como ya hemos comentado estas tienen la obligación de actuar en base a normas que regulan su actividad y todo lo que quede fuera de esas normas por sí misma la administración no puede actuar.

En todo caso se recomienda la revisión de todo el Capítulo II, considerando de especial interés al respecto el artículo 9, Tratamiento de categorías especiales de datos personales.

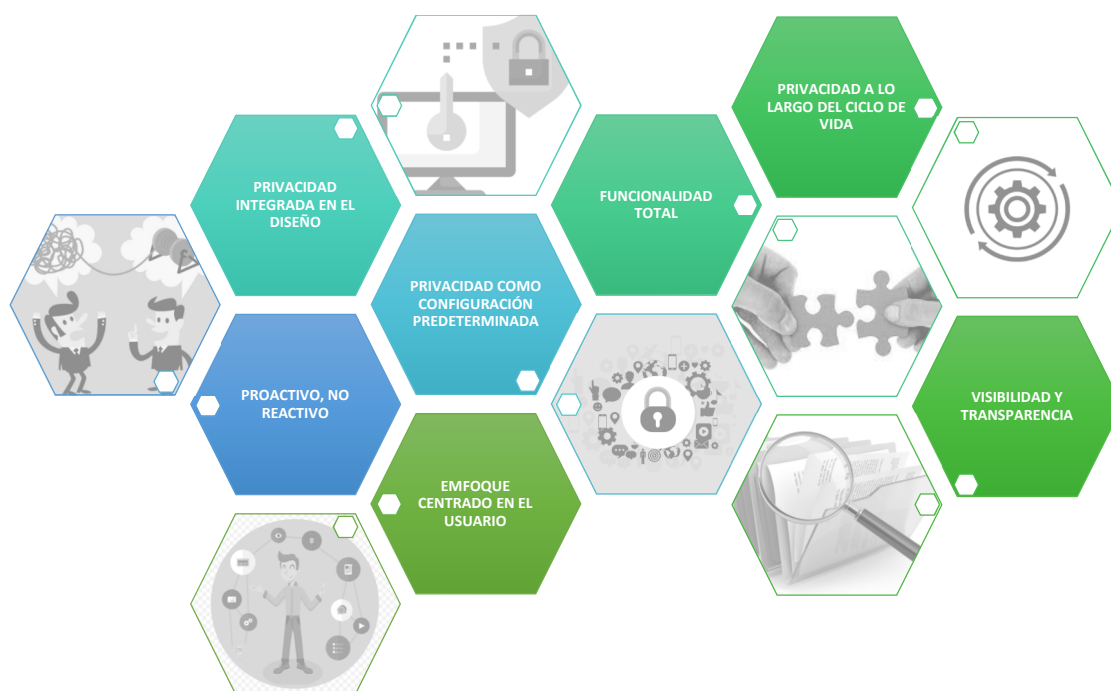
4. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO

El RGPD supone un cambio fundamental en la aplicación de la protección de datos respecto a la normativa anterior. Si bien antes estaba más centrada en que cada responsable indicaba la información sobre la que iba a hacer tratamiento a través de la publicación de “ficheros” y desde ese momento se daba casi por cumplida la obligación establecida en materia de protección de datos, más allá de las cuestiones propias de la técnica que tuvieran que ver con cuestiones de índole informática y tecnológica, a partir de esta nueva norma sigue recayendo en la figura del responsable de tratamiento, y del encargado cuando exista, la obligación de mantener activa la protección de datos mientras se haga el tratamiento de esos datos, es decir, por defecto (en todo momento). Pero si bien eso podría entenderse que es con carácter posterior a la puesta en marcha de la actividad de tratamiento, no debemos olvidar que también el reglamento establece la protección de datos desde el diseño, es decir, incluso antes de iniciar la actividad de tratamiento debe aplicarse la protección de datos hasta el punto que sí se entendiera que existe un elevado riesgo para los derechos y libertades de las personas por la aplicación de ese tratamiento se impediría su ejecución.

El RGPD aborda en su artículo 25 esta cuestión, pero lo hace de una manera muy general, concretamente: “1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.” Como vemos empieza condicionando su aplicación a las circunstancias actuales y su coste, vinculado a la situación contextual para la ejecución el tratamiento, por lo que si efectivamente un tratamiento de datos va a depender de otros muchos elementos como las personas a las que se aplica y su capacidad de decisión (pensando en tratamiento de tipo sanitario), de su capacidad de relación con la administración (que sigue utilizando un lenguaje complejo y poco asequible para la ciudadanía así como una estructura organizativa muy compleja, por ejemplo), ..., deja en manos del responsable contar con otras variables que puedan justificar la actividad de tratamiento. No obstante si que deja claramente recogido que deberá tanto al principio (“momento de determinar los medios”) como durante su ejecución establecer todos los medios necesarios para la protección de los datos, lo que supone que no es suficiente como se venía haciendo con anterioridad abordar esta cuestión al inicio si no que requiere de una revisión en el tiempo, entre otros motivos porque los riesgos y los medios que se aplican en el tratamiento también pueden cambiar a lo largo de la existencia de la actividad de tratamiento. El objetivo final: cumplir los requisitos que se establecen en la norma y sobre todo proteger los derechos de los interesados.

En su punto 2, este artículo vuelve a insistir en la aplicación de medidas técnicas y organizativas pero lo hace sin las limitaciones establecidas en el punto anterior, entendiendo que siempre es posible establecer algún tipo de medida de protección y prevención según los fines específicos del tratamiento, lo que nos lleva a pensar que si bien lo deja en manos del responsable, también le recuerda que no es suficiente tomar una decisión genérica que pueda servir para cualquier tratamiento de datos si no que las medidas deben adaptarse a cada finalidad. Y en esta línea indica que “Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la

intervención de la persona, a un número indeterminado de personas físicas”, lo que confirma con mayor rotundidad que la protección de datos desde el diseño y por defecto debe entenderse como una cuestión “individual y personalizada” a cada actividad de tratamiento y según la finalidad que se pretenda alcanzar.



5. DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS

En el Capítulo III, Derechos del interesado, Sección 2 (Información y acceso a los datos personales, artículo 15), Sección 3 (Rectificación y supresión, artículos 16 a 20) y Sección 4 (Derecho de oposición y decisiones individuales automatizadas, artículos 21 y 22) se desarrollan todos los derechos que se establecen en el RGPD y posteriormente se refuerzan en la LOPDGDD. Previo a su análisis encontramos que en el artículo 12 del RGPD (Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado) y el artículo 12 de la LOPDGDD (Disposiciones generales sobre ejercicio de los derechos) se recogen las condiciones generales para su aplicación:

- El ejercicio de los derechos puede realizarse directamente por las personas interesadas, sin necesidad de contar para ello de ningún representante legal. Ello supone por una parte reconocer a las personas cuyos datos se han tratado como interesadas y por lo tanto responsables de sus propios datos, y por otra que deben atenderse las peticiones que lleguen directamente sin poder derivar a que las mismas se hagan a través de terceros, lo que debe agilizar su atención además de reducir costes a las personas interesadas.
- Corresponde al responsable del tratamiento informar a las personas titulares de los datos sobre los medios que pone a su disposición para que pueda ejercer los derechos que le corresponden, que por otra parte deben ser fácilmente accesibles.
- El ejercicio de un derecho no podrá ser nunca denegado por el hecho que la persona interesada ha decidido utilizar un medio diferente al que ha dispuesto el responsable para el ejercicio de derechos.
- El encargado podrá atender, por cuenta del responsable y siempre que éste se lo haya autorizado mediante un contrato o en un acto jurídico suficiente (una resolución en el caso de las administraciones públicas, por ejemplo), las solicitudes de ejercicio formuladas por las personas interesadas.
- Ya sea el responsable del tratamiento o el encargado en su nombre que atienda la petición de ejercicio de derecho recibida, la demostración del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos corresponde al responsable.
- Cuando en leyes específicas se determine como aplicar los derechos que se establecen en el RGPD, serán éstas las que deban aplicarse según indiquen.
- En el caso de menores de 14 años corresponderá a quien ostente la patria potestad ejercer los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la LOPDGDD.
- Las actuaciones necesarias para dar respuesta a las peticiones de ejercicio de derechos de las personas interesadas serán gratuitas y asumidas por el responsable del tratamiento, o encargado en su caso, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del RGPD y en los apartados 3 y 4 del artículo 13 de la LOPDGDD, que establece condiciones especiales en situaciones de abuso.
- “Sin perjuicio de lo dispuesto en el artículo 11 del RGPD, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.” En el caso de la administración es frecuente tener que aplicar esta cuestión cuando la petición llega vía correo electrónico o de otro modo con carácter general, sin que la persona haya utilizado ninguno de los sistemas de firma electrónica

que se ponen a su disposición y permiten la comprobación de la identidad y por tanto que pueda entenderse como persona interesada.

- “El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.” Ello supone, por ejemplo, que se haya realizado una cesión de datos o una notificación de datos a la autoridad tributaria, en ese caso deberá informarse de ello, lo que supone tener un seguimiento adecuado tanto de las cesiones o remisiones de datos como de los ejercicios de derechos.
- Unido a lo anterior, entendemos oportuno recordar que en todo caso se deberá informar al interesado del resultado de su petición, no tanto por una cuestión en materia de protección de datos si no como una propia del procedimiento administrativo, que además nos servirá para poder acreditar lo ya mencionado como responsabilidad proactiva.

CUÁLES SON TUS DERECHOS DE PROTECCIÓN DE DATOS

La normativa de protección de datos te otorga una serie de derechos. Para ejercerlos, debes dirigirte ante quien está tratando tus datos (“responsable”)



Derecho de información

El responsable siempre debe identificarse, informarte para qué se utilizan tus datos y además decirte:

- La razón por la que tus datos son necesarios
- Hasta cuándo los conservará
- Cómo puedes ejercer tus derechos de protección de datos
- Cuál es la base jurídica del tratamiento
- Si los va a ceder a terceros o transferir a otros países
- Si los van a utilizar para elaborar perfiles tienes **derecho a oponerte si se adoptan decisiones automatizadas** que te afecten jurídicamente o de manera similar

Derecho de rectificación

Te permite corregir tus datos o completarlos si son inexactos o incompletos.

Derecho a la limitación de tratamiento

Permite solicitar la suspensión del tratamiento de tus datos cuando:

- Impugnes su exactitud, durante el periodo en el que se comprueba
- Te opongas al tratamiento, mientras se verifica si prevalece el interés legítimo del responsable
- El tratamiento sea ilícito, pero te opones a su supresión y en su lugar solicitas que se limite
- Cuando los necesites para la formulación, ejercicio o defensa de reclamaciones

Derecho de acceso

Utilízalo para saber si una entidad está tratando tus datos. Podrás obtener información sobre:

- Las categorías de los datos tratados, su finalidad y a quién se envían
- Si se producen transferencias internacionales de tus datos
- De quién se han obtenido y los plazos de conservación
- Si se elaboran perfiles y adoptan decisiones automatizadas
- Los derechos que te asisten

Derecho de oposición

Puedes oponerte a que una entidad trate tus datos:

- Por motivos personales salvo que el responsable acredite un interés legítimo
- Cuando el tratamiento tenga por objeto el marketing directo

Derecho de supresión (“derecho al olvido”)

Puedes solicitar la eliminación de tus datos personales cuando:

- Ya no sean necesarios para los fines para los que se recogieron
- Retires el consentimiento que diste, siempre que no haya otra causa que legitime el tratamiento
- Tus datos hayan sido tratados ilícitamente
- Te hayas opuesto a su tratamiento y no prevalezca el interés legítimo, o si el tratamiento tuviera por objeto el marketing directo
- Deban suprimirse para cumplir una obligación legal
- Se hayan obtenido siendo menor de edad en relación con los servicios de la sociedad de la información

Derecho a la portabilidad

Cuando el tratamiento esté basado en tu consentimiento o en la ejecución de un contrato, y se efectúa por medios automatizados, puedes recibir tus datos en un formato que permita transmitirlos a otro responsable.

Más información sobre tus derechos y cómo ejercerlos en:

<https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos>

www.aepd.es

[AEPD_es](https://twitter.com/AEPD_es)

Noviembre 2021

5.1. DERECHO DE ACCESO DEL INTERESADO (ARTÍCULO 15)

En este derecho “el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

- los fines del tratamiento;
- las categorías de datos personales de que se trate;

- c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;
- d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
- e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;
- f) el derecho a presentar una reclamación ante una autoridad de control;
- g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
- h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.”

Junto a lo anterior deberá informarse cuando se produzcan cesiones internacionales de datos. Como puede verse una parte de la información es la que habitualmente se ofrece a las personas interesadas cuyos datos se van a tratar según se establece en el artículo 13 del RGPD y que se vuelcan tanto en el Registro de Actividades de Tratamiento como en el Inventario de Actividades de Tratamiento de la Junta de Andalucía⁸. Esa misma información se puede encontrar también en los formularios normalizados que se usan en nuestra administración autonómica en aplicación del apartado 7.12 de la Guía de Normalización e Inscripción de Formularios de la Junta de Andalucía⁹.

El responsable del tratamiento tiene la obligación de hacer entrega de una copia de los datos personales objeto de tratamiento, pudiendo percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que indique que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

5.2. DERECHO DE RECTIFICACIÓN (ARTÍCULO 16)

Este artículo nos indica que “El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.” Como no puede ser de otro modo el responsable tiene que garantizar que los datos personales sobre los que hace tratamiento son los correctos por lo que aplicar este derecho debe hacerse a la mayor celeridad posible, máxime cuando además es el propio interesado quién se encarga de informar de ello y de no hacerlo se le puede generar un perjuicio.

⁸ Inventario de Actividades de Tratamiento de la Junta de Andalucía. Portal de la Junta de Andalucía.
<https://www.juntadeandalucia.es/protecciondedatos/buscadordatos.html>

⁹ Resolución de 17 de diciembre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba y publica la Guía de Normalización e Inscripción de Formularios de la Junta de Andalucía.
https://www.juntadeandalucia.es/boja/2020/245/BOJA20-245-00039-16054-01_00183285.pdf

5.3. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO») (ARTÍCULO 17)

La persona interesada tiene derecho a que a la mayor brevedad posible se atienda su petición, incluso en algunos casos debería haber sido el responsable el que actuara a iniciativa propia como en las letras a), d) y e). El responsable deberá hacerlo en todo caso cuando se den alguna de las siguientes situaciones:

- a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
- c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
- d) los datos personales hayan sido tratados ilícitamente;
- e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

Cuando los datos personales se hayan hecho públicos, como por ejemplo a través de una publicación en el Boletín Oficial de la Junta de Andalucía, el responsable deberá adoptar medidas razonables “con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos”, es decir, asumirá como obligación el informar a terceros que pudieran contener la información que se ha hecho pública sobre la voluntad de la persona interesada.

Pero lo anterior tiene excepciones en su aplicación, en concreto cuando se dé alguna de las siguientes:

- a) para ejercer el derecho a la libertad de expresión e información;
- b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; [recordemos que es de aplicación habitual el 6.1.c) en el caso de la administración pública].
- c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
- d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
- e) para la formulación, el ejercicio o la defensa de reclamaciones.

Por tanto, cada petición de ejercicio de este derecho requiere de un análisis en profundidad, tanto por el cumplimiento de las condiciones de su aplicación como las que lo impiden, así como se la información se haya podido hacer pública, cuestión habitual en el funcionamiento de la administración.

5.4. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ARTÍCULO 18)

Para que se limite la posibilidad de actuar sobre datos personales a petición del interesado debe darse alguna de las siguientes circunstancias:

- a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; [como por ejemplo un interesado puede solicitar un cambio de dirección postal pero el responsable debe asegurarse de ello porque podría suponer la imposibilidad de efectuar una notificación en un procedimiento, por lo que el responsable procederá a limitar los datos hasta que pueda comprobar la veracidad de los mismos]
- b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; [entendiendo que la persona interesada puede querer poder demostrar que se ha hecho un uso fraudulento por parte de la administración, por ejemplo]
- c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
- d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Hay que tener en cuenta que una vez que se produce la limitación del tratamiento tan solo se pueden tratar los datos para dos cuestiones: para su conservación o “para la formulación, el ejercicio o la defensa de reclamaciones”, siendo en cualquier otro caso necesario el consentimiento de la persona interesada. Una última obligación aplicable al responsable del tratamiento es que cuando se produzca el cese de la limitación debe informar de ello a la persona interesada.

5.5. DERECHO A LA PORTABILIDAD (ARTÍCULO 20)

Si bien es de difícil aplicación en el caso de la administración pública por cuanto se actúa en aplicación de la obligación legal (6.1.c) del RGPD) en la mayoría de los casos; y cuando sea a través del cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (6.1.e) del RGPD) está expresamente exceptuado de aplicación según se recoge en este artículo, su aplicación sería en los siguientes casos:

- a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
- b) el tratamiento se efectúe por medios automatizados.

5.6. DERECHO DE OPOSICIÓN (ARTÍCULO 21)

Fundamentalmente este derecho establece que “El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.”

Recordando que en el caso de las administraciones públicas está prohibido aplicar la letra f) del artículo 6.1. (interés legítimo), tan solo cabría la oposición en caso del “cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”, no siendo aplicable en el resto de los supuestos de legitimidad que habitualmente se aplican en la administración.

5.7. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES (ARTÍCULO 22)

Esta cuestión, cada vez de mayor relevancia en el funcionamiento de la administración con la incorporación de sistemas de gestión inteligentes que facilitan no solo la gestión documental si no que elevan a propuestas de resolución expedientes sin gestión humana previa, o realizan perfilado de personas usuarias con la finalidad de facilitarles desde la administración aquello que necesitan de una manera más ajustada a sus necesidades y realidad por ejemplo, establece que “Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.” En este caso la cuestión de relevancia es si se producen efectos jurídicos o le afecta de modo similar, sobre la persona, cuestión que deberá valorarse igualmente cuando se vaya a establecer la actividad de tratamiento y los medios y recursos para su ejecución.

No obstante, lo anterior no se aplicará si la decisión que se adopta:

- a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
- b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
- c) se basa en el consentimiento explícito del interesado.”
- d) En los casos de las letras a) y c), “el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.” Ello implica irremediamente que el responsable informará a los interesados que se aplicará un tratamiento automatizado ya que, de otro modo, si las personas interesadas no están informadas de ello, no podría ser aplicable el ejercicio de este derecho.
- e) “Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) -consentimiento- o g) -interés público esencial¹⁰-, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

¹⁰ Reglamento General de Protección de Datos, artículo 9, apartado 2, letra “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;” y letra “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;”

Por tanto, debemos entender que las decisiones automatizadas están permitidas, pero con carácter previo a su ejecución debería informarse a las personas interesadas y existen una serie de limitaciones a considerar con carácter previo.

6. CONCLUSIONES DE LA UNIDAD 1

Hemos visto, a modo de repaso de cursos anteriores y sin menoscabo que deba acudir a la normativa como fuente principal de la información, los principales conceptos (artículo 4 del RGPD) que deben manejarse hasta el momento para poder entender adecuadamente de qué hablamos cuando nos movemos en el ámbito de la protección de datos personales, tanto en conceptos básicos como en otros sobre quienes participan o qué debe hacerse.

Por otra parte hemos recordado cuales son los principios que deben regir en el tratamiento de los datos personales (artículo 5 del RGPD) sin los cuales no estaremos realizando adecuadamente dichos tratamientos, y en todo caso relacionados con la protección de datos desde el diseño (el momento en el que se entiende que es necesario realizar una actividad de tratamiento y se inicia toda la planificación necesaria para ello) y por defecto (durante todo el tiempo que vaya realizarse el tratamiento de los datos personales, relacionado ello con el ciclo de vida de esos datos).

En tercer lugar hemos entrado a ver las distintas causas por las que se puede actuar en el tratamiento de datos personales, es decir, en la licitud (artículo 6 del RGPD), destacando en el caso de la administración pública que suelen utilizarse los apartados c) (obligación legal para el responsable del tratamiento) y e) (cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento), así como la prohibición expresa en el caso de las administraciones del uso del apartado f) (interés legítimo).

Finalmente hemos repasado los distintos derechos que pueden ser ejercidos por las personas interesadas cuyos datos personales manejamos, ahondando asimismo cuando deben ser atendidos favorablemente y cuando no pueden serlo, así como otras condiciones en su aplicación.

