Las entidades locales y la protección de datos

Marcos Almeida Cerreda
Profesor Contratado Doctor de Derecho Administrativo
Universidad de Santiago de Compostela

RESUMEN

En el ejercicio de sus competencias, las Administraciones locales desarrollan numerosas actividades que requieren, para su correcta ejecución, que dichas entidades recaben y traten datos personales de los ciudadanos. En consecuencia, la reciente renovación del marco normativo en materia de protección de datos personales (con la aplicación del Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales), que implica un cambio de paradigma, introduciendo novedades radicales, ha tenido y tendrá, en los próximos tiempos, un fuerte impacto en la actuación cotidiana de las Administraciones locales españolas, que ha de adecuarse al mismo.

Con el presente trabajo se pretende, esencialmente, exponer de forma ordenada los elementos esenciales del nuevo régimen jurídico de la protección de datos, desde la perspectiva de las entidades locales. Por ello, este estudio se articula en dos partes: una primera, consistente en una aproximación sistemática a la nueva disciplina normativa de la protección de datos, y, una segunda, complementaria de la anterior, en donde, de forma sucinta, se da cuenta de determinados aspectos concretos, relacionados con la protección de datos, que se plantean en la actividad de las Administraciones locales, cuyo tratamiento ha sido abordado de forma específica por la citada Ley Orgánica 3/2018.

Palabras clave: datos personales; protección de datos; entidades locales.

ABSTRACT

When exercising their powers, local Administrations undertake numerous activities which, for their correct execution, require such Entities to collect and process citizens' personal data. Consequently, the recent renewal of the regulatory framework for the protection

of personal data (by applying Regulation EU 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data and the free circulation of such data and the approval of the Organic Law 3/2018, of 5 December, Protection of Personal Data and Guarantee of Digital Rights), which implies a paradigm shift, introducing radical novelties, has had and will have in the period ahead, heavy impact on the daily performance of Spanish local administrations, which must adapt to it.

This paper is essentially intended to present in an orderly manner the essential elements of the new legal system for data protection, from the perspective of local entities. Therefore, this study is divided into two parts: the first consists of a systematic approach to the new regulatory discipline of data protection, and the second, which is complementary to the previous one, gives a succinct account of certain specific aspects related to data protection, that arise in the activity of local administrations, the treatment of which has been specifically addressed by the aforementioned Organic Law 3/2018.

Keywords: personal data; data protection; local governments.

SUMARIO: I. INTRODUCCIÓN.—II. EL RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS: 1. El *hard law* en materia de protección de datos. 2. El *soft law* en materia de protección de datos.—III. APROXIMACIÓN A LOS ASPECTOS ESENCIALES DEL RÉGIMEN DE LA PROTECCIÓN DE DATOS, DESDE LA PERSPECTIVA DE LAS ADMINISTRACIONES LOCALES: 1. Aspectos subjetivos: 1.1. El responsable del tratamiento. 1.2. El encargado del tratamiento. 1.3. El delegado de protección de datos: 1.3.1. Vinculación, dedicación y adscripción. 1.3.2. Cualificación. 1.3.3. Estatus. 1.3.4. Funciones. 1.4. Los titulares de los datos personales y sus derechos: 1.4.1. Los titulares de derechos sobre los datos personales: 1.4.1.1. Las personas interesadas. 1.4.1.2. Las personas vinculadas a una persona interesada fallecida. 1.4.2. Los derechos de los titulares de los datos personales: 1.4.2.1. El elenco de derechos en materia de protección de datos. 1.4.2.2. Forma de ejercicio y sistema de tutela de los derechos. 2. Aspectos objetivos: 2.1. Los datos personales: 2.1.1. Concepto. 2.1.2. Tipología: las categorías especiales de datos y las limitaciones a su tratamiento. 2.2. El tratamiento de los datos personales: 2.2.1. Concepto. 2.2.2. Principios relativos al tratamiento de datos personales: 2.2.2.1. Principios básicos. 2.2.3. Metaprincipios: 2.2.3.1. Responsabilidad proactiva. 2.2.3.2. Protección de datos desde el diseño y por defecto. 3. Aspectos organizativos: 3.1. La evaluación de riesgos y la consulta previa. 3.2. El registro de actividades de tratamiento. 3.3. La seguridad en el tratamiento: 3.3.1. Las medidas y el nivel de seguridad. 3.3.2. La reacción frente a violaciones de seguridad. 3.4. El bloqueo de datos. 3.5. La responsabilidad por el tratamiento.—IV. ALGUNOS PUNTOS CRÍTICOS EN LA APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN EL ÁMBITO LOCAL: 1. Cuestiones relativas al tratamiento y uso de datos: 1.1. Cuestiones relativas al tratamiento de datos en el ámbito de la gestión de recursos humanos. 1.2. Cuestiones relativas al tratamiento de datos en los procedimientos en materia de transparencia: en el acceso a la información y en la publicidad activa. 1.3. Tratamientos en materia de policía y seguridad: 1.3.1. Tratamientos con fines de vigilancia y control. 1.3.2. Tratamientos de datos relativos a infracciones y sanciones administrativas. 1.4. Tratamientos de datos en el marco de los sistemas de denuncias internas. 1.5. Tratamientos de datos en el ámbito de los procedimientos administrativos: 1.5.1. La facultad general de verificación de datos de las Administraciones locales. 1.5.2. La facultad general de obtención de documentación administrativa por las Administraciones locales. 1.5.3. La identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos. 2. Cuestiones relativas a las comunicaciones de datos.—V. BIBLIOGRAFÍA.

I. INTRODUCCIÓN

El desarrollo de muchas de las actividades que las Administraciones locales llevan a cabo en el ejercicio de sus competencias exige que estas recaben y traten datos personales de los ciudadanos, incluso a gran escala. En consecuencia, la reciente renovación del marco normativo en materia de protección de datos personales, que implica un cambio de paradigma, introduciendo novedades radicales, ha tenido y tendrá, en los próximos tiempos, un fuerte impacto en la actuación cotidiana de dichas entidades locales, que ha de adecuarse al mismo.

Con el presente trabajo se pretende, en esencia, exponer de forma ordenada y fácilmente comprensible los elementos fundamentales del nuevo y complejo régimen de la protección de datos, desde la perspectiva de las entidades locales. Por ello, este trabajo se articula en dos partes: una primera, consistente en una aproximación sistemática a la nueva regulación de la protección de datos[1], y, una segunda, complementaria de la anterior, en donde, de forma sucinta, se da cuenta de determinados aspectos concretos relacionados con la protección de datos, que se plantean en la actividad de las Administraciones locales, cuyo tratamiento ha sido abordado, de manera específica, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

II. EL RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS

1. El *hard law* en materia de protección de datos

El núcleo esencial del régimen general de la protección datos lo constituye el bloque normativo formado por el Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD) y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDP)[2].

---

[1] Dado que el espacio con el que se cuenta para realizar esta exposición es limitado, no resulta posible abarcar el examen de todos los aspectos de la antedicha regulación. Por ello, se ha centrado en el análisis de los que, previsiblemente, son de mayor interés para las entidades locales. Así, por ejemplo, se debe señalar que se parte del presupuesto de que los tratamientos de datos responsabilidad de las Administraciones locales en su mayoría se realizan en el ámbito de la Unión Europea, y, en consecuencia, no se aborda la problemática de las transferencias internacionales.

[2] Es necesario advertir que, en algunos sectores, junto a estas normas generales, coexisten otras con relevancia en este campo que marcan diversas especialidades (si bien tienen un impacto escaso a nivel local), *vid.* L. Miguez Macho, «Normativa española con implicaciones en protección de datos», en C. Campos (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 69 y ss., y M.ª de los Á. Fernández, S. Lorenzo, J. P. Murga y A. Palma, «Normativas sectoriales afectadas por la protección de datos», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 275 y ss.

La LOPDP, como señala su art. 1, por una parte, desarrolla y complementa las disposiciones del RGPD, en especial, en aquellos puntos en los que el propio Reglamento remite a las normas nacionales para su especificación o restricción (como, por ejemplo, en caso de la edad mínima para otorgar el consentimiento por parte de los menores de edad), y, por otra parte, adapta el mismo al Ordenamiento español. Aunque la LOPDP, haciendo uso de la posibilidad excepcional que le concede el considerando 8 RGPD, incorpora algunas disposiciones del Reglamento, por razones de coherencia y comprensibilidad, no es posible emplear únicamentente esta para afrontar el estudio del sistema general de la protección de datos, pues muchas cuestiones se abordan de forma exclusiva en el RGPD. En consecuencia, tan solo examinando, de modo conjunto, el complejo normativo RGPD+LOPDP se puede dar cabal cuenta del antedicho régimen jurídico[3].

A su vez, la LOPDP no prevé que sus disposiciones, en general, sean desarrolladas reglamentariamente por el Ejecutivo, sino que tan solo contiene algunas remisiones normativas puntuales (DF 15.ª). Pero sí que contempla, en su art. 55, las potestades de regulación de la Agencia Española de Protección de Datos (en adelante, AEPD), a través de Circulares[4]. De acuerdo con este precepto, la Presidencia de la AEPD podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el RGPD y en la LOPDP, que se denominarán «Circulares de la Agencia Española de Protección de Datos». La elaboración de estas Circulares se sujetará al procedimiento establecido en el Estatuto de la AEPD, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados. Las antedichas Circulares serán obligatorias una vez publicadas en el *Boletín Oficial del Estado*. De acuerdo con el art. 57.2 LOPDP, las autoridades autonómicas de protección de datos también podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para AEPD.

Aunque la redacción es poco precisa, no cabe duda de que al amparo de este precepto la AEPD y las autoridades autonómicas[5] crearán normas reglamentarias que especificarán y detallarán las obligaciones impuestas por el RGPD y la LOPDP[6].

Es necesario advertir que, de conformidad con el art. 2 RGPD, este Reglamento no se aplica, en muchos de los antedichos sectores, ya que se refieren al ejercicio de actividades no comprendidas en el ámbito del Derecho de la Unión. No obstante, el art. 2.3 LOPDP dispone que los tratamientos a los que no sea directamente aplicable el RGPD, por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica, si la hubiere, y, supletoriamente, por lo establecido en el RGPD y en la LOPDP.

[3] No obstante lo dicho, de conformidad con la disposición derogatoria única de la LOPDP, continúan vigentes determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la misma, en cuanto no se opongan al RGPD y a la LOPDP. En este sentido, *vid.* J. L. Piñar Mañas, *Código de protección de datos*, Wolters Kluwer, Madrid, 2019, p. 12.

[4] *Vid.* J. Rubí Navarrete, «La agencia española de protección de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 513-516.

[5] *Vid.* Manuel Valín López, «Las autoridades autonómicas de protección de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 521 y ss.

(Vid. nota 6 en página siguiente)

2. El *soft law* en materia de protección de datos

La normativa antes citada se complementa con un heterogéneo conjunto de instrumentos paranormativos. Estos se caracterizan por contener indicaciones razonables de cómo interpretar la misma, pero, en principio, *per se,* carecen de fuerza obligatoria. No obstante, en la práctica, gozan de un notable nivel de vinculatoriedad, en la medida en que los organismos administrativos de control y los tribunales los tienen en cuenta a la hora de adoptar y fundamentar sus decisiones. Es necesario destacar que la incorporación del principio de responsabilidad proactiva, en el acervo de principios de la protección de datos, sin duda alguna, va a incrementar la fuerza vinculante propia de estos documentos: la gestión respetuosa con los principios de protección de datos requiere, ontológicamente, el seguimiento prudente y ponderado de las indicaciones contenidas en los instrumentos de *soft law*.

Dentro de estos instrumentos, a nivel europeo, hay que subrayar el importante conjunto de indicaciones del Grupo de Trabajo del artículo 29, creado al amparo de la Directiva 95/46/CE y que ha funcionado hasta 2018[7]. Entre sus últimas aportaciones, se pueden destacar las Directrices sobre el consentimiento en el sentido del RGPD[8]. La importante labor de este organismo se desarrolla ahora por el Comité Europeo de Protección de Datos, el cual de conformidad con el art. 68 RGPD, entre otras funciones, emite directrices, recomendaciones y buenas prácticas[9].

A su vez, en el ámbito nacional, es necesario destacar los múltiples instrumentos que, a lo largo del tiempo, ha ido elaborando la AEPD[10]. En particular, hay que referirse a sus Guías y, en especial, por lo que respecta a este trabajo, a la *Guía sobre protección de datos y Administración local*[11].

---

[6] *Vid.*, como ejemplo, la Circular 1/2019, de 7 de marzo, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales relativos a opiniones políticas y envío de propaganda electoral por medios electrónicos o sistemas de mensajería por parte de partidos políticos, federaciones, coaliciones y agrupaciones de electores al amparo del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (*BOE* del 11 de marzo de 2019).

En este sentido, hay que destacar también que el cambio normativo permite considerar superada la doctrina contenida en la STS 954/2007, de 16 de febrero.

[7] *Vid.* C. Trujillo Cabrera, «Directrices de interpretación del RGPD», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 265 y ss.

[8] Los documentos producidos por el mismo se pueden obtener en *https://ec.europa.eu/newsroom/article29/news-overview.cfm* (consultado en abril de 2019).

[9] De su actividad se da cuenta en *https://edpb.europa.eu/edpb_es* (consultado en abril de 2019). Asimismo, *vid.* L. Cervera Navas, «El comité europeo de protección de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 655 y ss.

[10] La LOPDP reconoce ahora en su DA 18.ª estos instrumentos: herramientas, guías, directrices y orientaciones.

[11] *Vid. https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf* (consultado en abril de 2019).

III. APROXIMACIÓN A LOS ASPECTOS ESENCIALES DEL RÉGIMEN DE LA PROTECCIÓN DE DATOS, DESDE LA PERSPECTIVA DE LAS ADMINISTRACIONES LOCALES

1. Aspectos subjetivos

1.1. El responsable del tratamiento

De conformidad con el art. 4.7 RGPD, el responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento [12]. Además, según el art. 33.2 LOPDP, también tendrán la consideración de responsable del tratamiento: *a)* quien figurando como encargado utilizase los datos para sus propias finalidades, y *b)* quien, en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico de encomienda del tratamiento [13]. Esta última previsión, de conformidad con el citado precepto, no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público [14].

Teniendo en cuenta lo dicho, las entidades locales, enumeradas en el art. 3 LBRL, así como las entidades u organismos vinculados o dependientes de las mismas tendrán la consideración de responsables de los tratamientos de datos que efectúen en el ejercicio de sus competencias —excluidas las de auxilio—, en cuanto que determinan los medios y fines de los mismos y en la medida en la que lo hagan.

Corresponde al responsable del tratamiento, de acuerdo con el art. 24 RGPD, determinar, aplicar, revisar y actualizar las medidas técnicas y organizativas apropiadas para garantizar (y poder demostrar) que el tratamiento es conforme con la normativa de protección de datos. En particular, según el art. 28 LOPDP, el responsable ha de valorar si procede la realización de la evaluación de impacto y/o la consulta previa. La elección de las citadas medidas se realizará, a tenor del citado art. 24 RGPD, 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 art. 28.2 LOPDP, en esta línea, indica a los responsables del tratamiento que tengan

---

[12] En el caso de que varios responsables determinen conjuntamente los fines y medios del tratamiento, de conformidad con los arts. 26 RGPD y 29 LOPDP, se estará ante corresponsables del tratamiento, siguiéndose el régimen de los citados artículos.

[13] *Vid.* R. Costa Hernandis, «Capítulo 12. Responsabilidad del responsable del tratamiento», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 409 y ss.

[14] Hay que tener en cuenta que, según el art. 28.10 RGPD, si un encargado del tratamiento infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

en cuenta, en particular, los mayores riesgos que podrían producirse en determinados supuestos. De entre los mismos, desde la óptica de las Administraciones locales, cabe destacar los dos siguientes: el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad, y, en particular, de menores de edad y personas con discapacidad, y el tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

De conformidad con el art. 24.3 RGPD, la adhesión a códigos de conducta o a un mecanismo de certificación podrán ser utilizados como elementos para demostrar el cumplimiento de las antedichas obligaciones por parte del responsable del tratamiento.

1.2. El encargado del tratamiento

De acuerdo con el art. 4.8 RGPD, el encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

En el ámbito del sector público español, según el art. 33.5 LOPDP, podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las Comunidades Autónomas, las entidades que integran la Administración local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido de la encomienda a la que se hace referencia más adelante.

Hoy por hoy, en el ámbito local, Diputaciones, Consejos y Cabildos insulares actúan como encargados del tratamiento en aquellos tratamientos vinculados con la prestación de asistencia a favor de los municipios. Asimismo, las entidades locales cuentan con encargados del tratamiento, en diferentes actividades: para la destrucción de documentación, para la elaboración de nóminas, etcétera[15].

Este encargado, de conformidad con el art. 28.1 RGPD, ha de poseer las capacidades, aptitudes y recursos adecuados para ofrecer garantías suficientes de que aplicará las medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la normativa de protección de datos y asegure la protección de los derechos de los ciudadanos. La adhesión del encargado del tratamiento a un código de conducta o a un mecanismo de certificación podrá utilizarse como elemento para demostrar la existencia de dichas garantías.

La encomienda del tratamiento por parte del responsable al encargado se articulará, de acuerdo con el art. 28.3 RGPD, a través de un contrato u otro acto jurídico que conste por escrito, inclusive en formato electrónico. Dicho documento podrá estar basa-

---

[15] *Vid. https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf* (consultado en abril de 2019).

do o no en unas cláusulas contractuales tipo fijadas por un organismo competente. No obstante, en todo caso, establecerá el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y los derechos y las obligaciones del responsable, y las demás previsiones contenidas en el citado precepto [16].

El encargado del tratamiento no recurrirá a otro encargado, sin la autorización previa, por escrito, específica o general, del responsable (art. 28.2 RGPD). En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado original. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado (art. 28.4 RGPD).

Según el art. 33.3 LOPDP, el responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales le deben ser devueltos, destruidos o, en su caso, entregados a un nuevo encargado. No obstante, no se procederá a la destrucción de los mismos, cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, quien garantizará su conservación mientras tal obligación persista. Además, el encargado del tratamiento podrá conservar, debidamente bloqueados, los datos, en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento (art. 33.4 LOPDP) [17].

1.3. El delegado de protección de datos

Según el art. 37 RGPD, las autoridades u organismos públicos que actúen como responsables o encargados de tratamientos han de designar un delegado de protección de datos (en adelante, DPD) y publicar sus datos de contacto. Dicha designación (así como el cese) se comunicará a la AEPD o a las autoridades autonómicas de protección de datos, en el plazo de diez días (art. 34.3 LOPDP).

En el ámbito local, esto implica que las entidades locales, enumeradas en el art. 3 LBRL, deben de contar con un DPD. Además, la referencia del art. 37 RGPD a «organismos públicos», atendiendo al carácter no formalista del Derecho de la Unión, ha de ser interpretada en el sentido de «organismos del sector público» y, en consecuencia, también las entidades del sector público institucional local (organismos autónomos,

---

[16] *Vid. https://www.aepd.es/media/guias/guia-directrices-contratos.pdf* (consultado en abril de 2019).

[17] *Vid.* J. L. Núñez García, «Responsabilidad y obligaciones del responsable y del encargado del tratamiento», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 353 y ss.

entidades públicas empresariales, sociedades, fundaciones, etc.) tienen que contar con un DPD[18].

El apartado 3 del citado art. 37 RGPD permite que se designe un único DPD para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño. En este punto, hay que señalar que la AEPD entiende que no es aconsejable que único DPD actúe respecto de grandes unidades u órganos con entidad y tareas claramente diferenciadas, por mucho que orgánicamente puedan depender de una misma entidad local[19].

Así las cosas, en el ámbito municipal, parece conveniente distinguir entre los municipios de gran población y los municipios de régimen general. Respecto de los primeros, cabe defender que estos, dependiendo de su estructura, quizá deberían tener más de un DPD. Por lo que se refiere a los municipios de régimen general, en función de sus dimensiones (la AEPD fija el umbral en 20.000 habitantes), estos podrían contar con un DPD propio o compartirlo entre varios, por acuerdo entre los mismos o con el apoyo de las Diputaciones provinciales. Asimismo, en los ayuntamientos de régimen general, el DPD podría actuar tanto al servicio de la Administración general, como de la institucional, cuando las dimensiones reducidas lo aconsejen, por razones de eficiencia y economía[20].

1.3.1. Vinculación, dedicación y adscripción

De acuerdo con el art. 37.6 RGPD, el DPD podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Por su parte, el art. 38.6 RGPD establece que es posible que el DPD desempeñe otras funciones y cometidos, además de las tareas propias de su ocupación principal. En este supuesto, el responsable o el encargado del tratamiento ha de garantizar que dichas funciones y cometidos no den lugar a conflicto de intereses. En esta línea, el art. 34.5 LOPDP precisa que el DPD podrá tener dedicación a tiempo completo o a tiempo parcial. Esta decisión ha de tomarse teniendo en cuenta, entre otros criterios: el volumen de los tratamientos, la categoría especial de los datos tratados o los riesgos para los derechos o libertades de los interesados que los tratamientos implican.

---

[18] Hay que señalar que la AEPD, en su Guía «Protección de Datos y Administración Local» (*https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf*, consultado en abril de 2019), p. 31, solo lo considera recomendable en función de los tratamientos de datos que estas entidades instrumentales lleven a cabo.

[19] Cfr. *https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf* y *https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf* (consultados en abril de 2019).

[20] La realidad es que el modelo de DPD único, con sus riesgos, se está imponiendo, *vid.* R. Martínez, «El delegado de protección de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 431 y ss.

En el ámbito local, en el caso de que no se opte por externalizar esta actividad, la AEPD parece inclinarse por que, en ayuntamientos de más de 20.000 habitantes, si existe un único DPD, este desempeñe sus funciones a tiempo completo. Considera además la AEPD que, en este supuesto, es, incluso, oportuno que el mismo esté respaldado por una unidad específicamente dedicada a la protección de datos. Por el contrario, en municipios de menos de 20.000 habitantes, la AEPD considera factible que el DPD compagine sus funciones con otras que no generen conflictos.

Ahora bien, tanto en el caso de grandes entes con varios DPD a tiempo parcial, como en el supuesto de pequeños entes con un único DPD a tiempo parcial, es necesario evitar conflictos de intereses entre las diversas ocupaciones. Como señala la AEPD, dado que el DPD actúa como asesor y supervisor interno, este puesto no puede ser desempeñado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p. ej., responsables de ITC o responsables de seguridad de la información). En este sentido, también advierte la AEPD que secretarios, interventores y tesoreros podrían actuar como DPD, siempre que no exista conflicto de intereses en relación con el ejercicio de sus respectivas funciones en la gestión ordinaria del ente local[21].

Por último, respecto de la adscripción del DPD, dadas sus funciones, la AEPD recomienda su vinculación a órganos o unidades con competencias y funciones de carácter horizontal.

1.3.2. Cualificación

De conformidad con el art. 37.5 RGPD, el DPD será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que le corresponden. Por su parte, el art. 35 LOPDP especifica que el cumplimiento de estos requisitos podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación, que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el Derecho y la práctica en materia de protección de datos[22].

1.3.3. Estatus

En aras a garantizar que el DPD desarrolle adecuadamente sus funciones, la normativa (en particular, los arts. 38 RGPD y 36 LOPDP) impone una serie de obligaciones positivas y negativas a los responsables y a los encargados del tratamiento.

---

[21] Cfr. *https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf* (consultado en abril de 2019).

[22] Cfr. M. Recio Gallo, *El estatuto jurídico del Data Protection Officer*, Wolters Kluwer, Madrid, 2019, pp. 213-279.

Dentro del conjunto inicial, se hallan: en primer lugar, el deber de garantizar la independencia del DPD en el interior de la organización, evitando cualquier conflicto de intereses[23]; en segundo lugar, la obligación de proporcionar al DPD un acceso total a los datos personales y a las operaciones de tratamiento, de acuerdo con el art. 36.3 LOPDP, así el responsable o el encargado del tratamiento no podrá oponerse a este acceso alegando la existencia de cualquier deber de confidencialidad o secreto; en tercer lugar, el deber de asegurar que el DPD participe, de forma adecuada y en tiempo oportuno, en todas las cuestiones relativas a la protección de datos personales; en cuarto lugar, la obligación de asegurar que el DPD rinde cuentas directamente al más alto nivel jerárquico de la entidad a la que presta sus servicios, esto implica, como señala la AEPD, que, en el caso de Administraciones locales, el nivel del puesto de trabajo tiene que ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones; en quinto lugar, el deber de facilitar al DPD los recursos necesarios para el desempeño de sus funciones, y, en sexto lugar, la obligación de colaborar con el mantenimiento de los conocimientos especializados del DPD.

Por lo que se refiere a las obligaciones negativas, hay que señalar que: en primer lugar, el responsable y el encargado del tratamiento garantizarán que el DPD no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones, y, en segundo lugar, que, cuando se trate de una persona física integrada en la organización del responsable o del encargado del tratamiento, el DPD no podrá ser removido, ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que, como precisa el art. 36.2 LOPDP, incurriera en dolo o negligencia grave en el ejercicio de las mismas.

1.3.4. Funciones

De acuerdo con los arts. 38 y 39 RGPD, el DPD tendrá como mínimo las siguientes funciones: *a)* informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, en general, de las obligaciones que les incumben en virtud de la normativa de protección de datos y, en particular, acerca de la evaluación de impacto relativa a la protección de datos; *b)* supervisar el cumplimiento de la normativa de protección de datos, de las políticas de la entidad para la que trabaja en este campo y de la evaluación de impacto efectuada por la misma; en este ámbito, el DPD podrá realizar inspecciones y emitir recomendaciones en el marco de sus competencias (art. 36.1 LOPDP), y, cuando aprecie la existencia de una vulneración relevante en materia de protección de datos, lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o del encargado del tratamiento (art. 36.4 LOPDP); *c)* cooperar con la autoridad de control y actuar como punto de contacto de la misma para cuestiones relativas al tratamiento, incluida la consulta previa,

---

[23] Sobre la independencia del DPD, en especial, en el seno de las Administraciones públicas, *vid.* M. Recio Gallo, *El estatuto jurídico del Data Protection Officer*, *op. cit.,* pp. 196-213.

y solicitar aclaraciones o consejos, en su caso, sobre cualquier otro asunto (en este punto, el art. 36.1 LOPDP precisa que el DPD, actuará como interlocutor del responsable o encargado del tratamiento ante la AEPD y las autoridades autonómicas de protección de datos), y *d)* atender a los interesados que se pongan en contacto con él por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos (art. 38.4 RGPD)[24].

Como el RGPD configura las funciones del DPD como un mínimo, el Legislador español las ha ampliado, atribuyéndole, a través del art. 37 LOPDP, una función de mediación en los supuestos de conflictos, ligada a la última de sus responsabilidades antes expuestas. Así, por una parte, cabe que los afectados, con carácter previo a la presentación de una reclamación ante la AEPD o, en su caso, ante las autoridades autonómicas de protección de datos, se dirijan al DPD de la entidad contra la que reclamen. En este caso, el DPD les comunicará la decisión que se hubiera adoptado, en el plazo máximo de dos meses, a contar desde la recepción de la reclamación. Y, por otra parte, es posible que, cuando un ciudadano presente una reclamación ante la AEPD, o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas remitan la reclamación al DPD, a fin de que este responda en el plazo de un mes; si transcurrido dicho plazo, el DPD no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará con el procedimiento de reclamación.

Finalmente, hay que destacar que el DPD está obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones (art. 38.5 RGPD)[25].

1.4. Los titulares de los datos personales y sus derechos

1.4.1. Los titulares de derechos sobre los datos personales

1.4.1.1. Las personas interesadas

Se considera que son titulares de derechos sobre sus datos personales las personas físicas, nacionales y extranjeras, residentes o no, mayores y menores de edad[26].

No obstante, la tutela que la normativa de protección de datos otorga a las personas interesadas se puede ver modulada por la actividad que las mismas desarrollan, como es el caso de los empleados públicos (respecto, por ejemplo, del puesto que ocupan) o de

---

[24] Cfr. M. Recio Gallo, *El estatuto jurídico del Data Protection Officer*, *op. cit.,* pp. 145-166.

[25] Sobre las obligaciones deontológicas del DPD, *vid.* C. Sánchez Ors, «Capítulo 20. El delegado de protección de datos», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 493 y ss.

[26] En el considerando 14 RGPD, se aclara: «El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto».

los empresarios individuales y de los profesionales liberales (en los términos del art. 19 RGPD).

1.4.1.2. Las personas vinculadas a una persona interesada fallecida

De conformidad con el considerando 27 RGPD, esta norma no se aplica a la protección de datos personales de personas fallecidas. No obstante, la misma recuerda que los Estados miembros son competentes para establecer disposiciones relativas al tratamiento de los datos personales de estas. En consecuencia, el legislador español, en el art. 3 LOPDP, regula el tratamiento de los datos de personas fallecidas.

En virtud de esta disposición, los familiares, de hecho o de derecho, los herederos, los albaceas digitales —según las instrucciones recibidas—, los representantes legales de menores fallecidos, o el Ministerio Fiscal, en su defecto, y los coadyuvantes de personas con discapacidad fallecidas podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.

Ahora bien, los familiares, de hecho o de derecho, y los herederos, no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo estableciese una ley. No obstante, esta prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

1.4.2. Los derechos de los titulares de los datos personales

1.4.2.1. El elenco de derechos en materia de protección de datos[27]

— *El derecho a ser informado*

De acuerdo con el art. 13 RGPD, cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que los recabe, facilitará al mismo toda la información indicada en el citado precepto, salvo que dicho interesado ya disponga de ella. De entre este amplio conjunto, a los efectos del presente estudio, se puede destacar: *a)* la identidad y los datos de contacto del responsable del tratamiento; *b)* los datos de contacto del DPD; *c)* los fines del tratamiento a que se destinan los datos personales y la base jurídica del mismo; *d)* el plazo durante el cual se conservarán los datos; *e)* la existencia de los derechos de acceso, oposición, limitación,

---

[27] Para un análisis más detallado de estos derechos, se puede acudir, entre otros, a: J. P. Murga Fernández, «Derechos de los individuos», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 77 y ss., y J. Aparicio Salom, «Capítulo 9. Derechos del interesado», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 345 y ss.

rectificación o supresión de datos personales, así como del derecho a la portabilidad de los datos y la existencia del derecho a retirar el consentimiento en cualquier momento; *f)* el derecho a presentar una reclamación ante una autoridad de control; *g)* el hecho de que, en su caso, la comunicación de datos personales es un requisito legal, de que el interesado está obligado a facilitarlos y de las posibles consecuencias de no hacerlo, y *h)* la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como sobre la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Según el art. 11.1 y 2 LOPDP, el cumplimiento de este deber se puede llevar a cabo facilitando al afectado una información básica (la identidad del responsable del tratamiento, la finalidad del tratamiento, la intención de elaborar perfiles y los derechos que le asisten, incluido el derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente) e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. Se consagra, de este modo, legislativamente, el sistema de información por capas o niveles[28].

A su vez, de conformidad con el art. 14 RGPD, cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento facilitará a este la información indicada en dicho precepto. Esta información coincide, sustancialmente, con la establecida en el art. 13 RGPD, si bien se incorpora el deber de indicar las categorías de datos personales de que se trate y el origen del que proceden los mismos, especificando, en su caso, si se han conseguido de fuentes de acceso público. La antedicha información se proporcionará: *i)* dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes; *ii)* si los datos personales han de utilizarse para la comunicación con el interesado, a más tardar en el momento de la primera comunicación con dicho interesado, o *iii)* si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez. No obstante, no será necesario facilitar la información: *a)* si el interesado ya dispone de ella; *b)* si la comunicación de tal información resulta imposible o supone un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o en la medida en que esta obligación pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento (en estos casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información); *c)* si la obtención o la comunicación está expresamente establecida por una disposición legal, cuando esta contenga medidas adecuadas para proteger

[28] *Vid.*, sobre este sistema, E. Chaveli Donet y P. Monreal Vilanova, «Configuración de los derechos de las personas tras la reforma. Su ejercicio en el ámbito local», en C. Campos (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 154-163. Un modelo del mismo, aplicable a los entes locales, se puede encontrar en *https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf* (consultada en abril de 2019).

los intereses legítimos del interesado, o *d)* si los datos personales deben seguir teniendo carácter confidencial, sobre la base de una obligación de secreto profesional.

De acuerdo con el art. 11.3 LOPDP, el cumplimiento de este deber de información se podrá realizar facilitando al interesado la información básica (la misma referida más arriba, pero sumándole: las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos), e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Tanto en el caso de los datos obtenidos del interesado como de otra fuente, si el responsable proyecta el tratamiento posterior de los mismos, para un fin que no sea aquel para el que se recogieron u obtuvieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información adicional pertinente (arts. 13.3 y 14.4 RGPD).

Según el art. 12 RGPD, la comunicación de esta información, así como cualquier comunicación relativa a los derechos de los interesados, además de ser gratuita, ha de realizarse: en primer lugar, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo (en particular, cualquier información dirigida específicamente a un niño), y, en segundo lugar, por escrito o por otros medios, inclusive, si procede, por medios electrónicos, salvo que el interesado solicite que se le facilite verbalmente. En este último sentido, cabe destacar que la información que deberá facilitarse a los interesados, en virtud de los citados arts. 13 y 14 RGPD, podrá transmitirse en combinación con iconos normalizados que permitan proporcionar, de forma fácilmente legible y comprensible, una adecuada visión de conjunto del tratamiento previsto[29].

— *El derecho de acceso*

De conformidad con el art. 15 RGPD, 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, tendrá derecho de acceso a los datos personales y a la información relativa al tratamiento (que, esencialmente, coincide con la analizada en el punto anterior).

Cuando el antedicho responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso, sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que especifique los datos o actividades de tratamiento a los que se refiere su solicitud (art. 13.1 LOPDP).

Para hacer efectivo este derecho, el responsable del tratamiento facilitará al interesado una copia de los datos personales objeto de tratamiento, eso sí, sin afectar negativamente a los derechos y libertades de otros. Cuando se presente la solicitud por medios electrónicos, y a menos que se solicite que se entregue de otro modo, la información

---

[29] *Vid.* J. Puyol Montero, «Transparencia de la información y derecho de acceso de los interesados en la nueva normativa de protección de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 275 y ss.

se facilitará en un formato electrónico de uso común. Sin perjuicio de la gratuidad del ejercicio de este derecho, el responsable podrá percibir, por cualquier otro tipo de copia solicitada por el interesado, un canon razonable, basado en los costes administrativos (art. 15 RGPD).

El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilita al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho (art. 13.2 LOPDP). Ello sin perjuicio de que el interesado pueda solicitar, en todo momento, al responsable la información referida a los extremos que no se incluyan en el sistema de acceso remoto.

— *El derecho de rectificación*

De acuerdo con el art. 16 RGPD, el interesado tendrá derecho a obtener, sin dilación indebida, del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Ello incluye el que, teniendo en cuenta los fines del tratamiento, el mismo tenga derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Al ejercer el derecho de rectificación el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Además, deberá adjuntar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento (art. 14 LOPDP).

— *El derecho de supresión o derecho al olvido*

Según el art. 17 RGPD, el interesado tendrá derecho a obtener del responsable del tratamiento la supresión de los datos personales que le conciernan. Este último estará obligado a eliminar, sin dilación indebida, los datos personales, si concurre alguna de las circunstancias siguientes: *a)* cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron obtenidos; *b)* cuando el interesado retire el consentimiento en que se basa el tratamiento, y este no pueda apoyarse en otro fundamento jurídico; *c)* cuando el interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento; *d)* cuando los datos personales hayan sido tratados ilícitamente, y *e)* cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal.

No obstante, no se procederá a la supresión de los datos cuando su tratamiento sea necesario: *i)* para ejercer el derecho a la libertad de expresión e información; *ii)* 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 conferidos al responsable; *iii)* para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado pudiera hacer imposible

u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o *iv)* para la formulación, el ejercicio o la defensa de reclamaciones.

Además, cuando haya hecho públicos los datos personales y esté obligado a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará las medidas razonables, incluidas medidas técnicas, 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 de cualquier copia o réplica de los mismos[30].

— *El derecho a la limitación del tratamiento*

De conformidad con el art. 18 RGPD, el interesado tendrá derecho a obtener del responsable la limitación del tratamiento de los datos, cuando se cumpla alguna de las condiciones siguientes: *a)* cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la corrección de los mismos; *b)* cuando 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; *c)* cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones, y *d)* cuando el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

De acuerdo con el art. 16.2 LOPDP, el hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Cuando el tratamiento de datos personales se haya limitado, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público prevalente.

Finalmente, hay que señalar que todo interesado que haya obtenido la limitación del tratamiento será informado por el responsable antes del levantamiento de dicha limitación.

— *El derecho a la portabilidad de los datos*

De conformidad con el art. 20.1 RGPD, el interesado tendrá derecho a recibir, sin afectar negativamente a los derechos y libertades de otros, los datos personales que le

---

[30] *Vid.* B. ADSUARA, «Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento)», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 313 y ss.

incumban y que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento cuando el tratamiento esté basado en el consentimiento o en un contrato y el mismo se efectúe por medios automatizados.

Es importante destacar, a los efectos de las Administraciones locales, que este derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Al ejercer esta facultad, el interesado tendrá derecho, además, a que los datos se transmitan directamente de responsable a responsable, siempre que sea técnicamente posible.

— *El derecho de oposición*

De acuerdo con el art. 21.1 RGPD, el interesado tendrá derecho a oponerse, en cualquier momento, por motivos relacionados con su situación particular, a que los datos personales que le conciernan sean objeto de un tratamiento basado en la necesidad de satisfacer un interés publico o un interés legítimo [art. 6.1.*e)* o *f)* RGPD], incluida la elaboración de perfiles. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. En este punto, teniendo en cuenta la naturaleza de los intereses enfrentados, las Administraciones locales han de ser especialmente cuidadosas a la hora de efectuar las respectivas ponderaciones.

A más tardar, en el momento de la primera comunicación con el interesado, el derecho de oposición será mencionado de forma explícita y presentado de modo claro y al margen de cualquier otra información.

— *El derecho a no ser objeto de decisiones basadas en tratamientos automatizados*

Según el art. 22 RGPD, todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos, incluida la elaboración de perfiles, que produzca efectos en su esfera jurídica o que le afecte significativamente de modo similar.

Si no se trata de categorías especiales de datos personales, o siendo así, en los supuestos normativamente autorizados [art. 9.2.*a)* o *g)* RGPD], si se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, no se podrá oponer este derecho al responsable del tratamiento en los siguientes supuestos: *a)* si el tratamiento automatizado está autorizado por una disposición legal que establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; *b)* si el tratamiento automatizado se basa en el consentimiento

explícito del interesado, o *c)* si el tratamiento automatizado es necesario para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento. En los dos últimos supuestos, el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, garantizando, como mínimo, el derecho a obtener una intervención humana, el derecho a realizar alegaciones y el derecho a impugnar la decisión[31].

— *El derecho al resarcimiento por los daños*

De conformidad con el art. 82.1 RGPD, toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de la normativa en materia de protección de datos tendrá derecho a recibir del responsable o del encargado del tratamiento una indemnización por tales daños y perjuicios padecidos[32].

1.4.2.2. Forma de ejercicio y sistema de tutela de los derechos

— *Forma de ejercicio de los derechos*

Los responsables del tratamiento están obligados a informar a los interesados sobre los medios a su disposición para ejercer los derechos que le corresponden.

Dichos medios han de ser fácilmente accesibles. Además, han de ser gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, salvo en contadas excepciones, normativamente previstas. Así, por ejemplo, cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: *a)* cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o *b)* negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud. En este sentido, para aligerar esta carga, en el art. 13.3 de la LOPDP se establece que se podrá considerar repetitivo el ejercicio del derecho de acceso, en más de una ocasión, durante el plazo de seis meses, a menos que exista una causa legítima para ello.

Cuando el afectado elija un medio distinto al que se le ofrece para el ejercicio de un derecho, este no podrá ser denegado por ese solo motivo. Ahora bien, si el medio de-

---

[31] *Vid.* J. Aparicio Salom, «Capítulo 11. Derecho de oposición y decisiones individuales automatizadas», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 397 y ss.

[32] *Vid.* E. Nieto Garrido, «Derecho a indemnización y responsabilidad», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 555 y ss.

mandado supone un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Los citados derechos podrán ejercerse directamente o por medio de representante, legal o voluntario, como recuerda el art. 12 LOPDP. Asimismo, en cualquier caso, los titulares de la patria potestad podrán ejercitar, en nombre y representación de los menores de catorce años, los derechos que pudieran corresponderles.

Cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud, podrá reclamar que se le facilite la información adicional necesaria para confirmar la identidad del interesado (art. 12.6 RGPD).

El responsable del tratamiento ofrecerá al interesado información relativa a sus actuaciones respecto de la solicitud del mismo, en el plazo de un mes, a partir de la recepción de esta. Dicho plazo podrá prorrogarse otros dos meses en caso de ser necesario, teniendo en cuenta la complejidad y el número de solicitudes. En todo caso, el responsable informará al interesado de la prórroga, indicando los motivos del retraso. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin tardanza, tanto de las razones de su no actuación, como de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales[33].

— *Sistema de tutela de los derechos*

De acuerdo con el art. 77 RGPD, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, si considera que un tratamiento de datos personales que le conciernen infringe la normativa de protección de datos.

Por otro lado, en virtud del art. 78 RGPD, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

Finalmente, el art. 79 RGPD consagra el derecho de todo interesado a reclamar directamente contra el responsable del tratamiento, en vía judicial, cuando considere que sus derechos en virtud de la normativa de protección de datos han sido vulnerados[34].

---

[33] *Vid.* J. A. Hernández Corchete, «Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 205 y ss.

[34] *Vid.* M. Recio Gallo, «Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, p. 539.

2. Aspectos objetivos

2.1. Los datos personales

2.1.1. Concepto

Según el art. 4.1 RGPD, se considera un «dato personal» toda información sobre una persona física identificada o identificable. A estos efectos, se entiende que una persona física es identificable cuando su identidad puede 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.

Los citados datos se conservan, para su tratamiento, en ficheros. Estos, de acuerdo con el art. 4.6 RGPD, son cualquier conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

2.1.2. Tipología: las categorías especiales de datos y las limitaciones a su tratamiento

En función del grado de protección creciente que se les otorga, los datos se dividen en: datos personales y datos personales pertenecientes a una categoría especial[35].

De conformidad con el art. 9.1 RGPD, tienen la consideración de categorías especiales de datos: los datos genéticos[36] y los datos relativos a la salud[37]; los datos biométricos[38], dirigidos a identificar de manera unívoca a una persona física, y los datos que revelen el origen étnico o racial; los datos que pongan de manifiesto las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical y los datos relativos a la vida sexual o la orientación sexual.

---

[35] *Vid.* M. Medina Guerrero, «Categorías especiales de datos», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 251 y ss.

[36] El RGPD define los «datos genéticos» como 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.

[37] El RGPD considera que los «datos relativos a la salud» son aquellos datos personales relativos a la salud corporal o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. De acuerdo con el considerando 35 RGPD, entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro.

[38] El RGPD establece que los «datos biométricos» son 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.

Con carácter general, el tratamiento de estos datos está prohibido. Excepcionalmente, será posible, si concurre alguna de las circunstancias recogidas en el art. 9.2 RGPD, como, por ejemplo, que el tratamiento sea consentido o que sea necesario por razones de un interés público esencial.

No obstante, si se trata de datos genéticos, datos biométricos o datos relativos a la salud, y siempre que sea preciso, de conformidad con el Derecho español, dicha circunstancia deberá hallarse amparada por una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

Por otro lado, de acuerdo con el art. 9 LOPDP, hay que señalar que, a fin de evitar situaciones discriminatorias, se prohíbe que el solo consentimiento del afectado baste para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico[39].

2.2. El tratamiento de los datos personales

2.2.1. Concepto

Según el art. 4.2 RGPD, el «tratamiento» se define como 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.

2.2.2. Principios relativos al tratamiento de datos personales[40]

2.2.2.1. Principios básicos

— *Principios relativos a la recogida de datos*

En primer lugar, se halla el principio de licitud. De acuerdo con este principio, consagrado en el art. 5 RGPD, los datos han de ser recogidos de forma legítima, esto es,

---

[39] En la Exposición de Motivos de la LOPDP, se puede leer la siguiente justificación de esta decisión: «Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del art. 9.2.*b)* del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del art. 9.2.*d)* de la misma norma europea».

[40] Además de los principios recogidos en el presente trabajo, algún autor ha propuesto considerar, de manera específica, en esta disciplina, otros principios, como el proporcionalidad. *Vid.* A. Palma Ortigosa,

su recopilación ha de contar con una adecuada justificación[41]. Así, el tratamiento será legítimo si se apoya en alguna de las siguientes bases[42]:

A) 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.

B) Es necesario para proteger intereses vitales del interesado o de otra persona física.

C) Es necesario para el cumplimiento de una obligación normativamente exigible al responsable del tratamiento. De conformidad con el art. 8 LOPDP, tal norma, con rango de ley, podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan. Además, dicha disposición legal podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras pertinentes.

D) Es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. De acuerdo con el art. 8 LOPDP, el tratamiento de datos personales solo podrá considerarse fundado en este supuesto, cuando derive de una competencia atribuida por una norma con rango de ley. A la luz del principio de autonomía local, esta cláusula ha de ser interpretada, en el caso de las entidades locales, de forma amplia, de manera que dentro de la misma se engloben tanto las competencias propias necesarias, como las competencias propias suplementarias[43].

E) 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. Hay que destacar que esta justificación no puede ser empleada por las autoridades públicas, incluidas las locales, en el ejercicio de sus funciones.

F) Es conforme con el consentimiento expresado por el interesado relativo al tratamiento de sus datos personales para uno o varios fines específicos.

Según lo dispuesto en el art. 4.11 RGPD, el consentimiento del afectado es toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de sus datos personales[44].

«Principios relativos al tratamiento de datos personales», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 39 y ss.

[41] *Vid.* N. Martos Díaz, «Capítulo 8. Principios», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 333 y ss.

[42] *Vid.* C. Trujillo Cabrera, «Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 51 y ss.

[43] Cfr. M. Almeida Cerreda, «La redelimitación de las competencias de los municipios en materia de educación, sanidad, salud y servicios sociales y su transferencia parcial a las Comunidades Autónomas», en T. Quintana López (dir.), *La reforma del régimen local,* Tirant lo Blanch, Valencia, 2014, p. 116.

[44] *Vid.* M. Vilasau Solana, «El consentimiento general y de menores», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 197 y ss.

Así, como recuerda el considerando 32 RGPD: «El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio *web* en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento»[45].

No obstante, de acuerdo con el art. 7.1 LOPDP, el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años, exceptuados los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o de la tutela para la celebración del acto o negocio jurídico en cuyo contexto se recabe el consentimiento. En consecuencia, el tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela.

En todo caso, para que el consentimiento sea una base adecuada para el desarrollo de un determinado tratamiento de datos, de acuerdo con los arts. 6 y 7 RGPD, han de darse las siguientes condiciones: *a)* no se podrá supeditar la ejecución de un contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual; *b)* cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades, será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas, y *c)* el responsable deberá ser capaz de demostrar que el interesado consintió en el tratamiento de sus datos personales.

---

[45] Esta exigencia del RGPD chocaba con el modelo de acceso a datos personales en el marco de procedimientos administrativos, contenido en el art. 28.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP). Según este precepto, se presumía que la consulta u obtención de datos, en el seno de un procedimiento, era autorizada por interesados, salvo que constase su oposición expresa o una ley requiriese el consentimiento expreso de los mismos para la realización de tales actividades.

Esta antinomia normativa ha sido resuelta por la DF 12.ª de la LOPDP, que da nueva redacción al art. 28.2 LPACAP. Según el nuevo tenor literal de este precepto, la Administración actuante en el procedimiento de que se trate podrá consultar o recabar documentos que ya se encuentren en su poder o hayan sido elaborados por cualquier otra Administración, salvo que el interesado se opusiera a ello. No obstante, no cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección. Como se puede inferir de este nuevo texto normativo, el Legislador español ya no funda la capacidad de las Administraciones de recabar documentos en un consentimiento presunto de los interesados, que no es compatible con el RGPD, sino en que dicha actuación es necesaria para el cumplimiento de una misión realizada en el ejercicio de poderes públicos, que es otra de las bases de legitimación.

Vid. L. Do Nascimento López, «Cuestiones prácticas para la directa aplicación de la normativa de protección de datos en las Administraciones Públicas», *REGAP,* núm. 57, 2019, en publicación.

Por último, hay que señalar que el interesado tendrá derecho a retirar su consentimiento en cualquier momento, de lo cual será informado antes de otorgarlo. Ahora bien, la retirada del consentimiento no afectará a la licitud de los tratamientos basados en él, efectuados antes de la misma. En este punto, el RGPD ordena que sea tan fácil retirar el consentimiento como darlo.

En segundo lugar, se encuentra el principio de finalidad limitada, consagrado en el art. 5.1.*b)* RGPD. De acuerdo con este principio, los datos han de ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. En este sentido, en el considerando 50 RGPD se aclara: «El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si 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, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros».

En tercer lugar, se halla el principio de minimización de datos, positivizado en el art. 5.1.*c)* RGPD. De conformidad con el mismo, tan solo se recabarán los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que los mismos sean tratados.

En cuarto lugar, se encuentra el principio de exactitud, recogido en el art. 5.1.*d)* RGPD. Según esta norma, los datos han de ser exactos y, si fuera necesario, han de ser actualizados. Este principio, en consecuencia, obliga a que se adopten todas las medidas razonables para que se supriman o rectifiquen, sin demora, los datos personales que sean inexactos, con respecto a los fines para los que se tratan. La LOPDP, en su art. 4.2, establece que, al responsable del tratamiento, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, cuando los datos inexactos: *a)* hubiesen sido obtenidos por el responsable directamente del afectado; *b)* hubiesen sido obtenidos por el responsable de un mediador o intermediario autorizado; *c)* fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o *d)* fuesen obtenidos por el responsable de un registro público.

— *Principios relativos a los tratamientos de datos*

En primer lugar, en este ámbito, rige el principio de trato leal y transparente de los datos en relación con el interesado, consagrado en el art. 5.1.*a)* RGPD.

Este principio exige, por una parte, que, en toda ocasión, para los interesados debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen (cdo. 39 RGPD). Y, por otra parte, el mismo prin-

cipio impone que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y sencilla de entender, por lo que en las mismas se ha de emplear un lenguaje claro y simple (cdo. 39 RGPD).

En segundo lugar, en el campo del tratamiento, opera el principio de limitación de la conservación de los datos. De conformidad con este principio, contenido en el art. 5.1.*d)* RGPD, los datos han de ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines de cada tratamiento. No obstante, los datos personales podrán conservarse durante periodos más largos, siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

En tercer lugar, en este sector, se han de respetar los principios de integridad y confidencialidad, tal y como se configuran en el art. 5.1.*f)* RGPD. Así, los datos personales han de ser tratados de tal manera que se garantice su adecuada seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas apropiadas. Entroncado directamente con este principio, se halla el deber de confidencialidad, desarrollado en art. 5 LOPDP. De acuerdo con el mismo, los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas a un deber específico de confidencialidad, que será complementario de los deberes de secreto profesional que les afecten y cuya vigencia se extiende aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

2.2.3. Metaprincipios

Con el término metaprincipios, en este contexto, se pretende hacer referencia a dos axiomas que, en su seno, condensan la esencia de los principios antes enunciados y de ella hacen derivar nuevas consecuencias que se proyectan sobre el diseño y la ejecución de los tratamientos de datos[46].

2.2.3.1. Responsabilidad proactiva

Este metaprincipio se encuentra positivizado en el art. 5.2 RGPD. El mismo exige, a todos los operadores que intervienen en el tratamiento de datos, tener una actitud

[46] *Vid.* R. Duaso Calés, «Los principios de protección de datos desde el diseño y protección de datos por defecto», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 295 y ss.; S. Lorenzo, A. Palma y C. Trujillo, «Responsabilidad proactiva», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 143 y ss.; y R. Miralles López, «Capítulo 13. Protección de datos desde el diseño y por defecto», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 421 y ss.

consciente, vigilante y diligente, de tal modo que ello les lleve a controlar de forma permanente y activa el diseño y desarrollo de dicho tratamiento. Esto implica que tales operadores han de determinar, en cada momento, qué medidas técnicas y organizativas son las apropiadas, según las circunstancias, para asegurar el cumplimiento de las obligaciones en materia de protección de datos; anticipándose, siempre, a cualquier tipo de acontecimiento, potencialmente dañoso, más o menos previsible, que pudiera acaecer. En consecuencia, obrando así, en todo tiempo, dichos operadores han de poder demostrar que el antedicho tratamiento se ajusta perfectamente a la normativa de protección de datos vigente[47].

2.2.3.2. Protección de datos desde el diseño y por defecto

El correcto cumplimiento de este metaprincipio, recogido en el art. 25 RGPD, requiere que los operadores jurídicos dispongan y ejecuten dos conjuntos de medidas técnicas y organizativas.

En primer lugar, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento, como en el momento de efectuar el propio tratamiento, las medidas técnicas y organizativas apropiadas (como la seudonimización), para cumplir de forma efectiva la normativa de protección de datos y asegurar los derechos de los interesados. La adecuación de dichas medidas se valorará teniendo en cuenta el estado de la técnica, el coste de su aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña dicho tratamiento para los derechos y libertades de los interesados.

En segundo lugar, el responsable del tratamiento implementará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. 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 una persona, a un número indeterminado de sujetos.

3. Aspectos organizativos

3.1. La evaluación de riesgos y la consulta previa

De conformidad con el art. 35.1 RGPD, los responsables de los tratamientos han de realizar, antes de iniciar los mismos, una evaluación del impacto de estos en la pro-

---

[47] Cfr. *https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf* (consultado en abril de 2019).

tección de los datos personales, cuando sea probable que dichos tratamientos, por su naturaleza, alcance, contexto, fines o medios (en especial, por el empleo de nuevas tecnologías) puedan entrañar un alto riesgo para los derechos y libertades de las personas físicas[48].

En todo caso, dicha evaluación será necesaria cuando se realice: *a)* una valoración sistemática y exhaustiva de aspectos personales de individuos que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para tales individuos o que les afecten significativamente de modo similar; *b)* un tratamiento a gran escala de categorías especiales de datos, o *c)* una observación sistemática a gran escala de una zona de acceso público[49].

Para incrementar la seguridad jurídica en este ámbito, el RGPD ordena que la autoridad de control, competente en cada territorio, establezca y publique una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto[50].

La antedicha evaluación incluirá como mínimo: *a)* una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; *b)* una evaluación de la necesidad y de la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; *c)* una evaluación de los riesgos para los derechos y libertades de los interesados, y *d)* las medidas previstas para afrontar los riesgos, incluidas las garantías, las medidas de seguridad y los mecanismos que avalen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Por otro lado, de acuerdo con el art. 36 RGPD, el responsable está obligado a consultar a la autoridad de control antes de proceder a un determinado tratamiento de datos, cuando una evaluación de impacto relativa a la protección de los datos evidencie que dicho tratamiento entraña un alto riesgo, si el responsable no toma las medidas

---

[48] *Vid.*, sobre las metodologías para elaborar esta evaluación, entre otros: M. Recio Gallo, «Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 351 y ss.; D. de la Prada Espina, «Evaluación de impacto de protección de datos», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 477 y ss.; R. Miralles López, «Capítulo 19. Evaluación de impacto relativa a la protección de datos y consulta previa», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 469 y ss.

[49] Cuando el tratamiento tenga su base jurídica en el Derecho de la Unión o en el Derecho de un Estado miembro, si tal Derecho regula la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, no será necesaria la realización de una evaluación de riesgos, excepto si el Estado considera necesario proceder a dicha evaluación.

[50] La AEPD ha hecho público, en mayo de 2019, el listado de tratamientos de datos personales en los que es obligatoria la realización de una evaluación de impacto (*vid. https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf,* última consulta en mayo de 2019).

oportunas para mitigarlo [51]. En estos supuestos, si la autoridad de control considera que el tratamiento previsto podría infringir la normativa en materia de protección de datos, en particular cuando el responsable no ha identificado o mitigado suficientemente los riesgos, dicha autoridad deberá asesorar por escrito al responsable, y, en su caso, al encargado, y podrá utilizar cualquiera de sus poderes para asegurar el adecuado cumplimiento de la citada normativa.

3.2. El registro de actividades de tratamiento

Los responsables y encargados del tratamiento o, en su caso, sus representantes, según el art. 30 RGPD, deberán mantener un registro de actividades de tratamiento, por escrito, inclusive en formato electrónico, salvo que operen a través de organizaciones que empleen a menos de 250 personas y que no realicen, habitualmente, tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados o que incluyan categorías especiales de datos personales. No obstante, de acuerdo con el art. 31.2 LOPDP, las Administraciones locales, cualquiera que sean sus dimensiones y actividades, han de hacer público un inventario de sus actividades de tratamiento que sea accesible por medios electrónicos; en él, ha de constar la base legal de los tratamientos y la información que el art. 30 RGPD exige que se incorpore a los registros de tratamiento de actividades. En este mismo sentido, en el art. 6 bis de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (en adelante, LTBG), se ordena que las Administraciones locales, en cuanto sujetos incluidos en el art. 77.1 LOPDP, publiquen su inventario de actividades de tratamiento.

De modo somero, se puede sintetizar el contenido de dichos registros, señalando que los mismos contendrán: *a)* el nombre y los datos de contacto de los responsables/encargados/representantes y de los DPD; *b)* los fines de los tratamientos; *c)* una descripción de las categorías de interesados y de las categorías de datos personales; *d)* las categorías y actividades de tratamiento; *e)* las categorías de destinatarios a quienes se comunicarán los datos personales; *f)* en su caso, las transferencias de datos personales a un tercer país; *g)* cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos, y *h)* cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad [52].

---

[51] No obstante, el Derecho nacional podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

[52] *Vid.* R. Costa Hernandis, «Capítulo 15. Registro de actividades del tratamiento», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 437 y ss.

3.3. La seguridad en el tratamiento

3.3.1. Las medidas y el nivel de seguridad

De conformidad con el art. 32 RGPD, el responsable y el encargado del tratamiento aplicarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que cada tratamiento pueda implicar[53].

La determinación de este nivel adecuado de seguridad se hará teniendo en cuenta: en primer lugar, el alcance, el contexto y los fines del tratamiento; en segundo lugar, el estado de la técnica y los costes de aplicación de las medidas de seguridad, y, en tercer lugar, la probabilidad y la gravedad de los riesgos para los derechos y libertades de las personas físicas, en especial, han de considerarse, en este punto, los riesgos que presente el tratamiento como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales o la comunicación o acceso no autorizados a los mismos.

En todo caso, entre las citadas medidas técnicas y organizativas, se incluirán las adecuadas para garantizar: *a)* la seudonimización y el cifrado de datos personales; *b)* la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; *c)* la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, y *d)* un proceso de verificación, evaluación y valoración regulares de la eficacia de dichas medidas. Además, en virtud de la DA 1.ª LOPDP, las entidades locales deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de entre las previstas en el Esquema Nacional de Seguridad; en especial, aquellas que se establezcan para evitar la pérdida, alteración o acceso no autorizado a los datos personales[54].

3.3.2. La reacción frente a violaciones de seguridad

En caso de violación de la seguridad de los datos personales, de conformidad con el art. 33 RGPD, el encargado del tratamiento notificará la misma, sin dilación indebida, al responsable del tratamiento.

---

[53] *Vid.* C. Romero Ternero, «Seguridad de la información», en J. P. Murga, M.ª de los Á. Fernández y M. Espejo Lerdo (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 401 y ss., e I. González Ubierna, «Capítulo 17. Seguridad del tratamiento», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 449 y ss.

[54] En este punto, es necesario destacar que las entidades locales tiene otras dos obligaciones. En primer lugar, impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones sujetas al Derecho privado y vinculadas a las mismas. Y, en segundo lugar, garantizar que, en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad que aplique se corresponden con las de la propia entidad local y que se ajustan al Esquema Nacional de Seguridad. Sobre este último y sus exigencias, *vid.* I. Alamillo Domingo, «Esquema Nacional de Seguridad: la administración electrónica y la seguridad de la información», en C. Campos (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 607 y ss.

Este, a su vez, si dicha violación de seguridad constituye un riesgo para los derechos y las libertades de las personas físicas, la notificará, sin demora (y en todo caso antes de que transcurran setenta y dos horas desde que haya tenido constancia de ella), a la autoridad de control competente[55].

En la citada notificación, como mínimo, se deberá: *a)* describir la naturaleza de la violación de seguridad, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; *b)* comunicar el nombre y los datos de contacto del DPD o de otro punto de contacto en el que pueda obtenerse más información; *c)* describir las posibles consecuencias de la violación de seguridad de los datos personales, y *d)* describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de seguridad, especificando, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Además de la antedicha notificación, de acuerdo con el art. 34 RGPD, cuando sea probable que la violación de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará a los interesados. Esta comunicación describirá, en un lenguaje claro y sencillo, la naturaleza de la violación de seguridad y contendrá, esencialmente, la información antes indicada. No obstante, no será preciso realizar esta comunicación si: *a)* como resultado de las medidas de protección adoptadas por el responsable del tratamiento, como el cifrado, los datos personales son ininteligibles para cualquier persona que no esté autorizada a acceder a ellos; *b)* el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no se concretizará un alto riesgo para los derechos y las libertades de los interesados, y *c)* la comunicación individualizada suponga un esfuerzo desproporcionado; en este último caso, se optará por una comunicación pública o una medida semejante que permita informar de manera igualmente efectiva a todos los interesados.

En todo caso, el responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas[56].

3.4. El bloqueo de datos

De acuerdo con el art. 32 LOPDP, el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión, salvo en los supuestos expresamente excepcionados por la AEPD o las autoridades autonómicas.

---

[55] Si la notificación a la autoridad de control no tiene lugar en el plazo de setenta y dos horas, deberá ir acompañada de una adecuada motivación de la dilación.

[56] *Vid.* M. Carpio Cámara, «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 335 y ss., y F. Pérez Bes, «Capítulo 18. La obligación de notificar una violación de seguridad de datos personales», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 457 y ss.

Según este mismo precepto, el citado bloqueo consiste en la identificación y reserva de los datos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para su puesta a disposición de Jueces y Tribunales, del Ministerio Fiscal o de las Administraciones públicas competentes, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3.5. La responsabilidad por el tratamiento

La infracción de las normas de protección de datos puede dar lugar a diferentes tipos de responsabilidad: patrimonial, sancionadora y disciplinaria.

En primer lugar, como ya se ha explicado antes, los ciudadanos tienen derecho a ser resarcidos por los daños y perjuicios que les ocasionen las infracciones de la normativa de protección de datos que les afecten. En consecuencia, las Administraciones locales deberán indemnizar a los interesados que se vean lesionados por sus acciones u omisiones que supongan un incumplimiento de la citada regulación. Lógicamente, ello se hará conforme a la normativa de responsabilidad patrimonial de las Administraciones públicas[57].

En segundo lugar, hay que señalar que, de conformidad con el art. 77.2 y 1.*c)* LOPDP, cuando una Administración local, en cuanto responsable o encargada de un tratamiento, cometa alguna de las infracciones tipificadas en los arts. 72 a 74 de la LOPDP, la Autoridad de protección de datos que resulte competente dictará resolución sancionando a la misma con apercibimiento[58]. Dicha resolución establecerá, asimismo, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. Esta resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso. Por otro lado, estas resoluciones se publicarán, cuando la autoridad competente sea la AEPD, en su página web, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción[59].

---

[57] La redacción del art. 82.1 RGPD parece apuntar a la existencia de una responsabilidad patrimonial objetiva, en este ámbito; reforzando, de este modo, la tradicional caracterización de la responsabilidad patrimonial de las Administraciones públicas en España.

[58] *Vid.* A. Corral Sastre, «El régimen sancionador en materia de protección de datos en el reglamento general de la Unión Europea», en J. L. Piñar (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 571 y ss., y N. Brito Izquierdo, «Capítulo 25. Recursos, responsabilidad y sanciones», en J. López (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 663 y ss.

[59] Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

En tercer lugar, a los empleados públicos, a los que sea imputable una violación de la normativa de protección de datos, se les exigirá la correspondiente responsabilidad disciplinaria. En este sentido, el art. 72.3 LOPDP ordena que la autoridad de protección de datos proponga, tras la sanción a una entidad local, la iniciación de actuaciones disciplinarias respecto de los empleados públicos correspondientes, cuando existan indicios suficientes para ello.

En este caso, el procedimiento a seguir y las sanciones a imponer serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación. En todo caso, además, según este mismo precepto, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción a la entidad local de que se trate, se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el *Boletín Oficial del Estado* o autonómico que corresponda.

IV. ALGUNOS PUNTOS CRÍTICOS EN LA APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN EL ÁMBITO LOCAL

1. Cuestiones relativas al tratamiento y uso de datos

1.1. Cuestiones relativas al tratamiento de datos en el ámbito de la gestión de recursos humanos

De conformidad con la DA 12.ª LOPDP, los tratamientos de los registros de personal del sector público, y, por ende, los de las Administraciones locales, se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables. Dichos registros podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

Asimismo, por concurrir una razón de interés público imperiosa, los datos cuyo tratamiento se halle limitado podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

1.2. Cuestiones relativas al tratamiento de datos en los procedimientos en materia de transparencia: en el acceso a la información y en la publicidad activa

De acuerdo con el art. 15.4 LTBG, si el acceso a una determinada información o la publicidad activa de la misma se efectúa previa disociación de los datos de carácter

personal, de modo que se impida la identificación de las personas afectadas, nada obsta, desde el punto de vista de la protección de datos, a dichas actuaciones.

Ahora bien, si no se efectúa dicha disociación a la hora de atender a peticiones de información, hay que distinguir dos conjuntos de supuestos. En primer lugar, si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, de acuerdo con el art. 15.1 LTBG, en este caso, únicamente se podrá autorizar el acceso si se cuenta con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos de que se trate, con anterioridad a que se pidiese el acceso. En un sentido similar, si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, comprendiese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley. En segundo lugar, cuando la información demandada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular, su derecho fundamental a la protección de datos de carácter personal.

1.3. Tratamientos en materia de policía y seguridad

1.3.1. Tratamientos con fines de vigilancia y control

De conformidad con los arts. 22 y 89 LOPDP, las Administraciones locales podrán llevar a cabo el tratamiento de imágenes, a través de sistemas de cámaras o videocámaras con dos finalidades: preservar la seguridad de las personas y bienes, así como de sus instalaciones, y controlar a los empleados públicos, de acuerdo con lo previsto en la legislación de función pública.

La primera posibilidad, no obstante, se halla condicionada, de conformidad con el art. 22 LOPDP, por dos límites fundamentales. En primer lugar, solo podrán captarse imágenes de la vía pública, en la medida en que resulte imprescindible, sin que, en ningún caso, se pueda filmar el interior de domicilios. Y, en segundo lugar, los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Respecto de estos tratamientos, hay que señalar que, por una parte, el deber de información se entenderá cumplido mediante la colocación de un dispositivo informativo en un lugar suficientemente visible, y, por otra parte, que a los mismos no les será aplicable la obligación de bloqueo.

La utilización de la segunda posibilidad, la videovigilancia de los empleados públicos, se halla condicionada a que las entidades locales informen con carácter previo, y de forma expresa, clara y concisa, a los empleados públicos, y, en su caso, a sus representantes, acerca de esta medida. No obstante, en el supuesto de que se haya captado la comisión flagrante de un acto ilícito, se entenderá cumplido el deber de informar, cuando existiese al menos el dispositivo informativo antes indicado. Además, en ningún caso, se admitirá la instalación de sistemas videovigilancia en lugares destinados al descanso o esparcimiento de los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

En esta línea de vigilancia de los empleados públicos, el art. 90 LOPDP permite que las entidades locales traten datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los empleados públicos previstas en la legislación de función pública. Con carácter previo, dichas entidades habrán de informar de forma expresa, clara e inequívoca a los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

No obstante lo dicho, hay que recordar que, de acuerdo con el art. 14.*j)* bis del Texto Refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, los empleados públicos tendrá derecho a la intimidad, frente al uso de dispositivos de videovigilancia y geolocalización. En consecuencia, la determinación de la licitud de la adopción de las anteriores medidas exige el control del respeto por las mismas del principio de proporcionalidad respecto de su incidencia sobre el derecho a la intimidad[60].

1.3.2. Tratamientos de datos relativos a infracciones y sanciones administrativas

De conformidad con el art. 27 LOPDP, dictado para complementar el art. 86 RGPD, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

Cuando no se cumpla alguna de las antedichas condiciones, estos tratamientos de datos habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley.

---

[60] Cfr. E. Chaveli Donet y P. Monreal Vilanova, «La garantía de los derechos digitales en la Ley de Protección de Datos», en C. Campos (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 244-246.

1.4. Tratamientos de datos en el marco de los sistemas de denuncias internas

De acuerdo con el art. 24.5 LOPDP, las Administraciones locales podrán crear y mantener sistemas de denuncias internas, a través de los cuales se pueda poner en conocimiento de las mismas, incluso anónimamente, la comisión en su seno o en la actuación de terceros que contraten con ellas, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que les es aplicable[61].

Este precepto, en relación con los datos contenidos en las antedichas denuncias, establece las siguientes reglas:

a) Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad local, en caso de que se hubiera identificado.

b) El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la Administración local, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un empleado, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

c) Los datos de quien formule la denuncia y de los empleados y terceros deberán conservarse en el sistema de información únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo.

1.5. Tratamientos de datos en el ámbito de los procedimientos administrativos

1.5.1. La facultad general de verificación de datos de las Administraciones locales

De conformidad con la DA 8.ª LOPDP, las Administraciones públicas —comprendidas, lógicamente, las locales— gozan de la potestad de contrastar los datos personales

---

[61] *Vid.* P. Llaneza González, «Tratamiento de datos con fines de videovigilancia y denuncias internas», en A. Rallo (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 793 y ss.

alegados por los interesados con los que obran en su poder. Así, según la citada disposición, cuando se formulen solicitudes por cualquier medio en las que los interesados declaren datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar, en el ejercicio de sus competencias, las verificaciones necesarias para comprobar la exactitud de dichos datos.

1.5.2. La facultad general de obtención de documentación administrativa por las Administraciones locales

El art. 28.2 LPACAP permite que todas las Administraciones públicas, en el seno de los procedimientos administrativos, consulten o recaben documentos que ya se encuentren en su poder o que hayan sido elaborados por cualquier otra Administración, salvo que el interesado se opusiera a ello. No obstante, según este mismo precepto, no cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Asimismo, de acuerdo con la citada norma, las Administraciones públicas no requerirán a los interesados documentos que hayan sido aportados anteriormente por los mismos ante cualquier Administración. A estos efectos, los interesados deberán indicar en qué momento y ante qué órgano administrativo presentaron los citados documentos, debiendo las Administraciones públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del/de los interesados o la ley especial aplicable requiera su consentimiento expreso.

1.5.3. La identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

La DA 7.ª LOPDP establece una serie de reglas que las Administraciones locales han de tener en cuenta a la hora de publicar o notificar mediante anuncios sus actos administrativos que contengan datos personales de los ciudadanos. Estas reglas son:

Primera. En ningún caso se debe publicar el nombre y apellidos de los interesados de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Segunda. Cuando el destinatario del acto careciera de cualquiera de los documentos antes mencionados, se le identificará únicamente mediante su nombre y apellidos.

Tercera. En la publicación de los actos administrativos, se identificará a los ciudadanos mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o

documento equivalente. Además, cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse[62].

Cuarta. En la notificación por medio de anuncios, en especial, en los supuestos de notificación infructuosa, se identificará a los interesados exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. Cuestiones relativas a las comunicaciones de datos

En este ámbito, es necesario recordar, en primer lugar, que, de acuerdo con el art. 33 LOPDP, el acceso por parte de un encargado del tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos.

Por otro lado, en segundo lugar, la DA 10.ª LOPDP autoriza a que las entidades locales comuniquen los datos personales que les sean solicitados por sujetos de Derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados, conforme a lo establecido en el art. 6.1.*f)* RGPD.

V. BIBLIOGRAFÍA

ADSUARA, B.: «Derechos de rectificación, supresión (olvido) y portabilidad (de los datos) y de limitación y oposición (al tratamiento)», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 313 y ss.

ALAMILLO DOMINGO, I.: «Esquema Nacional de Seguridad: la administración electrónica y la seguridad de la información», en C. CAMPOS (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 607 y ss.

ALMEIDA CERREDA, M.: «La redelimitación de las competencias de los municipios en materia de educación, sanidad, salud y servicios sociales y su transferencia parcial a las Comunidades Autónomas», en T. QUINTANA LÓPEZ (dir.), *La reforma del régimen local,* Tirant lo Blanch, Valencia, 2014, pp. 113 y ss.

[62] La aplicación por las diferentes Administraciones, en distintos casos, de esta regla, empleando fórmulas diversas, puede llevar a que se frustre el fin que persigue la norma, ya que se puede producir la publicación de diferentes cifras numéricas de los documentos identificativos en posiciones distintas en cada supuesto, posibilitando, en definitiva, la recomposición íntegra de dichos documentos. Para evitarlo, la Agencia Española de Protección de datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía han propuesto una orientación para la aplicación provisional de garantías de protección de la divulgación del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente de los interesados. Dicha propuesta se puede consultar en *http://www.avpd.euskadi.eus/contenidos/nota_prensa/20190304/es_def/adjuntos/Sorteo_Cifras_DNI-AVPD-es-eu.pdf* (consultado en abril de 2019).

APARICIO SALOM, J.: «Capítulo 9. Derechos del interesado», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 345 y ss.

— «Capítulo 11. Derecho de oposición y decisiones individuales automatizadas», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 397 y ss.

BRITO IZQUIERDO, N.: «Capítulo 25. Recursos, responsabilidad y sanciones», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 663 y ss.

CARPIO CÁMARA, M.: «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 335 y ss.

CERVERA NAVAS, L.: «El comité europeo de protección de datos», en A. RALLO (dir.*), Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 655 y ss.

CHAVELI DONET, E., y MONREAL VILANOVA, P.: «Configuración de los derechos de las personas tras la reforma. Su ejercicio en el ámbito local», en C. CAMPOS (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 143 y ss.

— «La garantía de los derechos digitales en la Ley de Protección de Datos», en C. CAMPOS (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 195 y ss.

CORRAL SASTRE, A.: «El régimen sancionador en materia de protección de datos en el reglamento general de la Unión Europea», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 571 y ss.

COSTA HERNANDIS, R.: «Capítulo 12. Responsabilidad del responsable del tratamiento», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 409 y ss.

— «Capítulo 15. Registro de actividades del tratamiento», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 437 y ss.

DE LA PRADA ESPINA, D.: «Evaluación de impacto de protección de datos», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 477 y ss.

DO NASCIMENTO LÓPEZ, L.: «Cuestiones prácticas para la directa aplicación de la normativa de protección de datos en las Administraciones Públicas», *REGAP*, núm. 57, 2019, en publicación.

DUASO CALÉS, R.: «Los principios de protección de datos desde el diseño y protección de datos por defecto», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 295 y ss.

FERNÁNDEZ, M.ª de los Á.; LORENZO, S.; MURGA, J. P., y PALMA, A.: «Normativas sectoriales afectadas por la protección de datos», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 275 y ss.

GONZÁLEZ UBIERNA, I.: «Capítulo 17. Seguridad del tratamiento», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 449 y ss.

HERNÁNDEZ CORCHETE, J. A.: «Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos», en J. L. PIÑAR (dir.), *Reglamento*

general de protección de datos. Hacia un nuevo modelo europeo de privacidad, Reus, Madrid, 2017, pp. 205 y ss.

LLANEZA GONZÁLEZ, P.: «Tratamiento de datos con fines de videovigilancia y denuncias internas», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 793 y ss.

LORENZO, S.; PALMA, A., y TRUJILLO, C.: «Responsabilidad proactiva», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 143 y ss.

MARTÍNEZ, R.: «El delegado de protección de datos», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 431 y ss.

MARTOS DÍAZ, N.: «Capítulo 8. Principios», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 333 y ss.

MEDINA GUERRERO, M.: «Categorías especiales de datos», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 251 y ss.

MIGUEZ MACHO, L.: «Normativa española con implicaciones en protección de datos», en C. CAMPOS (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* 2.ª ed., Wolters Kluwer, Madrid, 2019, pp. 69 y ss.

MIRALLES LÓPEZ, R.: «Capítulo 13. Protección de datos desde el diseño y por defecto», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 421 y ss.

— «Capítulo 19. Evaluación de impacto relativa a la protección de datos y consulta previa», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 469 y ss.

MURGA FERNÁNDEZ, J. P.: «Derechos de los individuos», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 77 y ss.

NIETO GARRIDO, E.: «Derecho a indemnización y responsabilidad», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 555 y ss.

NÚÑEZ GARCÍA, J. L.: «Responsabilidad y obligaciones del responsable y del encargado del tratamiento», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 353 y ss.

PALMA ORTIGOSA, A.: «Principios relativos al tratamiento de datos personales», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 39 y ss.

PÉREZ BES, F.: «Capítulo 18. La obligación de notificar una violación de seguridad de datos personales», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 457 y ss.

PIÑAR MAÑAS, J. L.: *Código de protección de datos*, Wolters Kluwer, Madrid, 2019.

PUYOL MONTERO, J.: «Transparencia de la información y derecho de acceso de los interesados en la nueva normativa de protección de datos», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 275 y ss.

RECIO GALLO, M.: «Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 351 y ss.

— «Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva», en J. L. PIÑAR (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2017, pp. 539 y ss.
— *El estatuto jurídico del Data Protection Officer*, Wolters Kluwer, Madrid, 2019.
ROMERO TERNERO, C.: «Seguridad de la información», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 401 y ss.
RUBÍ NAVARRETE, J.: «La agencia española de protección de datos», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 491 y ss.
SÁNCHEZ ORS, C.: «Capítulo 20. El delegado de protección de datos», en J. LÓPEZ (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 493 y ss.
TRUJILLO CABRERA, C.: «Las bases de legitimación del tratamiento de datos personales. En especial, el consentimiento», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 51 y ss.
— «Directrices de interpretación del RGPD», en J. P. MURGA, M.ª de los Á. FERNÁNDEZ y M. ESPEJO LERDO (dirs.), *Protección de datos, responsabilidad activa y técnicas de garantía,* Reus, Madrid, 2018, pp. 265 y ss.
VALÍN LÓPEZ, M.: «Las autoridades autonómicas de protección de datos», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 521 y ss.
VILASAU SOLANA, M.: «El consentimiento general y de menores», en A. RALLO (dir.), *Tratado de protección de datos,* Tirant lo Blanch, Valencia, 2019, pp. 197 y ss.