IMPACTO DE LA NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES EN EL ÁMBITO LOCAL

Concepción CAMPOS ACUÑA

Doctora en Derecho y Secretaria de Administración Local, categoría Superior

SUMARIO:

1. UN NUEVO MARCO LEGAL PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO LOCAL

La vigencia desde el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) ha obligado a las entidades locales a introducir relevantes novedades en su modelo de gestión y protección de los datos personales.

El RGPD, tal y como señala JIMÉNEZ ASENSIO se configura como la norma que desarrolla y regula directamente el derecho fundamental a la protección de datos recogido en la Constitución Española, en su artículo 18, adoptando la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) un papel complementario o auxiliar. El propio preámbulo de la Ley lo deja bien claro al afirmar que "*más que de incorporación cabría hablar de 'desarrollo' o complemento del Derecho de la Unión Europea*", su aprobación se explica por razones de salvaguardar el principio de seguridad jurídica "*tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento*" del RGPD.

Con anterioridad a la LOPDGDD y a la vista del retraso que llevaba su tramitación parlamentaria, se aprobaba el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, con el que, sin perjuicio de que los aspectos que configuran el contenido esencial del derecho fundamental a la protección de datos de carácter personal que requerían su incorporación a una ley orgánica, se daba respuesta a la adopción urgente de una norma con rango de ley que permita la adaptación del Derecho español al Reglamento General de Protección de Datos.

La LOPDGDD, publicada en el Boletín Oficial del Estado núm. 183, de 6 de diciembre de 2018, consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales. En su Disposición derogatoria única, establece que, sin perjuicio de lo previsto en la disposición adicional decimocuarta, relativa a Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE y en la disposición transitoria cuarta, relativa a Tratamientos sometidos a la Directiva (UE) 2016/680, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; asimismo queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos y cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y en la propia norma, entrando en vigor al día siguiente al de su publicación, de conformidad con lo establecido en su Disposición Final única.

No obstante, no todos los preceptos de la LOPDGDD gozan de la protección reforzada de la naturaleza de Ley Orgánica, pues tal y como señala la Disposición Final Primera tendrán naturaleza de ley ordinaria : el Título IV, el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico, el Título VIII, el Título IX, los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X, las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico, las disposiciones transitorias y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

A continuación realizaremos una breve aproximación a aquellos extremos regulatorios que presentan mayor impacto en la gestión de la protección de datos personales por parte de las entidades locales, sin perjuicio del análisis en profundidad que alguno de ellos pueden merecer, como es el novedoso Título X relativo a los derechos digitales y su impacto en los empleados públicos. Destaca también la regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido.

2. BASES LEGÍTIMAS DE TRATAMIENTO DE DATOS PERSONALES TÍPICAS DEL ÁMBITO LOCAL

El tratamiento de los datos de carácter personal constituye, en determinados supuestos, una actividad necesaria para el desarrollo de las competencias de las diferentes administraciones públicas, y de las entidades locales en particular, pero eso no justifica que se encuentren exentas de acreditación de dicho tratamiento sobre las bases jurídicas que ofrezcan legitimación al mismo, en clara coherencia con la protección que merece un derecho calificado por nuestro modelo constitucional como fundamental.

Para conocer cómo articular adecuadamente la legitimación de los tratamientos llevados a cabo por las entidades locales debemos recordar que los Considerandos 45 y 50 RGPD establecen que para poder ser llevado a cabo el tratamiento de datos personales, éste debe tener una base en el Derecho de la Unión o de los Estados miembros, es decir, que siempre que se traten datos personales por parte de la respectiva entidad local ha de existir algún tipo de habilitación y se debe tener en cuenta, entre otras cosas, cualquier relación entre los fines que justificaron la recogida de los datos y los fines del tratamiento previsto posteriormente, es decir, es precisa una base jurídica concreta.

Para la determinación de esta base jurídica concreta es preciso acudir al RGPD, que se ocupa de esa cuestión en su art. 6 RGPD y a la LOPDGDD con la incorporación del art. 8, en el que clarifica la aplicación del RGPD. De las bases de tratamiento recogidas en el art. 6 RGPD, resultan de aplicación a las entidades locales, específicamente las señaladas en los apartados c) y e)

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

Estableciendo expresamente que, o dispuesto en la letra f) del párrafo primero[1] no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

El recurso a estas bases de legitimación para el tratamiento de datos personales por las EELL se completa con lo dispuesto en el art. 8 LOPDGDD relativo al tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos, cuando señala que:

[1] *f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*

- El tratamiento de datos personales sólo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) RGPD, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV RGPD.

- El tratamiento de datos personales sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) RGPD, cuando derive de una competencia atribuida por una norma con rango de ley.

Sobre esta materia y el título que sirve de base para la legitimación ha venido también a incidir la LOPDGDD en un doble aspecto. Por una parte, modificando el art. 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), para legitimar la consulta y la cesión de datos personales entre las diferentes administraciones púbicas a través de las Plataformas de Intermediación y, por otra, en la Disposición Adicional Octava, relativo a la potestad de verificación de las Administraciones Públicas, como se examinará en el correspondiente apartado.

3. RÉGIMEN DE DERECHOS: ESPECIAL REFERENCIA AL BLOQUEO DE DATOS

El RGPD ampliaba el catálogo de derechos que recogía la LOPD, para garantizar la efectiva protección de datos personales de los afectados, en sus artículos 12 y siguientes contempla un nuevo régimen de derechos de los afectados frente al modelo de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) establecidos en la LOPD y que ahora se incorporan en la LOPDGDD: Acceso, Rectificación, Supresión, Oposición, Portabilidad, Limitación. Entre ellos destaca la amplia configuración del derecho a la información, pero también la incorporación de nuevos derechos como el derecho a la portabilidad de los datos, derecho a la supresión, que comprende el conocido como "derecho al olvido"[2], en base precisamente a la necesidad

[2] De creación jurisprudencial gracias a la conocida como "Sentencia Google", , la sentencia del TJUE 13-5-14, asunto C-131/12, Google Spain, S.L., Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González, dando respuesta a una cuestión prejudicial planteada por la Sala de lo Contencioso-administrativo de la Audiencia Nacional del Reino de España.que permitía la solicitud directa a Google del borrado de los datos personales que aparecen en el buscador indexados, y Google tendrá la obligación de hacerlo, pudiendo acudir de forma efectiva a solicitar la Tutela de la AEPD o de los Tribunales en caso de conflicto.

de contemplar una limitación temporal en la vida de los datos ante la inexistencia de fronteras espacio-temporales que ha impuesto la utilización de las nuevas tecnologías.

El Título III de la LOPDGDD, dedicado a los derechos de las personas, lleva a cabo la adecuación al ordenamiento jurídico español del principio de transparencia en el tratamiento RGPD que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas», mediante lo dispuesto en su art. 11. Las EELL estarán obligadas a incluir la información clara y precisa en sus sedes electrónicas sobre cómo ejercer dichos derechos facilitando toda la información de forma clara y transparente[3].

La LOPDGDD impone en su artículo 32 una obligación adicional al responsable: la de bloquear los datos cuando proceda al ejercicio de sus derechos de rectificación o supresión. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas, sin que los datos bloqueados no podrán ser tratados para ninguna finalidad distinta. Transcurrido ese plazo deberá procederse a la destrucción de los datos.

Cuando, para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

No obstante, este deber de bloqueo de los datos podrá excepcionarse cuando así lo determine la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, cuando, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

[3] Sobre esta cuestión y cómo cumplir esta obligación puede consultarse la "Guía para el cumplimiento del deber de informar" de la AEPD, disponible en el siguiente enlace https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

4. NUEVA ARQUITECTURA INSTITUCIONAL: EL MODELO DE GOBERNANZA

El considerando 78 del RGPD advertía ya la necesidad de introducir cambios organizativos para implantar el nuevo modelo de gobernanza de los datos, cambios que resultarán también de aplicación al sector público local

> *La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto*.

En este modelo organizativo destaca, frente a rígidos esquemas tradicionales, su carácter interdisciplinar, su aplicación requiere la combinación de diferentes áreas de conocimiento y la asunción de roles de distinta naturaleza para garantizar su eficacia, aunque en su definición queda suficientemente abierto, para que los sujetos obligados puedan adaptarlo a sus características organizativas y de funcionamiento, adaptación que en el caso de las administraciones públicas requiere de especiales condiciones, por un lado, por la configuración de la relación de empleo público de especial sujeción, como por el debido respeto a un marco legal definido en materia de contratación pública.

Este nuevo modelo de gobernanza de los datos se estructura en torno a tres figuras: el responsable, el encargado y el delegado de protección de datos, que se definen en el artículo 4 RGPD del siguiente modo:

Responsable	persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento
Encargado	persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento
Delegado de Protección de Datos	persona física o jurídica, empleado en plantilla o mediante contrato de servicio, que informa y asesora al Responsable, al Encargado y a otros empleados sobre las obligaciones del RGPD y supervisa su cumplimiento, cooperando y actuando como punto de contacto con las Autoridades de Control"

La figura del encargado del tratamiento se regula específicamente en el artículo 33 LOPDGDD, con una mención expresa a la proyección estructural de la figura en las Administraciones Públicas, en su apartado 4 y, en relación con los contratos del encargado de tratamiento, cabe destacar la importante disposición transitoria quinta, recogida ya en el Real Decreto Ley 5/2018, pero al que se le ha incorporado un párrafo nuevo, estableciendo la vigencia de los contratos hasta 2022, sin perjuicio de que cualquiera de las partes podrá exigir la modificación.

Con algunas modificaciones, la LOPDGDD mantiene la configuración del Delegado de Protección de Datos (DPD) que recoge el RGPD, destacando especialmente una novedad en su art. 37, relativo a la *"Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos"*, mediante el reconocimiento de su papel como órgano intermedio de control. De este modo, cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la AEPD o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al DPD de la entidad contra la que se reclame. En este caso, el DPD comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación. Habría que determinar si se configura como una autoridad intermedia de control, escenario que plantearía problemas en aquellos casos en los que las AAPP hayan recurrido a la vía de la contratación externa, vía LCSP, para el desempeño de estas funciones, dada la reserva del ejercicio de las funciones públicas de autoridad, o como un órgano de intermediación[4].

5. EL REGISTRO DE ACTIVIDADES DE TRATAMIENTO Y LAS NUEVAS OBLIGACIONES DE TRANSPARENCIA

El modelo de protección de datos personales previsto en la derogada LOPD sobre la base de ficheros de datos personales registrados ante la AEPD, evoluciona con la vigencia del RGPD a un modelo de autotutela de las entidades que llevan a cabo el tratamiento de los datos, y, señaladamente, de los responsables de tratamiento y que se erige sobre una pieza clave y novedosa: el registro de actividades de de tratamiento, al que se refiere el Considerando 82 RGPD señalando que

> *«para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a*

[4]La Agencia Española de Protección de Datos mantiene una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona, al cierre de este trabajo contiene los datos de contacto de cerca de 20.000 entidades, de las cuales alrededor de 3.000 corresponden al sector público y las restantes al sector privado. Se encuentra disponible en el siguiente enlace https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/consultaDPD.jsf;jsessionid=4ZrUUQGlNTW4ucv9Iz8WC0aU

su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento»

Corresponde a cada organización, de acuerdo al principio de responsabilidad proactiva que rige el RGPD, decidir el nivel de segregación o agregación con el que desea registrar los tratamientos de datos de carácter personal que requiere su actividad. Deberá valorar hasta qué punto la segregación de sus tratamientos en elementos diferentes se corresponde con finalidades, bases jurídicas y categorías de afectados distintos. Asimismo, le corresponde ponderar la optimización de la gestión de la protección de datos dentro de su organización para que resulte útil, ágil, efectiva y permita el cumplimiento de la finalidad que la legislación persigue: que los individuos cuyos datos de carácter personal son objeto de tratamiento puedan tener, en su caso, un control efectivo de los mismos.

Por su parte, la LOPDGDD destina su artículo 31 a regular el registro de las actividades de tratamiento, apuntando que los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 RGDP, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento, cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

Se introduce una nueva obligación para los sujetos enumerados en el artículo 77.1 LOPDGDD que harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 RGPD y su base legal. Y para ello, lleva cabo la modificación de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTBG), ampliando las obligaciones de publicidad activa, con la introducción de un nuevo artículo 6 bis relativo al Registro de actividades de tratamiento, vía Disposición final undécima.

Los sujetos enumerados en el artículo 77.1 LOPDGDD son los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, el Banco de España, las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las fundaciones del sector público, las Universidades Públicas, los consorcios y los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales, publicarán su inventario de actividades de tratamiento.

Por tanto, en aplicación de dicho precepto deberán publicarse en el Portal de Transparencia de la respectiva entidad local un Inventario basado en el registro de actividades, siguiendo la distinción establecida en el mismo, conforme al cual cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, con el contenido que se recoge en el mismo.

6. EL DEBILITADO RÉGIMEN SANCIONADOR APLICABLE A LAS ENTIDADES LOCALES

El Real Decreto-ley 5/2018 citado ya permitía anticipar la voluntad del estado español en cuanto a la definición del régimen sancionador aplicable a las administraciones públicas y, por extensión, a las entidades locales. La citada norma mantenía la vigencia de lo establecido en la LOPD en cuanto a esta materia, es decir, permaneciendo ajenas a la posibilidad de recibir una sanción de carácter económico, ofreciendo un perfil muy debilitado frente a las posibilidades que permite el RGPD.

En este marco, la LOPDGDD procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el RGPD establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea.

La especialidad diferencial en relación a otras entidades distintas a las previstas en la LOPDGDD radica en el tipo de sanción que se puede imponer, pues frente a las elevadas cuantías que contempla el RGPD para los sujetos de derecho privado, en este caso, cuando estos responsables o encargados cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 LOPDGDD, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento, resolución que también establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. La 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.

Asimismo, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación, por lo que habrá que distinguir la naturaleza o el vínculo existente entre el responsable y/o el encargado con la respectiva entidad local.

También se recoge una peculiaridad 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 se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda. En este caso, respecto al ámbito local se plantea una dificultad para su aplicación, pues si bien la determinación de la condición de autoridades estaría clara, en relación con los miembros de las Corporaciones locales, pero en el caso de los directivos, la inexistencia de esta categoría profesional, en los términos señalados en el artículo 13 del Real Decreto Legislativo 3/2015, de 30 de octubre, por el que se aprueba el Texto Refundido del Estatuto del Empleado Público (TREBEP), más allá de la determinación de órganos directivos de una serie de puestos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local (LRBRL).

Destaca la existencia de obligaciones de comunicación y publicación, como una medida adicional sancionadora:

a) Obligaciones de comunicación:

- Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con estas medidas y actuaciones

- Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

b) Obligaciones de publicidad:

- Cuando la autoridad competente sea la Agencia Española de Protección de Datos, ésta publicará en su página web con la debida separación las resoluciones, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

- 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.

7. GARANTÍA DE LOS DERECHOS DIGITALES

Se incorpora un nuevo Título X, con una novedosa regulación, relativa a la *"Garantía de los derechos digitales",* en la que se recogen derechos que introducen en el ordenamiento jurídico aspectos necesarios para adaptar la norma a la sociedad actual cuya actividad pivota en gran medida en un entorno digital, tal y como se puede ver a continuación:

Artículo 79	Los derechos en la Era digital
Artículo 80	Derecho a la neutralidad de Internet
Artículo 81	Derecho de acceso universal a Internet
Artículo 82	Derecho a la seguridad digital
Artículo 83	Derecho a la educación digital
Artículo 84	Protección de los menores en Internet
Artículo 85	Derecho de rectificación en Internet
Artículo 86	Derecho a la actualización de informaciones en medios de comunicación digitales
Artículo 87	Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral
Artículo 88	Derecho a la desconexión digital
Artículo 89	Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo
Artículo 90	Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral
Artículo 91	Derechos digitales en la negociación colectiva
Artículo 92	Protección de datos de los menores en Internet.
Artículo 93	Derecho al olvido en búsquedas de Internet.

Artículo 94	Derecho al olvido en servicios de redes sociales y servicios equivalentes.
Artículo 95	Derecho de portabilidad en servicios de redes sociales y servicios equivalentes
Artículo 96	Derecho al testamento digital.

De este conjunto abordamos, sintéticamente, aquéllos con mayor impacto en los empleados públicos y en su relación con la entidad.

7.1. Derecho a la desconexión digital en el ámbito laboral

Constituye uno de los derechos digitales y más novedosos, cuya finalidad es la de garantizar a los trabajadores, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

No obstante, resulta de compleja articulación a efectos de garantizar su eficacia en los distintos puestos. En todo caso, la entidad local elaborará una política interna dirigida a trabajadores, también los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática.

7.2. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Con el reconocimiento de este derecho se pretende proteger a los trabajadores frente a la utilización de imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas. Para ello, los empresarios están obligados a informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida.

7.3. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

Ante la indefensión que supone la indebida utilización de los sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores, resulta preciso arbitrar contrapesos para garantizar el derecho a la intimidad, facilitando información clara, expresa e inequívoca acerca de la existencia y características de estos dispositivos e igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

7.4. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral

Se reconoce este derecho a los empleados públicos en relación al uso de los dispositivos digitales puestos a su disposición por su empleador, estableciendo como límite que el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Asimismo, la entidad local deberá establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente

7.5. Derechos digitales en la negociación colectiva

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral, por lo que en el marco de la negociación colectiva, tanto convenios como acuerdos marco se irán incorporando las condiciones necesarias para garantizar la eficacia de estos derechos.

Por último, no pueden dejar de citarse las políticas de impulso de los derechos digitales que impone el artículo 97 al Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet y un Plan de Actuación. Aunque no se hace mención a las EELL, el despliegue de este tipo de políticas no puede realizarse sin contar con las entidades que tienen mayor presencia en el territorio y de proximidad al conjunto de la ciudadanía. Igual valoración merece la elaboración de un Plan de Actuación, concebido como un instrumento dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

8. MODIFICACIONES NORMATIVAS DE MAYOR RELEVANCIA PARA LA ADMINISTRACIÓN LOCAL

La LOPDGDD contempla en sus Disposiciones Adicionales numerosas modificaciones de otras normas, entre las cuales, destacaremos por su importancia, las que contempla en materia de transparencia, procedimiento administrativo común y empleo público.

8.1. Modificación de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno

A la modificación ya expuesta en relación con nuevas obligaciones de publicidad activa, la LOPDGDD reitera el criterio general consolidado de que la protección de datos es un derecho fundamental que matiza las obligaciones de transparencia en su Disposición Adicional Segunda "Protección de datos y transparencia y acceso a la información pública". Deja claro así la LOPDGDD que todas las obligaciones de transparencia, con independencia de si se trata de las impuestas en la modalidad de publicidad activa (artículos 6 a 8 LTBG), como las de publicidad pasiva (derecho de acceso a la información pública), están sometidas a los límites derivados de la protección de datos, con independencia de la fuente obligacional, bien sea la normativa estatal básica o las normas dictadas en la materia por las respectivas CCAA.

Por otra parte, lleva a cabo un ajuste en el ejercicio del derecho de acceso a la información pública, pues la redacción del apartado 1 del artículo 15 también es objeto de modificación, vía Disposición Final Decimotercera, para su adecuación a la terminología del RGPD que, frente al modelo de la anterior LOPD, que distinguía entre datos personales protegidos y datos personales especialmente protegidos, se limita a establecer una categoría general de datos personales, y categorías especiales de datos personales (aquéllos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física) recogidos en el artículo 9 RGPD.

Tras la modificación efectuada la redacción del apartado 1 del artículo 15 LTBG queda redactado como sigue:

> *«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.*

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese 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.»

Se trata de actualizar las reglas aplicables para resolver la tensión existente entre el derecho de acceso y uno de sus límites, de hecho el que podría considerarse como su mayor límite: la protección de datos personales, adecuado ahora a la nueva normativa europea.

8.2. Modificación de la Ley 39/2015, de de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

Uno de los temas más controvertidos en la utilización de las Plataformas de Intermediación de Datos (PID) por las AAPP en ejecución del principio *"once&only",* es la posible colisión entre el art. 28 LPAC y el RGPD, por cuanto este último veta la posibilidad de poder utilizar como base de legitimación el consentimiento tácito que es, en cierta medida, lo que recoge este precepto en su redacción original.

Tras la modificación efectuada en los apartados 2 y 3 del art. 28 LPAC, por la Disposición final duodécima, se mantiene el reconocimiento a los interesados del derecho a no aportar documentos que ya se encuentren en poder de la entidad local actuante o que hayan sido elaborados por cualquier otra Administración. La entidad local podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello, sin que quepa oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección. Para ello las EELL deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto. Las EELL tampoco requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. Su obtención se realizará de igual modo al anterior supuesto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso.

Esta nueva redacción debe leerse a la luz de lo establecido en la Disposición adicional octava LOPDGDD, relativa a la *"Potestad de verificación de las Administraciones Públicas"*, que otorga dicha legitimidad al señalar que cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las AAPP, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

8.3. Modificación del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido del Estatuto Básico del Empleado Público,

Como veíamos, la LOPDGDD establece que los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral, puede ser objeto de garantías adicionales en los términos establecidos en el art 91, relativo a los *"Derechos digitales en la negociación colectiva*", al tiempo que, como garantía básica y medida de protección de los trabajadores, se modifican las dos normas básicas que regulan las relaciones laborales.

En su Disposición final decimocuarta se lleva a cabo la modificación del TREBEP añadiendo una nueva letra j bis) en el art. 14, con la Disposición final decimocuarta, para recoger el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en esta normativa.

9. OTROS ASPECTOS REGULATORIOS DE INTERÉS

Sin perjuicio de otras medidas y a efectos de dar respuesta a la finalidad de aproximación a que obedece el presente estudio, señalaremos una serie de extremos que deben tomarse en consideración por parte de los operadores afectados por el nuevo marco legal.

9.1 Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

La Disposición adicional séptima LOPDGDD contempla una serie de prescripciones relativas a cómo habrá de realizarse la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos, garantizando la debida protección de datos personales. Para ello establece que cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente y cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el art. 44 LPAC, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando el

afectado careciera de cualquiera de los documentos mencionados se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

9.2. Registros de personal del sector público

La LOPDGDD regula específicamente los tratamientos de los registros de personal del sector público en su Disposición adicional duodécima, señalando que se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del RGPD, y facultando el tratamiento de los 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.

Igualmente contempla que de acuerdo con lo previsto en el artículo 18.2 RGPD, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 RGPD, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

9.3. Medidas de seguridad en los tratamientos de datos personales

Dentro del modelo de protección basado en la responsabilidad proactiva, en el caso de las EELL, como administraciones públicas, registran la especialidad de su sujeción al Esquema Nacional de Seguridad (ENS), aprobado por Real Decreto 3/2010, estableciendo la Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el ENS y que deberá ser objeto de adecuación. El art. 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP) dispone que el ENS tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha norma, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

La Disposición Adicional primera LOPDGDD, relativa a las medidas de seguridad en el ámbito del sector público, contempla que el ENS incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 RGPD. Los responsables enumerados en el artículo 77.1 LOPDGDD deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el ENS, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o

contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al ENS.

10. CONCLUSIÓN: LA PROTECCIÓN DE DATOS PERSONALES DESDE LA PREVENCIÓN

Como decíamos al inicio de este artículo, la LOPDGDD se encontraba fuertemente condicionada por el RGPD, y la naturaleza del mismo en el marco del ordenamiento jurídico europeo y la posición de los Estados miembros respecto al mismo, a diferencia de las Directivas comunitarias. Con esta norma se cumple la obligación de los Estados miembros de integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico.

El derecho a la protección de datos y el deber de protección que desarrollan ambas normas deben incardinarse en la desarrollo de las competencias locales en múltiples ámbitos de actividad, que exigen tomar en consideración las interacciones normativas que presentan mayores dificultades y soluciones de conflictos. Nos hallamos, una vez más, ante un marco jurídico complejo, nada más y nada menos que la protección de datos personales, en un entorno tecnológico cambiante, tan cambiante que no permite prácticamente predictibilidad de futuro y, por tanto, con muchas sombras en su aplicación y graves riesgos para la privacidad de la ciudadanía. Tal y como recoge el Considerando 6 RGPD

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

Nos enfrentamos pues a un nuevo modelo de gestión de los datos personales desde la perspectiva de su protección, a través de herramientas y mecanismos de carácter preventivo, frente al modelo anterior puramente represivo, que exige profundas transformaciones en el modelo de organización y funcionamiento de la administración,

pasando a un modelo de control previo con la figura del Delegado de Protección de Datos, y mediante la aplicación del principio «privacy por design», protegiendo los datos desde el diseño y por defecto, y obligando a las entidades locales a realizar una gestión de riesgos, inusual en la práctica administrativa más tradicional.

BIBLIOGRAFÍA

CAMPOS ACUÑA, Mª C. "Finalidades y bases jurídicas de los tratamientos de datos por parte de las entidades locales", en *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Wolters Kluwer, Madrid, 2018.

DELEGADO de protección de datos en las Administraciones Públicas, AEPD 2018 https://www.aepd.es/media/docs/funciones-dpd-en-aapp.pdf

GUÍA para la adaptación al Reglamento General de Protección de Datos de las Administraciones locales, AEPD 2018 https://www.dcd.es/ebooks/RGPD-administraciones-locales.pdf

GUÍA Protección de Datos y Administración Local, AEPD, 2018. https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

JIMÉNEZ ASENSIO, R. "(Algunas) Ideas-fuerza de la nueva Ley de Protección de Datos en su aplicación al Sector Público", en blog *La mirada institucional*, consultado el 17 de diciembre de 2018. https://rafaeljimenezasensio.com/2018/12/09/algunas-ideas-fuerza-de-la-nueva-ley-de-proteccion-de-datos-en-su-aplicacion-al-sector-publico/

ONTAÑÓN RAMOS, I. "El Tribunal de Justicia Europeo respalda el Derecho al Olvido", en *Noticias jurídicas*, 2014. http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4921-el-tribunal-de-justicia-europeo-respalda-el-derecho-al-olvido

POVEDANO, D. "Responsabilidad activa en la protección de datos: el responsable y el encargado del tratamiento en el ámbito local", en *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Wolters Kluwer, Madrid, 2018.