# El enfoque preventivo en la protección de datos personales en el RGPD y en la nueva LOPDGDD: elementos (Especial consideración de los Códigos de Conducta)[1]

**Rafael Jiménez Asensio (Consultor, Estudio Sector Público SLPU/Catedrático de** Universidad acreditado)
https://rafaeljimenezasensio.com/

**SUMARIO**



---

[1] Ponencia presentada al Seminario de Relaciones Colectivas de la FMC, Barcelona 19 de diciembre de 2018.

## *Presentación*

Este trabajo pretende centrar la atención en los elementos principales que conforman el enfoque preventivo de la protección de datos personales que se deriva de la plena aplicabilidad del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD, en lo sucesivo), así como conforme se prevé en la reciente Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (LOPDGDD, en lo sucesivo).

Para abordar esta materia, se abordan, en primer lugar, algunas nociones muy básicas de carácter general sobre el nuevo marco de protección de datos formado por el binomio normativo conformado por el RGPG y la LOPDGDD, a través de cuatro epígrafes. En segundo lugar, se tratan los elementos sustantivos del denominado como enfoque preventivo de la protección de datos de carácter personal y, en particular haciendo hincapié en algunos de los elementos de ese nuevo enfoque preventivo de la protección de datos personales que plantado inicialmente por el RGPD ha sido ratificado, como no podía ser de otro modo, por la reciente LOPDGDD.

De acuerdo con el encargo que me ha sido hecho, se tratará especialmente aquello que se corresponde con los códigos de conducta, pero se debe advertir de inmediato que, en lo que concierne a las Administraciones Públicas y a las entidades del sector público, la regulación de esta materia solo se aplica parcialmente y, además, dado el régimen sancionador que se prevé (con una aplicación blanda) por lo que respecta a las organizaciones públicas, su interés no es precisamente el mayor, sobre todo si se analiza en relación con el resto de herramientas o instrumentos que conforman lo que he venido en denominar como *nuevo modelo institucional y de gestión de la protección de datos en la Administración Pública.*

El presente trabajo se cierra con unas breves conclusiones y, asimismo, con un Anexo en el que se incluyen algunas Ideas-fuerza de la nueva LOPDGDD, que, si bien reiteran algunos de los contenidos tratados puntualmente en el texto, plantean un análisis general de ese texto normativo y pueden ayudar al lector a comprender mejor su alcance y sentido.

# I.- EL NUEVO MARCO NORMATIVO DE LA UE EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

## *1.- ¿Por qué una nueva regulación europea (RGPD) que ha sido desarrollada por la LOPDGDD?*

La necesidad objetiva de la nueva regulación europea en materia de protección de datos de carácter personal surge del propio contexto tecnológico y de su evolución en las dos últimas décadas. En efecto, en los más de veinte años transcurridos desde 1995 (fecha de aprobación de la Directiva 95/46/CE) hasta 2016 (fecha de entrada en vigor del RGPD) o 7 de diciembre de 2018 (entrada en vigor de la LOPDGDD) la digitalización y la revolución tecnológica, así como la globalización y transferencia internacional de los propios datos, ha generado nuevos e importantes retos para la protección de los datos personales y, en particular, para los derechos y libertades de los ciudadanos. Esta nueva regulación no solo se dicta para afrontar los retos del presente, sino en especial también para hacer frente a los grandes desafíos del futuro en materia de protección de datos y de garantía de los derechos y libertades de los ciudadanos, ámbitos que en estos momentos están comenzando a ser objeto de una erosión nunca conocida hasta la fecha.

Sin embargo, la orientación preferentemente *preventiva* o situada en un *enfoque de riesgos* precisamente tiende a evitar que los responsables y encargados de los diferentes tratamientos se encuentren ante situaciones nuevas que no puedan hacer frente y que, por consiguiente, esos nuevos e inciertos contextos que se produzcan en el ámbito tecnológico puedan erosionar los derechos de las personas físicas a través de la manipulación o uso torticero de los datos personales. Ante la evidente situación de incertidumbre que se atisba frente al desarrollo efectivo, las secuelas o efectos de la revolución tecnológica, ese enfoque anticipatorio o preventivo era la solución más idónea por parte del poder normativo europeo y del propio desarrollo de la LOPDGDD.

Tampoco conviene olvidar que cuando se aprobó la Directiva 95/46/CE el desarrollo de Internet era mucho menor. Las redes sociales y buena parte de las compañías tecnológicas no habían nacido o se encontraban en un estadio de desarrollo mucho menor.

Uno de los documentos más importantes que dio inicio al cambio normativo en materia de protección de datos en la Unión Europea fue la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, titulada *Un enfoque global de la protección de los datos personales en la Unión Europea*, COM/2010/0609 final. En el preámbulo de la propia LOPDGDD se hace expresa mención a este importante documento, que servirá de base inicial para el cambio de orientación de la normativa en materia de protección de datos.

Si esto era así en 2010 qué puede decirse en 2018 y qué podrá suceder en 2025 o 2030. Una de las claves para hacer frente a esa revolución tecnológica y a su afectación a la protección de datos personal radica en disponer de una mayor capacidad de (auto)control de la protección de datos personales, una idea que asimismo se recoge en el Preámbulo de la LOPDGDD y que enlaza con la jurisprudencia constitucional más relevante en esta materia (por todas: STC 292/2000).

En este contexto de avance de la revolución tecnológica o digital y de sus inevitables impactos sobre la protección de datos personales, el papel del Sector Público y, particularmente, de la Administración Pública, adquiere un rol de gran importancia para preservar los derechos y

libertades de la ciudadanía. Y la regulación de esta materia se convierte en una de claves de esa correcta preservación, tal como recoge el Considerando 6 del RGPD.

## *2.- ¿Cuáles son los motivos por los que se ha derogado la Directiva de 95/46/CE y se ha aprobado el Reglamento (UE) 2016/679, desarrollado posteriormente por la LOPDGDD?*

La derogación de la Directiva 96/45/CE y su sustitución por el RGPD no es una operación normativa menor. El cambio de instrumento regulador obedece, tal como se ha visto, a razones de contexto y a la necesidad objetiva de establecer un Reglamento (UE) que, como es sabido, es una disposición normativa europea que tiene un alcance general, es obligatoria en todos sus elementos y directamente aplicable.

La Administración Pública y las entidades de su sector público pueden tratar (y de hecho tratan) gran cantidad de datos personales (un volumen considerable) que, en determinados contextos, pueden ser causa o provocar situaciones de riesgo evidente.

Asimismo, es también obvio que el sector público trata en no pocas ocasiones "categorías especiales de datos" (datos sensibles), por utilizar la terminología del Reglamento UE. Todo ello requiere a los responsables y encargados del tratamiento en el sector público especial diligencia en tales procesos, pero en particular fomentar una cultura y actividad preventiva tanto en el diseño de los procesos de tratamiento como por defecto (esto, es de manera permanente, analizando en cada caso y circunstancia la necesidad de tales tratamientos), aplicando todas las medidas técnicas y organizativas que estén a su alcance para salvaguardar los derechos fundamentales de las personas físicas (el objetivo central, no se olvide, del RGPD).

Por consiguiente, la regulación que se ha llevado a cabo a través del Reglamento (UE) 2016/679 y posteriormente la LOPDGDD es particularmente importante por lo que afecta al sector público. Pero de inmediato cabe afirmar que, sin perjuicio de que se aplique también al sector público (a lo que el Reglamento denomina "autoridades y organismos públicos"), no es menos cierto que el foco central de preocupación de esa disposición normativa de la Unión Europea es el riesgo que para la protección de los derechos fundamentales y, en especial, la protección de datos de las personas físicas, se pueda producir como consecuencia del tratamiento masivo de datos, del cruce entre estos datos dirigido entre otras cosas a la elaboración de "perfiles" y de las observaciones masivas derivadas de los datos.

Una observación importante es, sin duda, resaltar que tanto el RGPD como la LOPDGDD, a diferencia del conjunto de leyes que solo se aplican a las Administraciones Públicas o a las entidades de su sector público (LPAC, LRJSP, LCSP, etc.), tienen como vocación reguladora tanto el sector privado (preferentemente) como el sector público. Por tanto, algunas de las previsiones de ese binomio normativo RGPD/LOPDGDD no tienen como objeto regular la Administración Pública (esto es, contienen algunas reglas que se aplican exclusiva o preferentemente a organizaciones o entidades del sector privado) y, en algunos casos, veremos cómo contienen asimismo determinados ámbitos normativos cuya aplicabilidad se modula o incluso se excepciona en lo que afecta a determinadas entidades del sector público (régimen sancionador, preferentemente).

La entrada en vigor del Reglamento UE 2016/679, como es sabido, se produjo a los veinte días de su publicación en el DOUE, pero su plena aplicabilidad se produjo a partir del 25 de mayo de 2018 (artículo 99 RGPD). En todo caso, la adaptación normativa del Derecho interno a ese RGPD ha sido tardía, pues no se ha producido hasta más de seis meses después de la citada fecha.

En los Considerandos 9 a 13 del RGPD se explicitan cuáles han sido los motivos que han justificado el cambio de instrumento normativo. Y cabe reenviar a esas razones para ver cómo se justifica la nueva configuración de ese marco normativo:

- La aplicación de la Directiva 1995 ha sido fragmentaria y desigual
- Se quiere garantizar un nivel uniforme y elevado de protección de datos personales, y que sea además equivalente en todos los Estados miembros.
- La protección efectiva de los datos personales exige reforzar las obligaciones de quienes los tratan. El endurecimiento del régimen sancionador es uno de los presupuestos de apoyo de tal normativa.
- La base jurídica para esta regulación se encuentra en el artículo 16. 2 del TFUE. El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea recoge, por su parte, el derecho fundamental.
- Regular esta materia por un Reglamento debería proporcionar seguridad jurídica y transparencia.

El Consejo de Estado, en su dictamen 757/2017, de 26 de octubre de 2017, sintetizó en una serie de ideas-fuerza el recurso al instrumento normativo del Reglamento, norma obligatoria en todos sus elementos y directamente aplicable en todos los Estados miembros (artículo 288 TFUE), como medio necesario para llevar a cabo esa reducción de las divergencias normativas que se habían producido con la aplicación de la Directiva 95/46/CE. Nos remitimos a lo allí expuesto.

Por consiguiente, el operador jurídico o técnico debe ser plenamente consciente de que, en este nuevo contexto normativo de protección de datos personales y a diferencia del marco normativo anterior (en el que la LOPD era la referencia determinante), deberá trabajar con dos herramientas normativas "en paralelo": una de carácter principal, reforzada además por la primacía del Derecho de la Unión Europea frente al Derecho de los Estados miembros, como es el Reglamento (UE) 2016/679, mientras que la otra es la LOPDGDD que se limita a "completar o aclarar" la regulación europea, así como a establecer determinadas excepciones solo cuando esté habilitada específicamente para ello por la normativa europea.

El resultado, como se dirá en su momento, es bien obvio: el Reglamento (UE) 2016/679 se convierte en la norma de cabecera en materia de protección de datos y la actual LOPDGDD será una disposición normativa, por mucho que se califique de "orgánica", de carácter complementario o de desarrollo. Así lo conforma con claridad evidente el propio preámbulo. Es más, si la Ley Orgánica está llamada a desarrollar los derechos fundamentales y libertades públicas recogidos en la sección primera del capítulo segundo del título primero de la Constitución, en este caso el desarrollo del contenido esencial de este derecho fundamental, como ha expuesto la mejor doctrina (Luís Rodríguez Álvarez) se ha realizado –como luego se verá- por el propio Reglamento UE y no por la LOPDGDD, que realiza un mero reenvío, al menos en lo que a las dimensiones del derecho a la protección de datos respecta, a los establecido en la disposición normativa europea.

## *3.- El nuevo marco normativo del RGPD y de la LOPDGDD como cambio de paradigma*

Este punto requiere un desarrollo algo más detenido. En efecto, la nota distintiva del actual marco normativo, comprendido por el binomio RGPD/LOPDGDD frente al anteriormente existente (Directiva-LOPD), reside que el nuevo modelo transita *desde un modelo reactivo a un modelo proactivo o centrado en el "enfoque de riesgos".* Ese cambio de "filosofía" de la nueva regulación europea está perfectamente descrito en los Considerandos del RGPD, así como se

refleja tangencialmente en diferentes disposiciones normativas de ese Reglamento europeo. Una vez más el preámbulo de la LOPDGDD se hace eco perfectamente de este nuevo enfoque y de ese tránsito citado como se verá de inmediato.

Las razones de ese tránsito en la concepción del problema han sido expuestas anteriormente, pero todas ellas tienen que ver con dos factores sustantivos:

a) La posición dominante de las grandes compañías tecnológicas que tienen una posición de cuasi monopolio en todo lo que afecta a los datos personales con un volumen de información cada vez más abrumador, lo que puede tener serias consecuencias sobre los derechos de la persona y la propia subsistencia del Estado democrático tal como lo hemos concebido tradicionalmente;
b) El acelerado e incierto desarrollo tecnológico que, basado en el dato personal y en los algoritmos, está inaugurando una nueva revolución tecnológica de resultados altamente inciertos, un contexto que exige incidir especialmente en la prevención o en el denominado "enfoque de riesgos", algo que obligará a las Administraciones Públicas (en cuanto organizaciones que tratan gran cantidad de datos personales y algunas veces datos de carácter sensible) a establecer un registro de actividades de tratamiento, incrementar las medidas de seguridad dirigidas a proteger los derechos fundamentales de las personas que sean titulares de esos datos, así como a llevar a cabo una serie de análisis de riesgos y, en su caso, evaluaciones de impacto, aparte de dotarse de una arquitectura organizativa dirigida a cumplir esos fines establecidos por el Reglamento (funciones de los responsables y encargados del tratamiento; la figura del Delegado de Protección de Datos; Códigos de Conducta y mecanismos de Certificación, el papel de las autoridades de control; etc.). Todo ello se pormenoriza en la LOPDGDD.

En cierta medida se puede afirmar que se traslada a la protección de datos de carácter personal (aunque con algunas limitaciones, según se verá) el esquema propio de la *política de compliance*, en el que la dimensión preventiva o anticipadora es una de las claves de bóveda del modelo que se pretende construir. Ante la más que evidente incertidumbre que plantea el desarrollo tecnológico el binomio normativo RGPD/LOPDGDD transmite la idea de que se debe estar siempre alerta, también en el ámbito de lo público, con el fin de evitar todas esas intromisiones y afectaciones sobre el derecho de protección de datos personales y el resto de los derechos fundamentales, por conexión o consecuencia.

Como se ha venido reconociendo, también por la AEPD (Informe sobre el proyecto de LOPD), en verdad con este nuevo marco normativo impulsado por el RGPD se ha producido un *auténtico cambio de paradigma* en el modo y manera de gestionar los datos personales con innegables consecuencias, no solo presentes sino sobre todo futuras. Se puede afirmar, sin riesgo a equivocarse que el RGPD es una disposición normativa que afronta una regulación con vistas a resolver problemas inmediatos, pero que se dota de los instrumentos necesarios para enfrentarse a los innumerables retos e incertidumbres que se abren en el futuro.

La Unión Europea ha sido el primer espacio geográfico supraestatal que se ha inclinado por una regulación "regional" de la protección de datos personales y por exigir a las grandes empresas tecnológicas (así como al resto de sujetos obligados, entre ellos las Administraciones Públicas) el cumplimiento de una exigente normativa.

El nuevo marco normativo (RGPD/LOPDGDD) se asienta sobre una serie de principios que todos los responsables y encargados del tratamiento deben respetar, algunos de ellos redefinidos, y asimismo con un nuevo catálogo ampliado de dimensiones de derechos específicos vinculados con la protección de datos personales, que deberán ser garantizados en su ejercicio por las Administraciones Públicas. También hay nuevas facetas de tales derechos (derecho a la limitación de los tratamientos, derechos a la portabilidad de datos o derecho al olvido) y redefinición de algunos otros de ellos. La Sentencia del TJUE de 2014 (Google contra

España) tuvo en este punto importancia destacable, al menos para impulsar ese denominado "derecho al olvido", una redefinición del derecho a la cancelación de datos personales, ya existente. La LOPDGDD ha ido incluso más lejos al regular dentro de ese texto normativo unos denominados *derechos digitales* que tienen una conexión relativa con el real objeto de la norma jurídica, que es la protección de datos personales, e inclusive pueden llamar a cierta confusión.

La Administración Pública, a través de los responsables y encargados del tratamiento, debe cumplir fielmente los principios relativos al tratamiento, debiendo estos informar toda la actuación pública en cualquier tratamiento de datos personales (artículo 5 RGPD) y, especialmente, teniendo en cuenta la "base jurídica" o "licitud del tratamiento", sea esta el consentimiento del interesado o afectado (en los términos que se recogen en el citado RGPD, aunque en el ámbito de las Administraciones Públicas, como veremos, la propia Agencia Española de Protección de Datos pone en cuestión que esa sea una base legítima de tratamiento en el sector público), el cumplimiento de una obligación legal aplicable al responsable de tratamiento o, en su caso, el cumplimiento de una misión realizada en interés público o en el ejercicio de los poderes públicos conferidos al responsable de tratamiento (artículo 6 RGPD, letras a), c) y e). Aspectos estos últimos determinantes para que la Administración Pública pueda tratar legítimamente los datos personales.

Con ser importante esa cuestión, en el campo de la Administración Pública resulta trascendental la articulación a través del RGPD y de la LOPDGDD de una serie de elementos perfectamente estructurados que tienden a salvaguardar la orientación principal de esa normativa: prevenir riesgos futuros en el tratamiento de datos personales. Gran parte de esa arquitectura de elementos instrumentales o de gestión se encuadran en esa *política de compliance* sobre la cual se inspira el modelo, pero otros disponen de autonomía propia, aunque encuentran su pleno sentido en ese enfoque de riesgos reiteradamente citado.

En verdad, el binomio normativo RGPD/LOPDGDD combina acertadamente instrumentos de gestión de protección de datos basados en ese enfoque de riesgos, con una redefinición del modelo institucional que fortalece el papel de las autoridades de control y articula un conjunto de medidas sancionadoras con fuerte componente de disuasión para evitar la erosión de los derechos fundamentales de la persona física a través del tratamiento de datos personales; aunque tales medidas sancionadoras se diluyan casi completamente cuando de aplicarlas a las Administraciones Públicas y a sus entidades del sector público se trata, tal como ha quedado regulado el artículo 77 de la LOPDGDD, que sigue la línea de tendencia de la anterior LOPD de 1999, como si nada hubiera cambiado ni en el contexto ni el futuro de esta importante materia.

En esta lógica preventiva se enmarcan diferentes instrumentos o instituciones que se articulan dentro de lo que se podría denominar, según decíamos anteriormente, como un nuevo modelo institucional y de gestión de las protección de datos en las organizaciones públicas, que descansa principalmente sobre una serie de ejes de la configuración del sistema de protección de datos a partir del binomio normativo RGPD/LOPDGDD.

Este nuevo modelo de gestión de protección de datos debe ser seguido fielmente por parte de las Administraciones Públicas y por las entidades de su sector público, puesto que en este caso todos y cada uno de esos elementos (con algunas singularidades tales como la necesidad de llevar a cabo evaluaciones de impacto, las excepciones en los supuestos del régimen se supervisión de códigos de conducta o las derivadas en materia de el régimen específico de sanciones que se pueda definir, entre otras) se aplican también a las organizaciones públicas

## ELEMENTOS DEL NUEVO MODELO DE GESTIÓN DE DATOS PERSONALES EN LAS ADMINISTRACIONES PÚBLICAS

1. Nuevo rol o nuevo marco de responsabilidades del responsable y, particularmente, del encargado del tratamiento de datos. Especialmente todo lo relativo a la protección de datos desde el diseño y por defecto.
2. Registro de las actividades de tratamiento. Instrumento de obligada existencia, con unas excepciones muy tasadas.
3. Medidas de Seguridad y, en particular, obligaciones específicas vinculadas con la seguridad o con las brechas de seguridad (*breach data*)
4. Análisis de Riesgos en el tratamiento.
5. Evaluación de impacto de aquellas operaciones de tratamiento que lo exijan.
6. Implantación de la figura del Delegado de Protección de Datos (preceptiva en las Administraciones Públicas)
7. Códigos de conducta.
8. Mecanismos de certificación
9. Reforzamiento del papel de las autoridades de control en su diseño institucional, en sus funciones y en sus poderes.
10. Régimen de responsabilidad y sanciones (con modulaciones importantes en su aplicación a las Administraciones Públicas, de conformidad con lo establecido en la LOPDGDD, artículo 77 LOPDGDD

Todos y cada uno de los elementos o ejes de ese Nuevo Modelo de Gestión de Protección de Datos Personales deben ser puestos en marcha, con distinta intensidad como se decía, por todas y cada una de las Administraciones Públicas. Sin duda, el reto es importante. Y no cabe orillar que el proceso de adaptación de las estructuras organizativas de las Administraciones Públicas y de sus entidades del sector público será lento y gradual.

En verdad, la adaptación de la gestión de protección de datos al nuevo modelo dibujado por el RGPD implicará, en primer lugar, la interiorización de cuál es la visión y sentido de ese binomio normativo (qué pretende y por qué), así como, en segundo plano, un cambio de cultura organizativa y algunas modificaciones estructurales de importancia, como también dedicar recursos tanto personales como materiales, tecnológicos y financieros, a esa finalidad.

En cualquier caso, este Modelo de Gestión de Protección de Datos se tendrá que ir desarrollando paulatinamente, pues no cabe prever que a corto plazo de produzcan cambios sustantivos en el modo y manera de tratar los datos personales por las Administraciones Públicas. El cambio de modelo es tan radical que convendrá hacer una prudente digestión (y aplicación gradual, pero persistente) de sus innovadores elementos. Tal vez, como se dirá al final, el acelerado desarrollo de las tres oleadas de la revolución tecnológica (digitalización, automatización e Inteligencia Artificial) seguramente irán incorporado gradualmente a las Administraciones Públicas esa necesaria presión para hacer frente a tan importantes y complejos retos, que se materializarán, como expone el propio RGPD (artículo 25.1) en "los *riesgos de diversa probabilidad y gravedad* (que efectivamente se puedan ir produciendo) para los derechos y libertades de las personas físicas" (idea que se pretende concretar en el artículo 28 LOPDGDD). También la Administración Pública y el conjunto del sector público deben impulsar de modo efectivo el desarrollo de la economía digital, pero asimismo deben salvaguardar la protección de datos personales y su adecuada utilización de conformidad con lo establecido en el binomio normativo RGPD/LOPDGDD. En ese justo y complejo equilibrio es en el que deberá moverse la acción de los poderes públicos. Y, por consiguiente, tiene interés especial tratar, siquiera sea sucintamente, tales elementos que conforman ese nuevo Sistema de Gestión de la Protección de Datos Personales en ese marco normativo.

## *4.- La LOPDGDD: Ideas-fuerza del proceso de elaboración y del Preámbulo de la citada Ley.*

El BOE del pasado jueves 6 de diciembre publicó la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD), cuya entrada en vigor se produjo el día 7 de diciembre. Esta regulación deroga la anterior LOPD de 1999 (LO 15/1999) y al reciente Real Decreto Ley 5/2018, que tenía una vocación puramente transitoria, tal como exponía su disposición final única ("El presente real decreto-ley entrará en vigor al día siguiente de su publicación en el 'BOE' y lo estará hasta la vigencia de la nueva legislación orgánica de protección de datos (…)"). Se da cumplimiento, así, a la necesaria adaptación normativa del Derecho interno a las previsiones del Reglamento (UE) 2016/679 (RGPD, en lo sucesivo).

Este breve epígrafe no tiene por finalidad llevar a cabo un estudio exhaustivo de la LOPDGDD. Nuestra única pretensión en estos momentos es resaltar telegráficamente algunos de aquellos aspectos que, por lo que afecta a la Administración Pública y a su sector público institucional (sin adentrarme en el sector salud), incorporan novedades importantes en relación con lo tratado en el propio RGPD o, en su caso, regulan otras previsiones que conviene tener presentes para una cabal interpretación de este nuevo *marco normativo dual* (RGPD/LOPDGDD) de la protección de datos personales con el que necesariamente deberá obrar el aplicador del Derecho a partir de ahora en el ámbito público.

Antes una importante precisión: el RGPD, salvo en aquellas materias en las que permita excepcionalmente una regulación que restrinja sus previsiones por una norma de Derecho interno (supuestos tasados), es la disposición normativa que –dada su naturaleza- dispone de primacía aplicativa en caso de antinomia, desplazando en ese caso a cualquier norma de Derecho interno, Ley Orgánica incluida. Por tanto, que nadie piense (si es que hay alguien que a estas alturas lo pretende) que "estudiando" solo la LOPDGDD podrá resolver los problemas que se susciten en materia de protección de datos. Eso ya es el pasado. Cualquier operador público deberá actuar a partir de ahora, tal como decíamos, con *dos pantallas normativas (RGPD/LOPDGDD)*, con las precisiones antes expuestas.

En este sentido, debe ponerse de relieve que –como reconociera en su día José Luís Rodríguez Álvarez- el RGPD (una disposición normativa del Derecho de la Unión Europea) es en verdad la norma que desarrolla y regula directamente el contenido esencial del derecho fundamental a la protección de datos recogido en la CE (algo insólito en materia de regulación primaria de los derechos fundamentales), adoptando la LOPDGDD un papel meramente complementario o auxiliar[2]. La utilización, por tanto, de la forma de *ley orgánica* no puede esconder que en este caso el papel de este tipo de norma está subordinado a lo dispuesto en una disposición normativa de la Unión Europea con una especial fuerza activa, como es el RGPD, cuyo alcance general, obligatoriedad, aplicabilidad y eficacia directa condiciona totalmente el espacio de configuración de la citada Ley orgánica y, por tanto, de las propias Cortes Generales, que en este caso juega el papel de concreción de lo que una norma europea establece. 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*". Por consiguiente, la propia LOPDGDD admite en el citado preámbulo su carácter *vicarial*, puesto que advierte que 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.

---

[2] Ver: L. Rodríguez Álvarez: "Artículo 18.4 CE", *Comentarios a la Constitución de 1978, Libro Homenaje al Profesor Luís López Guerra*, Tirant lo Blanch, Valencia, 2018.

Este nuevo marco normativo ha venido además adornado por la inclusión (estirando hasta el infinito el artículo 18.4 CE) de los denominados *derechos digitales* cuyo parentesco con el objeto de la Ley se visualiza exclusivamente en *el dato personal* como medio a través del cual se pueden ejercer o, en otros muchos casos, entorpecer o dificultar, el ejercicio de determinados derechos fundamentales de la persona física que se ven plenamente afectados por el mundo de Internet y por las redes sociales, cuando no por la propia revolución tecnológica. Pero, aparte de esa vinculación con "el dato" (en un caso *de* la persona y en los otros que afectan *a* la persona), realmente se trata de cuestiones distintas que –como bien expresó Víctor Almonacid- hubiesen requerido un tratamiento normativo diferenciado en sendas leyes orgánicas distintas (de protección de datos personales y de garantía de derechos digitales): pero no cabe ocultar que las tentaciones de aprovechar la tramitación parlamentaria de la LOPD (que no tenía especiales dificultades en la articulación de un consenso suficiente para ser aprobada en sede parlamentaria ante la imperiosa necesidad de adaptar la legislación interna al RGPD) para insertar ese catálogo amplio de derechos digitales fueron muy altas. Así, se utilizó a la LOPD como una suerte de "Caballo de Troya" para la inclusión de unos derechos digitales que, de otro modo, no se hubiesen podido insertar en el sistema jurídico al requerir su tramitación por ley orgánica y exigir un plazo de aprobación, así como unas mayorías, que con toda seguridad no se hubiesen podido conseguir.

Sin embargo, no trataré en este texto de esta cuestión, puesto que ya la abordé en un comentario anterior[3]. Sobre este mismo tema han reflexionado recientemente diferentes autores en distintos espacios abiertos, como por ejemplo: Eduardo Rojo Torrecilla, por lo que afecta al campo de los derechos digitales en el ámbito laboral[4]; o Concepción Campos Acuña, desde una óptica más general[5], entre otras muchas referencias que se podrían traer a colación. Está por ver, en cualquier caso, que mediante regulaciones nacionales (en este caso por Ley, anticipándose a su anunciado reflejo constitucional, como así se recoge en el preámbulo de la LOPDGDD) se puedan garantizar plenamente el ejercicio y los efectos de derechos con proyección global. Al menos se intenta. Con el paso del tiempo iremos viendo si su efectividad es tal, pues dentro de esos denominados "derechos digitales" hay desde principios o normas directiva hasta auténticos derechos u otros que se difieren en su concreción posterior a normas jurídicas de distinto carácter o a propias normas convencionales.

Por tanto, lo que a continuación sigue es una mera identificación de algunos aspectos importantes que pueden tener interés de la nueva regulación en cuento que innovan determinadas cuestiones en relación con la normativa anteriormente vigente. Pero este análisis se realizará ahora a través de la exposición de algunas ideas-fuerza recogidas en el Preámbulo (aunque a algunas de ellas ya se ha hecho referencia anteriormente y no se reiterarán), así como, más adelante, de aquellas otras que se pueden extraer del articulado, teniendo como foco de atención la Administración Pública y, en particular, sus posibles impactos sobre las entidades locales.

En cuanto al contenido del preámbulo conviene resaltar, aparte de lo ya expuesto, cuatro puntos especialmente:

- El Preámbulo de la LOPDGDD inicia su exposición con la obligada referencia al artículo 18.4 CE (una auténtica percha de dimensiones descomunales a partir de esta ley de donde cuelgan implícitamente un número desorbitado de derechos digitales, diecinueve concretamente, aparte del propio derecho a la protección de datos

[3] Ver: https://rafaeljimenezasensio.com/2018/10/22/proteccion-de-datos-y-derechos-digitales/

[4] Ver: http://www.eduardorojotorrecilla.es/2018/12/los-derechos-digitales-laborales-en-la.html

[5] http://concepcioncampos.org/10-puntos-que-debes-conocer-ya-de-la-nueva-lopd-y-gdd/

personales, esta vez por decisión del legislador y no de la jurisprudencia constitucional). Allí se reitera la jurisprudencia más significativa del Tribunal Constitucional (especialmente la importante STC 292/2000) y se indica que ese derecho fundamental tiene por objeto en este caso "el control de los datos" por parte de las personas físicas, así como se configura –una cuestión ya conocida- como "un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a terceros, sea el Estado (Administraciones Públicas) o un particular".

- La Ley Orgánica 3/2018 es, por tanto, la tercera ley orgánica en esta materia desde 1992 (Ley Orgánica 5/1992), lo que implica cambios permanentes de ese marco legislativo en un plazo que supera en poco los 25 años. Y ello es debido, sin duda, a la enorme volatilidad de esta materia y a los constantes cambios que la revolución tecnológica y digital están imprimiendo en su contenido. Sucede, en consecuencia, a la Ley Orgánica 15/1999, que asentada en la Directiva de 1995 se había quedado, al igual que esta, muy desfasada y, en todo caso, inadaptada a las exigencias 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. El objetivo de regular esta materia por parte de la UE de forma uniforme estaba logrado a través de la aprobación de ese RGPD, lo que exigía una adaptación del marco normativo interno a tales previsiones, que es lo realizado por la LOPDGDD.
- La LOPDGDD, por consiguiente, es, tal como ya se ha dicho, una *regulación de segundo grado*. A pesar de la solemnidad que implica aprobar esa normativa por "Ley Orgánica" y tras una larga deliberación parlamentaria, lo cierto es que los márgenes de configuración (o de innovación) normativa que tiene ese legislador orgánico son más bien escasos. Aun así se ha intentado apurar el contenido y se ha procedido a aprobar una Ley Orgánica de una extensión e intensidad más que notable (97 artículos, 29 disposiciones adicionales, 6 disposiciones transitorias, una disposición derogatoria, y 16 disposiciones finales, en las que se modifican un buen número de Leyes y Leyes Orgánicas: LOREG, LOPJ, LGS, LOU, LJCA, LEC, LOE, LPAC, ET, TREBEP, etc.).
- La inclusión de un listado de derechos digitales en el contenido de la LOPDGDD se pretende justificar en la omnipresencia de Internet ("la red") en estos momentos de la vida social, profesional y personal de la ciudadanía, así como en los riesgos y oportunidades que ese mundo ofrece. Hay una pretendida conexión objetiva (aunque el preámbulo no incide sobre este punto) con "el dato como mercancía" de ese mundo digitalizado, pues al utilizarse como tal se puede producir una innegable afectación a los derechos fundamentales de la persona (o a determinados derechos fundamentales), aunque los derechos digitales se configuran en su mayor parte como medios de proteger los derechos fundamentales frente a una invasión digital que puede obstaculizar, preterir o, incluso, anular la arquitectura tradicional de los derechos fundamentales que tanto ha costado construir en los siglos pasados. La duda que sobrevuela a todo este nuevo marco de digitalización intensiva y de revolución tecnológica es si los derechos fundamentales de la persona saldrán bien parados de tales procesos o serán puestos en cuestión mediante un vaciamiento de su efectividad. Sobre este punto no cabe sino especular, pero algunas pistas no contienen predicciones muy halagüeñas precisamente.

## II.- SISTEMA INSTITUCIONAL Y DE GESTIÓN DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA (RGPD/LOPDGDD)

## *1.- Introducción*

El nuevo modelo de Protección de Datos que se prevé en el binomio normativo RGPD/LOPDGDD se asienta, tal como se viene reiterando, sobre la *responsabilidad proactiva*, lo que tiene especiales consecuencias a la hora de articular el sistema institucional y de gestión de protección de datos en las Administraciones Públicas. Efectivamente, ese cambio de paradigma obliga a las organizaciones del sector público a *construir* un modelo de gestión que dé respuesta cabal a los hipotéticos riesgos que se puedan producir en un futuro inmediato o mediato, objetivo para el cual se debe repensar gradualmente el modelo organizativo y recomponer las piezas que sean necesarias para que este se articule efectivamente en la orientación y finalidad del RGPD/LOPDGDD.

Se pone, por tanto, el acento principalmente en hacer frente a "los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas" (artículo 24.1 RGPD) y, por tanto, en la adopción de determinadas medidas tales como, entre otras, la protección desde el diseño y por defecto, el análisis de riesgos y la evaluación de impacto que conlleva determinados tratamientos de datos personales, así como la adopción de códigos de conducta y mecanismos de certificación; es decir, el foco se sitúa en la anticipación y en la prevención, una suerte de garantía y aplicación de la política de cumplimiento (*compliance*) también en las organizaciones públicas.

Ni que decir tiene que, como también se viene reiterando, este enfoque de riesgos y preventivo implica un cambio de cultura organizativa frontal en lo que al tratamiento de datos respecta. Al menos impone una forma distinta de trabajar en todos los procesos, procedimientos y proyectos que impliquen tratar datos de forma masiva, que entrañen alto riesgo y aquellos otros que se encuadran en "categorías especiales" (datos sensibles). También supone articular de modo efectivo todas las piezas de ese nuevo modelo institucional y de gestión en las distintas organizaciones públicas, aspecto sobre el que se deberá trabajar de forma especial en los próximos tiempos.

Y es aquí donde se hallan los principales problemas para transitar correctamente de un modelo de protección de datos "reactivo" a otro "proactivo". La formación se torna ineludible y las políticas de sensibilización y es una herramienta o palanca de cambio o transformación imprescindible para ir introduciendo paulatinamente la nueva cultura de gestión en la protección de datos personales.

El tránsito será lento, también en el sector público. Se ha comenzado tarde y habrá que ajustar paulatinamente los distintos elementos de esa nueva arquitectura institucional y de gestión que deberá funcionar en un plazo razonable de forma armónica, sobre todo si, según se decía, se quiere que los datos personales y los derechos fundamentales de las personas físicas no sufran menoscabo alguno.

De hecho, ese nuevo sistema de gestión (que debería haber estado ya listo para funcionar con anterioridad al 25 de mayo de 2018), se ha demorado mucho en su puesta en marcha por la tardía aprobación de la LOPDGDD. En cualquier caso, no hay excusa, puesto que el RGPD se aprobó con un largo periodo que difería su aplicabilidad precisamente para garantizar su efectividad y llevar a cabo tal proceso de adaptación y su aplicabilidad era pleno desde la fecha indicada. Pero aún así todavía pesa mucho la cultura jurídica que vive apegada al BOE y sigue teniendo un peso relativo el Derecho de la Unión Europea hasta que diferentes pronunciamientos de los tribunales de justicia nos lo recuerdan, momento en el cual ya nada tiene remedio.

Y, para articular razonablemente, las diferentes piezas que gravitan en torno a la construcción de ese nuevo modelo institucional y de gestión de la protección de datos personales en el sector público, se deben tener presentes, aparte de los principios y derechos antes recogidos,

una serie de elementos organizativos e institucionales que tienden a configurar un nuevo Sistema de Gestión de la Protección de Datos en el Sector Público que se configura de los siguientes elementos básicos:

| ***Elementos Básicos del Sistema de Gestión de Protección de Datos*** | ***Ubicación sistemática en el RGPD*** |
|---|---|
| Responsables/Encargados del tratamiento | Capítulo IV RGPD (artículos 24-29)<br>Artículos 28, 29, 30, 33 y DTR 5ª LOPDGDD |
| Registro de las Actividades de tratamiento | Artículo 30 RGPD<br>Artículo 31 LOPDGDD |
| Seguridad de los datos personales | Artículos 32-34 RGPD<br>Artículo 32 LOPD |
| Análisis de Riesgos | Proceso previo, en su caso, a la evaluación de impacto (Artículo 24-25 y 35-36 RGPD y 28 LOPDGDD) |
| Evaluación de impacto relativa a la protección de datos | Artículos 35-36 RGPD |
| Delegado de Protección de Datos | Artículos 37-39 RGPD<br>Artículos 34-37 LOPDGDD |
| Códigos de Conducta | Artículos 40-41 RGPD<br>Artículo 38 LOPDGDD |
| Mecanismos de Certificación | Artículos 42-43<br>Artículo 39 LOPDGDD |
| Autoridades de Control (AEPD/ACPD) | Artículos 51-59 (especialmente)<br>Títulos VII y VIII LOPDGDD |
| Régimen de Sanciones | Capítulo VIII RGPD<br>Título IX LOPDGDD |

El objeto, por tanto, de esta segunda parte no es otro que analizar brevemente y de forma descriptiva estos elementos que configuran la arquitectura básica del Sistema Institucional y de Gestión de la Protección de Datos en las organizaciones públicas, con la finalidad de que este análisis sirva como medio de activar la puesta en marcha de todas esas piezas de este complejo engranaje a la mayor brevedad por parte de las Administraciones Públicas y de sus entidades del sector público institucional, pero especialmente de las Administraciones locales que son el objeto central de estas líneas.

## *2.- Responsables de tratamiento y Encargados de tratamiento: sus peculiaridades aplicativas en el ámbito del gobierno local.*

### *Responsable de tratamiento*

El Considerando 78 RGPD comienza del siguiente modo: "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". Asimismo, cabe tener en cuenta lo dispuesto en los Considerandos 79 y 81 del RGPD.

La puesta en marcha de esas medidas técnicas y organizativas apropiadas es una responsabilidad de una figura clave en el modelo de protección de datos, también en el sector público: el responsable del tratamiento. Y, además, compete a este responsable del tratamiento implantar los principios de protección de datos desde el diseño y por defecto. Este último aspecto es, sin duda, determinante del nuevo modelo, que se asienta en la prevención de riesgos en los tratamientos de datos de carácter personal actuales y futuros.

El responsable del tratamiento es quien determina, según la definición del artículo 4, los fines y medios del tratamiento. La regulación específica de la figura del responsable de tratamiento se halla en los artículos 24 a 27 RGPD, si bien el Reglamento está plagado de referencias permanentes a esta figura, que se transforma así en pieza clave para garantizar el perfecto cumplimiento de las obligaciones derivadas de la norma europea o del Derecho interno de los Estados miembros, así como en garante último de que se adoptarán las medidas técnicas y organizativas apropiadas para su adecuación a tal normativa. Esta idea se refleja perfectamente en el artículo 24.1 RGPD.

Por tanto, la aplicación de las medidas técnicas y organizativas que debe poner en marcha quien ejerza las funciones de responsable del tratamiento dependerán de la naturaleza, contexto y fines del tratamiento, pero especialmente (y aquí viene la dimensión preventiva articulada con la evolución futura de este problema) teniendo en cuenta *los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas.* Tal como expresa el artículo 24.3 RGPD la adhesión a códigos de conducta o mecanismos de certificación "podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento". Y sobre esta cuestión volveremos luego.

El artículo 25 RGPD, por su parte, recoge una de las ideas sustantivas del nuevo modelo centrado específicamente en la gestión de riesgos. Así, la protección de datos desde el diseño y por defecto es responsabilidad exclusiva del propio responsable del tratamiento, que deberá asimismo aplicar las medidas técnicas y organizativas apropiadas teniendo en cuenta lo establecido en el primer inciso de ese mismo precepto.

Por lo que respecta a la LOPDGDD, particular importancia tienen, por lo que afecta al nuevo modelo de gestión de protección de datos en el sector público (asentado en un enfoque de riesgos) las obligaciones generales del responsable y del encargado del tratamiento recogidas en el artículo 28, especialmente por lo que se refiere a los criterios para determinar los mayores riesgos en la adopción de las medidas organizativas y técnicas (artículos 24 y 25 RGPD; 28 LOPDGDD y legislación sectorial aplicable, en su caso). Esta regulación normativa sirve de complemento a la establecida en el RGPD. Así, para la adopción de medidas técnicas y organizativas por parte de los responsables y encargados del tratamiento, se tendrán en cuenta, en particular, los mayores riesgos que podrían producirse, entre otros (no es un listado exhaustivo) en una serie de supuestos, por ejemplo cuando el tratamiento:

- Pueda generar situaciones de discriminación, usurpación de identidad, fraude, pérdidas financieras, daño para la reputación, etc.
- Pueda privar a los afectados de derechos o libertades o impedirles el control de sus datos personales.
- Si afecta, siempre que el tratamiento no sea incidental o accesorio, a las categorías especiales de datos o a los datos de infracciones administrativas.
- Implique una evaluación de aspectos personales o cree o utilice perfiles personales
- Afecte a grupos en situación de vulnerabilidad o menores de edad, así como discapacitados
- Implique un tratamiento masivo por el número de afectados o la gran cantidad de datos personales.
- Fuesen a ser objeto de transferencia internacional.

- Y cualesquiera otros que, a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación, lo que dota a estos mecanismos de un papel especialmente relevante en lo que afecta a esa política de enfoque de riesgos o de naturaleza preventiva.

Asimismo, la LOPDGDD reenvía en materia de "corresponsabilidad del tratamiento" (artículo 29) a lo establecido en el RGPD (artículo 26), con la única precisión que la determinación de las responsabilidades "se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento".

En el ámbito local de gobierno la figura del responsable de tratamiento será habitualmente el Alcalde o Alcaldesa, salvo que tal atribución haya podido ser delegada en un miembro de su equipo de Gobierno o, asimismo, en la persona titular de un órgano directivo en los municipios de gran población. Esta caracterización de un órgano de naturaleza política como responsable del tratamiento (de cualquier tratamiento) no deja de ser una ficción jurídica, puesto que por regla general tales "responsables" desconocen cuáles son sus responsabilidades efectivas en esta materia y desplazan hacia la estructura funcionarial la necesidad de asesorar, cuando no redirigir, qué deben o no deben hacer tales "responsables". Este pésimo planteamiento conceptual del problema tal vez explique el motivo real de ese régimen sancionador blando que se ha adoptado en la LOPDGDD (artículo 77), pues al fin y a la postre se está reconociendo que no hay, en verdad, un responsable efectivo sobre el cuál pueda desplegarse la responsabilidad y, sobre todo, el régimen de sanciones, cuando se cometen errores evidentes o se incumplen las previsiones del RGPD/LOPDGDD. Da la impresión de que el desplazamiento de esas responsabilidades puede terminar recayendo en el personal funcionario, cuando así se inste por parte de la autoridad de control la puesta en marcha de un procedimiento sancionador, como luego se verá. En este marco de tanta incertidumbre sería razonable que las Administraciones Públicas regularán qué es responsabilidad de los responsables, cuál de los encargados y en qué medida deben asumir las consecuencias los funcionarios o empleados públicos. Los códigos de conducta pueden servir, en ausencia de normativa propia que regule esta materia, como medio de concreción de estas importantes cuestiones vagamente reguladas por el binomio RGPD/LOPDGDD (sobre todo por esta última).

***Encargado de protección de datos***

El Considerando 97 delimita a rasgos generales cuál es el papel y perfil que debe tener esta figura. Su regulación en el RGPD se encuentra recogida en los artículo 28 y 29, principalmente en el primero que resulta fundamental para concretar los criterios generales expuestos en el Considerando 97 sobre cuál es el régimen aplicable a la figura del encargado de tratamiento.

Dada la finalidad del RGPD de protección de los datos de carácter personal y, concretamente, de los derechos fundamentales de las personas físicas que se puedan ver afectados por tales tratamiento de datos, la norma europea introduce algunas novedades importantes en la regulación del encargado del tratamiento, con el objetivo de apuntalar el cumplimiento estricto del propio Reglamento, puesto que en las Administraciones Públicas tales datos en unas ocasiones serán tratados por encargados "internos", pero en no pocas de ellas por encargados "externos", mediante procedimientos de contratación pública, encomiendas de gestión, convenios u otros instrumentos jurídicos.

La regulación sustantiva de esa figura se lleva a cabo en el artículo 28 RGPD, del que se pueden destacar, entre otros, los siguientes aspectos:

- Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, éste elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar

medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

- El encargado del tratamiento no podrá recurrir a otro encargado sin la autorización previa por escrito, específica o general, del responsable. Debiendo informar de todo cambio.
- El tratamiento por el encargado se regirá por un contrato o acto jurídico, que deberá estipular, en particular, una serie de exigencias que se detallan en el artículo 28.3 RGPD.
- Cuando un encargado recurra a otro para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se le impondrán, también por contrato o acto jurídico, las mismas obligaciones de protección de datos estipuladas en el contrato o acto jurídico existentes entre el responsable y encargado principal (artículo 28.4)
- La adhesión a códigos de conducta o mecanismos de certificación podrá utilizarse como elemento para demostrar que se cumplen las garantías establecidas en ese artículo 28.1 a 4 RGPD.
- Y, en fin, se incorpora una importante cláusula de desplazamiento de la responsabilidad en determinados supuestos (artículo 28.10).

Por lo que afecta a la LOPDGDD, la figura del encargado del tratamiento se regula específicamente en el artículo 33, con una mención expresa a la proyección estructural de la figura en las Administraciones Públicas (33.4); esto es, podrán atribuirse las competencias propias de un encargado a un determinado órgano de la Administración mediante la adopción de un norma reguladora, lo que facilita la distinción estructural entre quien es responsable y quien deba asumir otras funciones diferenciadas que son las propias del encargado, acotando así el reparto de las responsabilidades de cada uno de ellos y cómo se deban depurar las responsabilidades que se puedan derivar en cada caso, tal como se señalaba anteriormente. Y, en relación con los contratos del encargado de tratamiento, cabe destacar la importante disposición transitoria quinta de la LOPDGDD, recogida ya en el RDL 5/2018, pero al que se le ha incorporado un párrafo nuevo (vigencia de los contratos hasta 2022, pero cualquiera de las partes podrá exigir la modificación).

Concretamente, las notas más relevantes de esta figura de encargado tal como aparecen recogidas en el artículo 33 de la LOPDGDD, son las siguientes:

- "El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos" (33.1), siempre que se cumpla lo establecido en el RGPD y en la LOPDGDD.
- Tendrá la consideración de responsable del tratamiento y no la de encargado 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 con el contenido fijado en el artículo 28.3 RGPD. Se exceptúan de esta regla los encargos efectuados en el marco de la legislación de contratación del sector público.
- "Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades" (33.2, párrafo 2).
- El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos de carácter personal deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. Se establece alguna excepción (33.3). No procederá la destrucción de los datos cuando una previsión legal obligue a su conservación (será obligación del responsable conservarlos).
- "El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

- Tal como señalábamos, el artículo 33.5 contiene esta importante previsión: "En el ámbito del sector público 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 exigido por el artículo 28.3 del Reglamento (UE) 2016/679".

## *3.- Registro de las Actividades de tratamiento*

Se trata, sin duda, de una de las novedades más significativas del RGPD, que enlaza directamente con la filosofía que impregna el nuevo modelo de gestión de datos personales.

La creación u mantenimiento de un registro de actividades de tratamiento es una obligación que deben llevar a cabo necesariamente los responsables del tratamiento (o sus representantes) y los encargados del tratamiento (o sus representantes). Y sustituye la antigua obligación de notificar los ficheros y tratamientos a las autoridades de control. No es un registro de ficheros, sino de tratamientos.

El marco regulatorio de ese Registro de actividades viene establecido por el artículo 30 RGPD.

Cabe tener en cuenta que el artículo 31 LOPDGDD, que reenvía a lo establecido en el artículo 30 RGPD, regula también el Registro de Actividades de tratamiento. Y se añade que el Registro podrá organizarse en torno a conjuntos estructurados de datos, debiendo especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás exigencias establecidas por el RGPD. Se deberá comunicar al DPD  Las Administraciones Públicas y sus entidades del sector público institucional (con excepción de las sociedades mercantiles públicas) "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" (artículo 31.2 LOPDGDD). A tal efecto, se debe resaltar que la disposición final undécima modifica la Ley 19/2013, de 9 de diciembre (LTAIBG), incorporando un artículo 6 bis, donde se establece precisamente que los sujetos enumerados en el artículo 77 de la LOPDGDD (Administraciones Públicas y entidades de su sector público, salvo empresas públicas), "publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica".

Hay que tener en cuenta que estos Registros de Actividades de tratamiento del Responsable o del Encargado tienen distinta intensidad en cuanto a su contenido, tal como establecen los apartados 1 (Responsable) o 2 (Encargado) del artículo 30 RGPD:

| ***Responsables de tratamiento*** | ***Encargados de tratamiento*** |
|---|---|
| Nombre y datos de contacto del responsable o de su representante | Nombre y datos de contacto del encargado o de su representante |
| Nombre y datos de contacto del DPD | Nombre y datos de contacto del DPD |
| Fines del tratamiento | Categorías de tratamientos |
| Categorías interesados y de datos personales | |
| Categorías destinatarios comunicaciones, incluidos destinatarios terceros países | |
| Transferencias internacionales tercer país | Transferencias internacionales tercer país |
| Plazos previstos supresión categorías | |

| | |
|---|---|
| datos | |
| Medidas técnicas y organizativas de seguridad: descripción general | Medidas técnicas y organizativas de seguridad: descripción general |

## *4.- Seguridad de los datos personales*

En el RGPD la seguridad se vincula estrechamente con la protección de datos personales y con la salvaguarda de los derechos y libertades de las personas físicas. Este es un enfoque de seguridad diferente, pues tiende a formar parte de ese Sistema de Gestión de Datos Personales que deben activar todas las organizaciones públicas.

Las novedades que introduce el RGPD en este ámbito también son importantes, sobre todo por la naturaleza proactiva de los tratamientos y la necesidad de tener el enfoque de riesgos estrechamente vinculado con los sistemas de seguridad. Ello imprime un concepto de seguridad "dinámico" o "instantáneo", que depende del responsable del tratamiento. Este concepto de seguridad se debe enmarcar necesariamente en un contexto de revolución tecnológica que tendrá impactos potencialmente muy fuertes sobre el ámbito de los datos personales.

El marco regulatorio es muy preciso y se recoge en los artículos 32 y 33 del RGPD.

Por lo que respecta a la LOPDGDD cabe señalar expresamente lo establecido en la disposición adicional primera que recoge una importante regulación sobre las medidas de seguridad en el ámbito del sector público (mejor dicho a los responsables enumerados en el artículo 77.1 de esa misma ley orgánica), y que extiende su aplicabilidad también (medidas equivalentes) a las empresas (en este caso sí) y fundaciones vinculadas a las Administraciones matriz, así como en los casos en que un tercero preste servicios en régimen de concesión, encomienda de gestión o contrato (cuyas medidas de seguridad se corresponderán con las de la Administración de origen y se ajustarán al Esquema Nacional de Seguridad). Es curioso, por tanto, que si bien en materia de régimen sancionador las empresas públicas y fundaciones quedan extramuros del *régimen blando* previsto en la norma, en materia de seguridad se les incluya dentro del perímetro aplicativo, lo cual es una decisión adecuada por razones obvias. La aplicación correcta del Esquema Nacional de Seguridad, como se viene afirmando, es un presupuesto necesario para que el nuevo sistema de gestión de la protección de datos personales funcione adecuadamente en cualquier Administración Pública. El parentesco o imbricación de ambos planos es evidente, tal como se ha puesto de relieve por la mejor doctrina. Se trata también de una importante novedad del RGPD. Se regula en los artículos 33 y 34, ofreciendo un doble régimen jurídico de notificación o comunicación inmediata ("sin dilación indebida") por parte del responsable del tratamiento a la autoridad de control y a los interesados, respectivamente, en los casos de violación de seguridad que comporten pérdida, alteración o destrucción de datos.

Por lo que respecta a las violaciones del sistema de seguridad (Data Breach) cabe recordar lo siguiente. Hay, en esta materia, una obligación institucional doble por parte del responsable: por un lado, debe notificar a la autoridad de control, en el plazo estipulado y siempre que constituya un riesgo para los derechos y libertades de la persona física, de las violaciones que se produzcan en la seguridad (artículo 33 RGPD); y, por otro, deberá asimismo comunicar al interesado *las violaciones del sistema de seguridad que entrañen alto riesgo para los derechos y libertades de las personas físicas.* El encargado lo debe poner de inmediato en conocimiento del responsable.

## *5.- Análisis de Riesgos*

El enfoque predominantemente "proactivo" del Sistema de Gestión de Datos Personales que se deriva del RGPD impone al responsable y encargado del tratamiento la exigencia de llevar a cabo con carácter previo un Análisis de Riesgos, al menos para descartar que deba de realizar una "Evaluación de Impacto relativa a la protección de datos" que se analiza en el siguiente epígrafe de esta Guía.

Esta cuestión está asimismo entrelazada con el Sistema de Seguridad que se implante, pues el análisis de riesgos debe formar parte de la propia evaluación del nivel de seguridad.

Y ello lo pone de relieve el artículo 32.2 RGPD de forma diáfana:

> *"Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de protección de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos".*

El análisis de riesgos está por tanto imbricado con la seguridad y también con la prevención o anticipación, forma parte "existencial" por tanto del nuevo Sistema de Gestión de Datos Personales, también en el sector público.

## *6.- Evaluación de Impacto sobre la Protección de Datos*

Conviene tener claro desde el inicio que una Evaluación de Impacto sobre la Protección de Datos (EIPD) no se requiere siempre. Por eso es importante llevar a cabo con carácter previo el Análisis de Riesgos (aunque en algunos casos, como se verá, no es necesaria esta fase si la EIPD es obligatoria).

El Análisis de Riesgos puede conducir perfectamente a que no existe riesgo alguno en el tratamiento o los riesgos que conlleva son de orden menor (fácilmente controlables), adoptando las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos personales y su no afectación a los derechos y libertades de las personas físicas. En ese caso no hay que pasar a la EIPD.

El marco regulatorio de la EIPD está recogido en el importante artículo 35 RGPD. Y en el artículo 36 RGPD se recoge el trámite de "consulta previa" estrechamente relacionado con los tratamientos de alto riesgo.

## *7.- El Delegado de Protección de Datos*

La figura del Delegado de Protección de Datos (DPD) es nueva, aunque tiene algunos precedentes que ahora no es necesario citar. Se inserta, como una pieza más e importante, en el nuevo Sistema Institucional y de Gestión de Datos Personales que se enmarca en esa política "proactiva", anticipatoria o preventiva por la que aboga el RGPD y la LOPDGDD.

Para las Administraciones Locales la nota más importante es la obligatoriedad que establece el RGPD: todas ellas deben disponer de un DPD. Realmente, esa exigencia, como tantas otras que se contienen en el RGPD, iban más dirigidas a las Administraciones Públicas de gran tamaño y a otras sectoriales donde los riesgos, el uso masivo y las categorías especiales en el tratamiento de datos personales son la moneda corriente. Pero la obligación normativa está ahí y, por tanto, ha de cumplirse.

Hay que insertar la figura del DPD en ese cambio de modelo de gestión de datos personales al que se viene haciendo referencia. Y hay que verlo como ventana de oportunidad, pues el DPD debería ayudar a ese proceso de transformación organizativa y al cambio en los tratamientos que el RGPD exige.

Esa transformación o tránsito de una cultura "reactiva" a otra "proactiva" no es fácil, menos aún en un sector público en el que el endurecimiento del régimen sancionador del RGPD se ve hasta cierto punto descafeinado, al descansar principalmente sobre "multas administrativas", que de momento no parece que se vayan a proyectar sobre los responsables o encargados del tratamiento en las Administraciones Públicas (según redacción del artículo 77.1 LOPDGDD).

En ese contexto, el DPD debe ser una palanca de transformación que haga posible la implantación de la cultura proactiva también en las instituciones públicas y, por lo que ahora interesa, en la Administración Local.

Pero, además, el DPD es importante que tenga conocimientos especializados y cualificación pertinente, pues es el punto de apoyo principal del responsable y encargado del tratamiento (esto es, quien les asesora), al efecto de cumplir debidamente las obligaciones del RGPD. Debería actuar, por tanto, como "cortafuegos" que impidiera incumplimientos. Especialmente importante es su papel en los procesos de Evaluación de Impacto.

Es en el considerando 97 dónde se dibujan las líneas maestras de esa nueva figura del DPD, que luego serán desarrolladas por los artículos 37 a 39 del RGPD, así como a través de referencias incidentales (algunas que ya se han visto) a lo largo del resto del articulado.

Cuatro son, por tanto, las ideas-fuerza que cabe resaltar del DPD según este Considerando 97:

1.- El DPD es un colaborador necesario, aunque también supervisor, del responsable o encargado del tratamiento en el sector público.

2.- Debe ser DPD una persona que acredite conocimientos especializados del Derecho y de la práctica de protección de datos.

3.- El DPD puede ser empleado público o ser provisto de forma externa.

3.- El DPD ejerce sus funciones y cometidos "de manera independiente"

Antes de adentrarnos en el análisis de la regulación normativa y en algunos aspectos operativos o prácticos que plantea a corto plazo esta figura, es conveniente delimitar su alcance en el ámbito de lo que hasta ahora indeterminadamente llamamos "sector público"

¿Qué cabe entender por "autoridad y organismo público" según el RGPD?

El RGPD utiliza *la expresión "autoridad y organismo público"* a la hora de atribuir la exigencia de crear necesariamente la figura del DPD.

¿Y qué cabe entender por "autoridad y organismo público" según el RGPD?

Esta es una noción que, como expuso el Grupo de Trabajo del Artículo 29 en el documento que seguidamente se cita (*Directrices sobre los delegados de protección de datos*), reenvía al Derecho interno de los Estados miembros.

Y, por tanto, debería ser la LOPDGDD la que precise su perímetro. De momento, la redacción que se ha dado al artículo 34 LOPDGDD no aclara qué entidades del sector público son las que están obligadas a disponer de esta figura del DPD.

Para resolver el problema se puede intentar acudir al artículo 77 LOPDGDD, donde se regula cuál es el "Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento" (todas ellas, salvo un supuesto, aplicables a las Administraciones Públicas y a les entidades del sector público) que, por una razón de paralelismo, cabría estimar que son las entidades que sí tendrían la obligación de disponer de un DPD, por lo que cabe deducir que son las que el legislador orgánico ha considerado que se encuadrarían en esa noción que emplea el RGPD de "autoridades y organismos públicos". Por lo que afecta al ámbito local de gobierno, el perímetro de aplicación de tal régimen singular se proyectaría, así, sobre las siguientes entidades:

- Los entes que integran la Administración Local (Ayuntamientos, Veguerías o Diputaciones, Áreas Metropolitanas, Comarcas, Mancomunidades y Entidades Municipales Descentralizadas)
- Los organismos públicos y entidades de Derecho Público vinculadas o dependientes de la Administración Local (organismos autónomos y entidades públicas empresariales)
- Las fundaciones del sector público adscritas a entes locales.
- Los consorcios adscritos a un ente local.

Si se puede trasladar ese esquema institucional a las entidades que están obligadas a disponer de un DPD, ello supondría que las sociedades mercantiles de carácter público no tendrían esa obligación "ex RGPD" (salvo que ejerzan funcionalmente algunas de las actividades que se relatan para las entidades recogidas en el artículo 34.1 LOPDGDD, en cuyo caso deberán disponer de un DPD), pero que sí podría exigírseles en los mismo términos que a las empresas del sector privado cuando concurrieran las circunstancias previstas en el citado RGPD. Aunque ya hemos visto que la LOPDGDD no es muy coherente en ese trazado, pues no hay una justa correspondencia en el perímetro que fija el artículo 77.1 LOPDGDD en relación con el régimen sancionador y lo que establece la disposición adicional primera LOPDGDD, que sí incluye a las sociedades mercantiles de naturaleza pública dentro de la aplicación del Esquema Nacional de Seguridad y de las medidas allí recogidas.

Por tanto, no parece tener mucho sentido que se incluya a las Fundaciones y no a las sociedades mercantiles de capital público. Algunas de ellas llevan a cabo precisamente tratamiento de datos de forma extensa e intensa (piénsese, por ejemplo, en todas aquellas sociedades mercantiles de capital público que prestan servicios informáticos de apoyo a la entidad matriz). Por tanto, lo más recomendable es que, dado que también en aquellos supuestos en los que las entidades o empresas no tengan la obligación de dotarse de un DPD lo puedan hacer, las sociedades mercantiles designen también un DPD o, en su caso, de acuerdo con lo establecido en el artículo 37.2 RGPD, se valgan de aquel que haya sido designado por la Administración Pública a la que estén vinculadas.

La regulación de esta figura se recoge principalmente en los artículos 37 a 39 RGPD.

El artículo 37, dedicado a "la designación" del DPD, prevé los siguientes extremos:

- La designación es preceptiva en algunos casos: ¿Cuándo ha de designarse según el RGPD por el responsable del tratamiento preceptivamente un DPD? (artículo 37.1 RGPD) El caso de las autoridades y organismos públicos ya ha sido analizado. Lo que no impide que cualquier organización lo pueda designar voluntariamente o si así lo exige la legislación de un Estado miembro (artículo 37.4 RGPD)
- ¿Cuántos DPD puede haber?: Pretende dar respuesta a si cabe nombrar uno o varios DPD (por grupo de empresas o autoridad u organismo público, atendiendo a "su estructura organizativa y su tamaño" (artículo 37.2 y 3 RGPD)

- ¿Qué conocimientos o competencias deben acreditar?: Las exigencias profesionales y conocimientos que debe acreditar quien sea designado DPD, vinculadas a las funciones de la figura (artículo 37.5 en relación con artículo 39 RGPD)
- ¿Deben ser internos o externos? El DPD podrá formar parte de la plantilla o ser un externo a la organización (contratación de servicios) (artículo 37.6 RGPD)
- Publicidad del DPD: El responsable o encargado publicarán (presumiblemente en la Web o Portal de Transparencia) los datos de contacto del DPD y los comunicarán a la autoridad de control.

Por su parte, el artículo 38 tiene como objeto "la posición" del DPD en relación con el responsable o encargado del tratamiento:

- Colaborador necesario: Se prevé una garantía de participación del DPD en "todas las cuestiones relativas a la protección de datos personales" (artículo 38.1 RGPD).
- Recursos: Se le deben facilitar al DPD los recursos necesarios para el desempeño de sus funciones y para el mantenimiento de sus conocimientos especializados (formación) (artículo 38.2 RGPD)
- Estatuto "de independencia": Garantía de que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones, no pudiendo ser destituido ni sancionado por su desempeño, y rindiendo cuentas al más alto nivel jerárquico de la organización (artículo 38.3 RGPD)
- Punto de contacto: Los interesados podrán ponerse en contacto con el DPD en todo lo relativo a sus datos personales y al ejercicio de sus derechos (artículo 38.4 RGPD).
- Confidencialidad: El DPD está obligado a mantener el secreto o confidencialidad por el desempeño de sus funciones (artículo 38.5 RGPD)
- DPD "a tiempo parcial": El DPD podrá desempeñar otras funciones siempre que no den lugar a conflictos de interés (artículo 38.6 RGPD)

Y, en fin, el artículo 39 RGPD define cuáles son, como mínimo, las funciones del DPD, vinculándolas todas ellas especialmente a "los riesgos asociados a las operaciones de tratamiento"(artículo 39.2 RGPD). A saber:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados sobre las obligaciones del RGPD y del Derecho interno.
- Supervisar el cumplimiento del presente RGPD, promover su implantación en la organización e impulsar la formación.
- Ofrecer asesoramiento sobre la EIPD y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control.

La regulación de la figura del DPD en la LOPDGDD la figura del Delegado de Protección de Datos reitera algunas de las características recogidas en el RGPD (artículos 37 a 39), pero con algunas exigencias adicionales. Veamos cuáles son sus rasgos más relevantes según la regulación que lleva a cabo la citada Ley Orgánica 3/2018:

- La obligación de designar un DPD por parte de las Administraciones Públicas se deriva del propio RGPD.
- Una vez designado, se establece la obligación de comunicación a la autoridad de control en el plazo de diez días el nombramiento y, en su caso, del cese del DPD (artículo 34.3)
- Se prevé, al igual que el RGPD, la dedicación a tiempo completo o parcial del DPD, en función del tipo de datos que se traten por cada organización (artículo 34.5)

- Tiene el DPD acceso a los datos personales y procesos de tratamiento, no pudiendo el responsable o encargado oponerse a este acceso invocando confidencialidad o secreto
- La "obtención de titulación universitaria" (la imprecisión de la norma es notable, pero parece referirse a postgrados o, en su caso, masteres y no propiamente a grados universitarios) se tendrá especialmente en cuenta para demostrar a través de mecanismos de certificación el cumplimiento de los requisitos del artículo 37.5 RGPD
- Se prevé, también en línea con el RGPD, la garantía, siempre que se trate de persona física, de no remoción y de independencia, evitando cualquier conflicto de intereses del DPD (Art. 36.2), lo que puede poner en duda algunos nombramientos en función del tipo de tareas que se desarrollen (dedicación parcial). Dicho de otra manera, la exigencia de que no haya conflictos de intereses (que aparecía reflejada en las *Directrices* sobre los delegados de protección de datos del Grupo del Artículo 29) se trasladan a la LOPDGDD como garantía de independencia y objetividad en el funcionamiento de tal figura, lo que desaconseja que se atribuya esa condición a puestos de trabajo que puedan tener tareas de informe jurídico o técnico relacionadas directa o indirectamente con la protección de datos personales, sobre todo en aquellos casos en los que la dedicación a tales funciones es parcial. Tal vez ello desaconseje que en el ámbito local de gobierno tales funciones de DPD se sitúen en el ámbito de la Secretaría o de la Secretaría-Intervención, por los hipotéticos conflictos de intereses que se pudieran producir.
- La facultad del DPD de inspeccionar los procedimientos relacionados con el objeto de la Ley y emitir recomendaciones (artículo 36)
- La facultad de documentar y comunicar a los órganos competentes la existencia de una vulneración relevante en materia de protección de datos.
- Y el régimen de intervención del DPD en los supuestos de reclamaciones ante las autoridades de control (artículo 37), donde se admite que el afectado pueda presentar una reclamación ante el DPD con carácter previo a la presentación de la reclamación ante la autoridad de control, incorporando una suerte de recurso potestativo de carácter administrativo que deberá resolver el órgano competente, pues difícilmente esa resolución la podrá emitir en DPD, menos aún si es una figura externalizada, pues se trataría del ejercicio de funciones de autoridad, aunque estos aspectos no se tratan en la LOPDGDD. Se refuerza así el papel del DPD como "punto de contacto" entre la ciudadanía (afectados) y la Administración Pública (responsable o encargado) que ha llevado a cabo el correspondiente tratamiento. También se prevé que la propia autoridad de control, una vez recibida una reclamación, dé traslado al DPD a efectos de que por parte de este se responda en el plazo de un mes a la citada reclamación. Si no hubiera DPD la autoridad de control podrá dirigirse al responsable o encargado del tratamiento (artículo 65.3 LOPDGDD).

## *8.- Códigos de Conducta y Mecanismos de Certificación*

Se trata de dos instrumentos que entroncan perfectamente con el enfoque "proactivo" que imprime el RGPD. Tienen, por tanto, una orientación preventiva o anticipatoria. Esta es su verdadera esencia.

Asimismo, ambas son herramientas de carácter *dispositivo*, pero que, en el caso de los Códigos de Conducta, una vez asumidos por quienes se adhieran a los mismos tendrán carácter vinculante.

En cualquier caso, sin perjuicio de lo que se dirá, cabe presumir que la adhesión a tales códigos puede implicar la atenuación en sus caso de las responsabilidades derivadas por un tratamiento de datos incorrecto (el artículo 83.2 RGPD incluye, en efecto, la adhesión a códigos de conducta o mecanismos de certificación como circunstancias "a tener en cuenta" cuando de imposición de multas administrativas se trate), si bien cabe resaltar que a las Administraciones Públicas ni a sus responsables o encargados no se les imponen sanciones, tal como prevé el artículo 77 LOPDGDD). Aunque, en el supuesto de los mecanismos de certificación, expresamente se recoge la idea de que la certificación no limitará la responsabilidad del responsable o del encargado (artículo 43.4 RGPD). De ahí que se hablara anteriormente de una *política de compliance* atenuada trasladada a la protección de datos.

Esa impresión inicial puede desvanecerse si se analizan estas herramientas en el marco del conjunto de previsiones del RGPD.

En efecto, los rasgos del sistema preventivo y de cumplimiento son evidentes en ciertos pasajes del RGPD. Tal como prevén los artículos 24.3 y 28.5 RGPD, la adhesión a códigos de conducta o mecanismos de certificación "pueden ser utilizados como elementos para demostrar el cumplimiento" o la existencia de una serie de garantías, respectivamente, por parte del responsable o del encargado del tratamiento.

Asimismo, la adhesión a un Código de Conducta o a un mecanismo de certificación "podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos" (en materia de seguridad) en el artículo 32.1 RGPD (artículo 32.3 RGPD).

También el cumplimiento de los códigos de conducta "se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados", en particular cuando se lleve a cabo una EIPD.

Por consiguiente, disponer de códigos de conducta y mecanismos de certificación es no solo adoptar una visión preventiva en línea con la finalidad del RGPD, *sino especialmente dotarse de una política de cumplimiento que salvaguarda la función del responsable o encargado del tratamiento de cualquier organización pública (Administración autonómica, así como en su sector público), también de la Administración Local.*

***Regulación de los códigos de conducta:***

***a) En el RGPD:***

El RGPD regula en los artículos 40 a 43 los códigos de conducta y los mecanismos de certificación. A pesar de su carácter de libre adhesión, cabe constatar que algunas de tales previsiones no se aplican a "las autoridades y organismos públicos" (por tanto, a las Administraciones Públicas y a las entidades de su sector público).

El artículo 40.1 RGPD prevé una labor de promoción de los códigos de conducta que será llevada a cabo, por lo que ahora interesa, por las autoridades de control, en la que se tendrán en cuenta las características específicas de los distintos sectores de tratamiento. Los códigos de conducta están destinados a contribuir a la correcta aplicación del RGPD (artículo 40.1).

Por su parte, el artículo 40.2 se refiere a que "las asociaciones y otros organismos representativos de categorías de responsables o encargados de tratamiento *podrán* elaborar códigos de conducta". Como podría ser, por ejemplo, el caso de las asociaciones o federaciones de municipios o entes locales, en su caso.

La elaboración de tales códigos de conducta, así como su modificación o ampliación, tiene por objeto, entre otras, la aplicación de las siguientes cuestiones (artículo 40.2 RGPD):

- El tratamiento leal y transparente
- Los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
- La recogida de datos personales
- La seudonimización de datos personales
- La información proporcionada al público y a los interesados
- La información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño
- Las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas de seguridad del tratamiento a que se refiere el artículo 32
- La notificación de violaciones de la seguridad de datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados
- La transferencia de datos personales a terceros países
- (…)

De esas circunstancias descritas se puede advertir cuál puede ser el contenido orientativo de un código de conducta en esta materia.

Es importante, asimismo, tener en cuenta que tales asociaciones y cualesquiera otro organismos que promuevan esos códigos de conducta deben presentar el proyecto de código ante la autoridad de control para que por parte de esta se dictamine si es conforme al RGPD y proceda a aprobar tal código "si considera suficiente las garantías adecuadas ofrecidas". Por parte de la autoridad de control se registrará y publicará tal código (artículo 40.5 y 6 RGPD).

Cabe también tener en cuenta (y este es un punto muy importante por lo que afecta al sector público) que el artículo 41 RGPD ("Supervisión de los códigos de conducta aprobados"), así como por conexión el artículo 40. 4 del RGPD, no se aplicarán a los tratamientos realizados por autoridades y organismos públicos (artículo 41.6 RGPD: "El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos")

***b) En la LOPDGDD***

La regulación de los códigos de conducta en la LOPDGDD se contiene en su artículo 38 y tiene, por lo que a la Administración Pública o Local interesa, los siguientes rasgos:

- Los códigos de conducta serán vinculantes por quienes se adhieran a los mismos 38.1).
- Podrán promoverse por asociaciones y organismos, pero también por los responsables o encargados a los que se refiere el artículo 77.1 LOPD. Por tanto, por los responsables o encargados de cualquier Administración Pública, ente local, organismo público, consorcio o fundación puede promover la elaboración y aprobación de tales códigos de conducta (38.2).
- Ante la inaplicación al sector público (autoridades y organismos públicos) del artículo 41 RGPD (organismos o entidades de supervisión), el artículo 38.2, párrafos segundo a cuarto, no se aplicaría tampoco a tales entidades públicas, con lo que tendría plena aplicación en materia de reclamaciones previas de carácter potestativo o de reenvío por las autoridades de control lo previsto en el artículo 37 LOPDGDD.
- Los códigos serán aprobados por las autoridades de control competentes en cada caso (38,3)
- Las autoridades de control someterán los proyectos de código de conducta al mecanismo de coherencia establecido en el artículo 63 RGPD, en relación con lo previsto en el artículo 40.7 RPD (38.4).

- La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán un registro conjunto de los códigos de conducta aprobados (38.5)
- Por Real Decreto se establecerá el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta (38.6).

Por consiguiente, en lo que afecta a códigos de conducta, las Administraciones y entidades del sector público, tendrían una serie de modulaciones en lo que respecta exclusivamente a las funciones de supervisión y resolución extrajudicial de conflictos que aparecen reguladas en el artículo 41 del RGPD, pero que se detallan, por lo que respecta a que tales organismos o entidades de supervisión conocieran de las reclamaciones previas, pues este procedimiento específico no es aplicable a las Administraciones Públicas, de conformidad con lo establecido en el artículo 3º LOPDGDD, de conformidad con el reiterado artículo 41 RGPD.

***Regulación de mecanismos de certificación***

***En el RGPD***

Los artículos 42 y 43 RGPD regulan los mecanismos y organismos de certificación.

En el artículo 42.1 también se recoge una labor de "promoción" que debe ser ejercida entre otros por los Estados miembros y las autoridades de control con la finalidad de crear mecanismos de certificación en materia de protección de datos y sellos y marcas de protección de datos. El objetivo de tales instrumentos es siempre "demostrar el cumplimiento de lo dispuestos en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"

Los mecanismos de certificación (sellos o marcas) tienen como finalidad principal demostrar que, por parte de los responsables y encargados del tratamiento, se cumple el RGPD. Tienden, por tanto, a salvaguardar la actuación de responsables y encargados. De ahí la importancia de dotarse de ellos.

Las líneas básicas de esa regulación son las siguientes:

- La certificación será voluntaria y estará disponible a través de un proceso transparente (artículo 42.3 RGPD).
- La certificación no limitará las responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento (artículo 42.4 RGPD)
- Será expedida por los organismos de certificación regulados en el artículo 43 RGPD o por la autoridad de control competente, sobre la base de criterios aprobados por dicha autoridad en los términos establecidos en el artículo 42 RGPD.
- Obligación de los responsables y encargados del tratamiento de proveer toda la información necesaria para llevar a cabo el procedimiento de certificación.
- La certificación será expedida al responsable o encargado del tratamiento por un período máximo de tres años, renovables en las condiciones expuestas (artículo 42.6 RGPD)

***En la LOPDGDD***

El artículo 39 LOPDGDD confiere la competencia para llevar a cabo la acreditación de las instituciones de certificación a la Entidad Nacional de Acreditación (ENAC), que será la que comunique a las autoridades de control respectivas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

Se ha de tener asimismo en cuenta la disposición transitoria segunda del LOPDGDD en relación con los Códigos tipo inscritos en las autoridades de protección de datos de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre: Adaptación de su contenido al artículo 40 RGPD en el plazo de un año.

## *9.- Autoridades de control independientes: Idea general*

No cabe duda que la correcta implantación del RGPD y de la LOPDGDD, también en los distintos niveles de gobierno (y, en particular, en la Administración Local) requiere de esa pieza institucional imprescindible que son las autoridades de control.

No es objeto de este trabajo analizar el papel y funciones de tales autoridades de control, a las que el RGPD y la propia LOPDGDD dedican un buen espacio regulador.

En estas páginas solo interesa destacar cuál es la finalidad de tales autoridades de control, y poner de relieve algunos de sus elementos más relevantes, pues se trata sin duda, del mecanismo de cierre para que el nuevo Sistema Institucional y de Gestión de Protección de Datos de las Administraciones Locales funcione adecuadamente.

Bajo este punto de vista es oportuno resaltar que la finalidad principal de las autoridades de control no es otra que la protección de las personas físicas con respecto al tratamiento de datos de carácter personal.

Esta es una idea que se recoge perfectamente en el Considerando 117 y en otros sucesivos (por ejemplo, en el Considerando 123 donde se añade a la finalidad anterior la de "facilitar la libre circulación de los datos personales en el mercado interior"). En el ejercicio de esas funciones "deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión".

No interesa abordar aquí las cuestiones relativas a la posición institucional de estas autoridades de control ni tampoco a la existencia de varias autoridades de control o a la designación, en este caso, de una autoridad de control que ejerza como "punto de contacto único" (Considerando 117). Pero sí puede ser oportuno resaltar que los amplios cometidos funcionales que el RGPD encomienda a tales autoridades de control implicarán necesariamente un refuerzo de recursos financieros y humanos, que no parece ser muy viable en época de contención fiscal.

### *Regulación de las autoridades de control en el RGPD*

La regulación de las autoridades de control en el RGPD está contenida en su Capítulo VI. Este Capítulo se estructura en diferentes secciones que abordan, entre otros, los siguientes ámbitos materiales:

- Designación de una o varias autoridades por Estado
- Estatuto de independencia de tales autoridades (ajenos a toda influencia externa, ya sea directa o indirecta y no admitirán ninguna instrucción) (artículo 52 RGPD)
- Condiciones aplicables a los miembros de las autoridades de control y normas relativas al establecimiento de la autoridad de control. (artículos 53 y 54 RGPD)
- Competencias de la autoridad principal de control (artículos 55 y 56 RGPD)
- Funciones es el aspecto más importante a nuestros efectos y se trata de forma singularizada (artículo 57 RGPD)
- Poderes, que se desdoblan en poderes de investigación, correctivos o de autorización y consultivos (artículo 58 RGPD).
- Informe de actividad (artículo 59 RGPD)

Se pueden identificar, a tal efecto, algunas funciones de esas autoridades de control en relación con las Administraciones Públicas y, con lo que ahora interesa, con las Administraciones Locales, a saber:

- Controlar la aplicación del presente Reglamento y hacerlo aplicar.
- Asesorar a las instituciones sobre las medidas administrativas a adoptar para la protección de los derechos y libertades con respecto a los tratamiento de datos.
- Promover la sensibilización de los responsable y encargados del tratamiento sobre sus obligaciones derivadas del presente Reglamento.
- Tratar las reclamaciones presentadas.
- Llevar a cabo investigaciones sobre aplicación del presente Reglamento.
- Adoptar cláusulas contractuales tipo
- Elaborar lista relativa al requisito de Evaluación de Impacto.
- Ofrecer asesoramiento sobre operaciones de tratamiento.
- Alentar la elaboración de códigos de conducta, dictaminar y aprobarlos.
- Fomentar la creación de mecanismos de certificación de la protección de datos y aprobar los criterios de certificación.
- (El desempeño de las funciones de la autoridad de control será gratuito para el interesado y para el delegado de protección de datos; salvo las excepciones tasadas en la norma (artículo 57.4 RGPD).

Por lo que respecta a la determinación de algunos *poderes correctivos* de tales autoridades de control, se pueden citar, entre otros, los siguientes:

- Sancionar a todo responsable o encargado del tratamiento con una advertencia.
- Sancionar a todo responsable o encargado del tratamiento con un apercibimiento
- Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del RGPD
- Ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten al RGPD
- Ordenar al responsable de tratamiento que comunique las violaciones de la seguridad de los datos personales.
- Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.
- Ordenar la rectificación o supresión de datos personales o la limitación de tratamiento.
- Retirar una certificación
- Imponer una multa administrativa (ver régimen singular entidades sector público)

Hay que tener en cuenta que esos poderes correctivos se modulan convenientemente por lo que respecta a las Administraciones Públicas y (a la mayor parte) de las entidades del sector público (salvo las empresas públicas), de acuerdo con lo establecido en el artículo 77 LOPDGDD, como seguidamente veremos.

***Regulación de las autoridades de control en la LOPDGDD***

El Título VII de la LOPDGDD regula exhaustivamente las Autoridades de protección de datos. Por su parte, el título VIII establece las reglas aplicables al procedimiento en caso de posible vulneración de la normativa de protección de datos. Asimismo, se deben tener en cuenta las previsiones recogidas en la disposición adicional vigésima y en las transitorias primera y tercera.

No puede ser objeto de este trabajo un análisis detenido de tales previsiones. Por tanto, solo se dará noticia puntual de algunos de los puntos de esa propuesta normativa a efectos de pura

información y obviamente de aquellos que puedan afectar con mayor intensidad a las entidades locales.

Algunos aspectos de interés de esa regulación del título VII a efectos del presente trabajo serían los siguientes:

- En el Capítulo I, relativo a la Agencia de Española de Protección de Datos, conviene resaltar lo siguiente:
  - La creación de la figura de un Adjunto, en quien la dirección podrá delegar sus funciones y que, dado el sistema de nombramiento y la necesaria ratificación (al igual que la Dirección) por mayoría de 3/5 de los miembros de la Comisión de Justicia en primera votación o de mayoría absoluta en la segunda, se prestará a un "cambio de cromos" entre aquellas fuerzas políticas que sumen tal mayoría absoluta, repartiéndose los dos puestos (artículo 48).
  - Se modifica la composición del Consejo Consultivo de la Agencia (artículo 49)
  - En cuanto a publicidad, serán públicas las resoluciones de la Presidencia que sanciones con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley orgánica (artículo 50).
  - En el ámbito de las potestades de investigación y planes de auditoria preventiva hay que tener en cuenta lo dispuesto en el artículo 51 sobre ámbito de la investigación y personal competente para llevarla a cabo.
  - Igualmente es importante el deber de colaboración de las Administraciones Públicas establecido en el artículo 52.
  - Hay unas importantes reglas sobre el alcance de la investigación (artículo 53)
  - Las potestades de regulación ("disposiciones que fijen los criterios a los que responderá la actuación de esta autoridad") a través de "Circulares de la Agencia Española de Protección de Datos"
  - O las funciones relacionadas con la Acción exterior.
- En el Capítulo II relativo a las Autoridades autonómicas de protección de datos, se contienen algunas previsiones importantes en el ámbito autonómico, foral y local.
  - Por ejemplo, algunas de ellas vinculadas con el ejercicio que a tales autoridades de control se les reconoce de las funciones establecidas en los artículos 57 y 58 RGPD, cuando se refieran a:
    - Tratamientos de los que sean responsable las entidades integrantes del sector público de la correspondiente Comunidad Autónoma de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.
    - Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómico o Local.
  - Asimismo, las autoridades autonómicas de control podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la AEPD en el artículo 55 de la LOPDGDD.
- Cabe presumir igualmente que la normativa reguladora de las Autoridades de control de las Comunidades Autónomas deberán adaptarse a lo establecido en el RGPD.

Por su parte, el Título VII regula el procedimiento en caso de posible vulneración de la normativa de protección de datos, en el que se incorporan muchas de las previsiones recogidas en el Real Decreto-Ley 5/2018, antes citado. Y, entre otras muchas cuestiones que ahora no procede analizar, se encontraría el reconocimiento de la facultad de la AEPD, "antes de resolver sobre la admisión a trámite de la reclamación, de remitir tal reclamación a l DPD a los efectos previstos en los artículos 37 y 38.2 de la LOPDGDD (artículo 65.4). Si no se hubiera designado DPD, será el responsable o

encargado del tratamiento quien deberá dar respuesta a la reclamación en el plazo de un mes.

## *10.- Régimen de responsabilidades y sanciones: Idea general. Aplicación al Sector Público*

Uno de los pilares de esta nueva regulación europea en materia de protección de datos personales era dotar a la normativa (y, en particular, a las autoridades de control) de "poderes coercitivos más contundentes" con el fin de proteger los derechos y libertades de las personas físicas como consecuencia de los tratamientos de datos personales. Detrás de todo ello está, sin duda, el avance imparable de la revolución tecnológica y el poder cuasi absoluto de las empresas de ese mismo ámbito que despliegan su actividad con el manejo y cruce de toda la información recuperada a través de los motores de búsqueda, de las redes sociales o de los correos electrónicos. Es algo muy conocido, más todo lo que esté por llegar en un escenario plagado de fuertes incertidumbres (Ver: Epílogo).

Con esa finalidad de fortalecer la aplicabilidad del nuevo marco normativo en esta materia, no quedaba otra opción que hacer el necesario hincapié en el poder sancionador. Y eso es algo que se recoge en los Considerandos 149 y siguientes del RGPD.

En todo caso, como anuncia el título del presente epígrafe, la pretensión de estas líneas es solo dar una idea general de esta problemática, entre otras cosas porque su aplicabilidad a las entidades del sector público se ve mediatizada por la regulación que se prevé en la LOPDGDD, dónde –a pesar del cambio cualitativo que implica el RGPD- en el ámbito sancionador se sigue el viejo patrón de la LOPD de 1999, con algunos matices.

Y, en este punto, por lo que ahora interesa solo cabe hacer mención a la previsión establecida en el artículo 83.7 del RGPD, que a tal efecto expone: "*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*".

El Título IX del LOPDGDD trata del Régimen sancionador. Y muy brevemente nos interesa hacer mención a la previsión recogida en el artículo 77 LOPDGDD, puesto que tal regulación representa un régimen sancionador absolutamente *blando* en comparación con el que se prevé para el sector privado, lo que da a entender una suerte de blindaje de la clase política (no en vano esta ocupa, como altos cargos o asimilados, la condición de *responsables del tratamiento* en las Administraciones Públicas y en las entidades de su sector público) frente al endurecimiento del régimen sancionador que, con carácter general, impuso el RGPD.

El "régimen aplicable a determinadas categorías de responsables o encargados del tratamiento", locución que esconde denominar a las cosas por su nombre (esto es, excepcionar o singularizar mediante una "rebaja" la aplicación del régimen sancionador para los responsables y encargados de la Administración Pública y de sus entidades del sector público (salvo empresas públicas), se recoge en el importante artículo 77 LOPDGDD.

Por lo que ahora importa, las novedades más destacables de esa regulación (que en buena medida sigue los pasos, con algunas variaciones, de la recogida en el derogado artículo 46 de la LOPD 15/1999. En efecto, se ha implantado de nuevo ) un *régimen light* en materia de régimen sancionador aplicable al sector público (aunque el contexto normativo es radicalmente distinto, muy exigente para el resto y blando para el sector público). Nada

hubiese impedido, sin embargo, aplicar un régimen de sanciones singular o específico a los responsables o encargados del tratamiento, así como al personal al servicio de las Administraciones Públicas, tipificando las sanciones que se pueden imponer en ese caso, que bien podrían ser individualizadas (al menos para los responsables y encargados), tal como se ha hecho en la normativa de transparencia que han aprobado diferentes Comunidades Autónomas, lo cual no deja de ser paradójico que cuando está en juego un derecho fundamental como la protección de datos personales se persiga con menos intensidad que cuando se trata de un derecho de configuración legal (al menos de momento) como es el de derecho de acceso a la información pública o de la propia transparencia. Este *régimen blando en materia sancionadora* se caracteriza por los siguientes elementos:

- El ámbito de aplicación de ese régimen se extiende a todas las Administraciones Públicas, organismos públicos, fundaciones y consorcios, así como (blindaje político puro) a los grupos parlamentarios y a los grupos políticos locales. Pero no, adviértase, a las sociedades mercantiles vinculadas a la Administración matriz, a las que se les aplicaría el régimen general de sanciones del RGPD y de la LOPDGDD.
- Si el responsable o encargado cometieran alguna infracción sería sancionado con *apercibimiento* y adopción, en su caso, de las medidas pertinentes. La notificación se trasladará también a los interesados.
- La autoridad de control "propondrá" (atentos a la fórmula verbal) también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello, que se tramitarán según la normativa sancionadora aplicable.
- En cualquier caso, si la infracción es imputable a una autoridad o directivo, y se acredita que se apartaron de los informes técnicos o recomendaciones sobre el tratamiento (la figura del DPD, emerge), "en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará su publicación en el Boletín Oficial del Estado o autonómico que corresponda". Nada se dice de publicarlo también como exigencia de publicidad activa en el Portal de Transparencia o en la página Web de la entidad pública a la que pertenezca, en su caso, el responsable o encargado del tratamiento.
- Asimismo, se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones (las de carácter disciplinario o sancionador y cualesquiera otras) a que se refieran los apartados anteriores.
- También se deben comunicar al Defensor del Pueblo e instituciones autonómicas análogas las actuaciones realizadas y las resoluciones dictadas al amparo de lo previsto en el artículo 77 LOPDGDD
- Si la autoridad competente es la Agencia Española de Protección de Datos se procederá a publicar la resolución referida en el artículo 77.1 LOPDGDD, "*con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción*. Si la competencia es de la autoridad autonómica de protección de datos, se estará en cuanto a publicidad a lo que disponga su normativa específica. Aplazamiento, por tanto, del tema, mientras se aprueban las leyes autonómicas respectivas (de Cataluña y del País Vasco, así como, en su caso, de Andalucía).

## BREVES CONCLUSIONES

El binomio normativo RGPD/LOPDGDD representa, por tanto, un cambio de paradigma en el modo y manera de entender el tratamiento de los datos personales, también en el sector

público. Y ello implica, cuando menos, tener en cuenta una serie de elementos en ese proceso de implantación ineludible del modelo pergeñado por el Derecho de la Unión Europea (RGPD) y su desarrollo por la LOPDGDD. Sucintamente serían los siguientes:

1.- La citada normativa, a pesar de tener un carácter general e imprimir algunas singularidades e inclusive menores exigencias para el sector público (en materia de régimen sancionador, por ejemplo) impacta particularmente en las Administraciones Públicas y en las entidades de su sector público institucional, por lo que las entidades locales deberán tenerla especialmente en cuenta, con las implicaciones que ello comporta de cambio de modelo de gestión de la protección de datos personales.

2.- Hay, a lo largo del RGPD y de la propia LOPDGDD un conjunto de obligaciones que las Administraciones Públicas y, particularmente, las entidades locales, deberán cumplir. El papel de las autoridades de control en la exigencia del cumplimiento de tales obligaciones será, sin duda, muy importante, aunque –como se ha reiterado-se ha impuesto en la LOPDGDD un régimen de sanciones "blando" para el sector público, lo que puede conducir a un relajamiento no solo en la puesta en marcha de las innovaciones del binomio normativo expuesto, sino sobre todo (lo que es más preocupante) en la aplicación efectiva de tales obligaciones normativas, algo que puede llegar a poner en peligro en determinados casos la protección de los derechos fundamentales de las personas físicas por actuaciones poco diligentes del sector público.

3.- El proceso de adaptación efectiva de la normativa citada (RGPD/LOPDGDD) va a ser presumiblemente largo por lo que afecta a su puesta en marcha por las Administraciones Públicas, pues el cambio de modelo de un sistema de "control de cumplimiento" a otro de "responsabilidad proactiva" será complejo, por las dificultades intrínsecas que ello comporta y por los recursos técnicos, económicos y personales que han de poner en circulación las Administraciones Públicas y las entidades del sector público.

4.- Todo ello comporta inevitablemente un cambio de cultura organizativa que implica muchas transformaciones en las organizaciones públicas. A modo de ejemplo se pueden citar las siguientes:

- La adopción real del rol de responsable del tratamiento en el sector público, algo que se ve tremendamente dificultado por la habitual consideración de responsable de tratamiento a órganos de extracción política sin competencias ni conocimientos efectivos en estas materias (especialmente, aunque no solo en el ámbito local de gobierno) y que, por lo común, ni conocen realmente de la materia y de sus implicaciones ni frecuentemente entra en su orden de prioridades más inmediato, a lo que se une ese sistema de sanciones blandas, de las que solo la publicación de los incumplimientos puede actuar como elemento de disuasión de conductas poco diligentes o indiferentes hacia los tratamientos de datos en sus respectivas organizaciones.
- La diferenciación efectiva del papel del responsable y la del encargado, asumiendo el primero su rol efectivo y reordenando estructuralmente las organizaciones (al menos de cierta complejidad o tamaño) con el fin de que ambas funciones se delimiten en cuanto a su estructura o sus papeles. Las directrices y vigilancia efectiva del encargado se tornan necesarias en el nuevo modelo, así como la elección precisa de este último en función de sus cualificaciones profesionales.
- La puesta en marcha del Registro de actividades de tratamiento es, sin duda, una de las primeras piezas de puesta en marcha del modelo, aparte de que se deben cumplimentar las exigencias de publicidad activa previstas en la LTAIBG, reformada a tal efecto.

- Las medidas de seguridad se tornan asimismo estrictamente necesarias en un modelo de enfoque de riesgos y, por consiguiente, se debe articular el sistema de seguridad (Esquema Nacional de Seguridad) de cada Administración Pública con el contexto de aplicación del binomio normativo RGPD/LOPDGDD en lo que a protección de datos respecta.
- El análisis de riesgo y la adopción de las medidas técnicas y organizativas necesarias para paliar el riesgo en cualquier impacto sobre el tratamiento de datos personales es, asimismo, un elemento sustantivo del modelo, al igual que la evaluación de impacto relativa a la protección de datos cuando ella sea necesaria. En ambos casos el responsable y encargado del tratamiento tienen como punto de apoyo el asesoramiento de la figura del Delegado de Protección de Datos.
- La designación, por tanto, de un Delegado de Protección de Datos es, asimismo, un paso necesario para la puesta en marcha efectiva del modelo de gestión de protección de datos inspirado en un enfoque de riesgos. Se debe acertar en quién se designa y que disponga de las competencias técnicas necesarias para el cumplimiento de las atribuciones que tiene tan importante figura, así como garantizarle un estatuto de independencia y autonomía funcional, sin entorpecer en ningún caso su labor.
- En ese contexto los códigos de conducta y los mecanismos de certificación son dos herramientas de carácter dispositivo, pero de indudable importancia, que se enmarcan en esa *política de compliance* que dibuja tanto el RGPD como la LOPDGDD. Si bien es cierto que en el ámbito del sector público algunos de los mecanismos previstos en el RGPD no se aplican (artículo 41), no lo es menos que las Administraciones Públicas y las entidades del sector público pueden disponer de tales herramientas para salvaguardar mejor el cumplimiento efectivo de ese cambio de paradigma que se debe producir en el tratamiento de datos personales (enfoque de "responsabilidad proactiva"; artículo 5.2 RGPD). En cualquier caso, las Administraciones Públicas y entidades del sector público deberían dotarse de tales instrumentos con la finalidad de implantar de modo más efectivo ese nuevo modelo de gestión, aunque los incentivos o castigos (sanciones) sean, sobre todo, en este último caso, menores, por la aprobación de un régimen sancionador blando para la inmensa mayoría de las entidades públicas (artículo 77 LOPDGDD).
- El papel de las autoridades de control, también en el ámbito público, es determinante. Y en ese caso, inclusive, se puede decir que más, puesto que al no tener "la espada de Damocles" de fuertes sanciones oscilando por la cabeza, los responsables y encargados del tratamiento en el sector público pudieran estar tentados de caer en un cierto relajamiento o autocomplacencia. Deberán ser, por tanto, muy exigentes las autoridades de control en el cumplimiento real de las obligaciones que este nuevo marco normativo impone a las Administraciones Públicas y a las entidades del sector público, con la finalidad sobre todo de salvaguardar la protección de los datos personales y de los derechos fundamentales de las personas físicas cuando los datos sean tratados por el sector público, pues sus poderes sancionadores en este caso (aun de cierta relevancia) están muy disminuidos en relación con el que ostentan en relación al sector privado. Tendrán, por tanto, que utilizar de forma inteligente otras facultades correctivas y recursos que les ofrece la actual normativa. Un papel, sin duda, nuclear para el éxito o fracaso del nuevo modelo en el sector público.
- Y, en fin, el régimen sancionador que se ha impuesto en la LOPDGDD para las Administraciones Públicas y entidades del sector público (salvo por lo que respecta a las empresas públicas) es sencillamente poco incisivo para garantizar de estas el estricto cumplimiento de las exigencias normativas. Se podría haber sido mucho más creativo. No se trata de multar a las organizaciones públicas (algo complejo de defender en un sistema de Hacienda Pública) sino de depurar responsabilidades individuales, también de los responsables, cuando no de los encargados del tratamiento. Da la impresión de que será más fácil incoar expedientes sancionadores a los funcionarios o empleados

públicos por incumplimiento de sus obligaciones (acudiendo al procedimiento disciplinario general) que a los propios responsables (por lo común, cuyos titulares son cargos de designación política), pues en estos últimos no hay procedimiento sancionador previsto en lo que afecta a tipificación de infracciones ni tampoco a la determinación de sanciones. La única medida de disuasión, como decíamos, es la publicidad del responsable que haya cometido la infracción, pero que solo es personalizada de momento en aquellos procedimientos que incoe la Agencia Española de Protección de Datos. De todos modos, sorprende sobremanera las enormes exigencias que en esta materia tienen que cumplir las organizaciones del sector privado y el relajo con el que el legislador ha regulado los incumplimientos, por muy graves que sean, de tales exigencias en el sector público (apercibimiento). Una situación completamente desigual que no es sostenible en el tiempo.

4.- La implantación de este nuevo modelo de gestión comportará necesariamente un cambio en la cultura de las organizaciones públicas, pues en caso contrario sus impactos serán irrelevantes. Y ese cambio supondrá tiempo y una dedicación de recursos a tales finalidades, pero sobre todo disponer del objetivo claro de impulsar una política de protección de datos personales, ya que todo el modelo de gestión y sus distintos elementos van encaminados única y exclusivamente a ese finalidad.

5.- Por consiguiente, resulta meridianamente obvio que la implantación de ese modelo preventivo será complejo. Y requiere ordenar bien el proceso de implantación. En primer lugar exige un plan de sensibilización, tanto en el nivel político (responsables del tratamiento) como técnico, que identifique cuáles son las consecuencias a corto y medio plazo que la implantación de ese sistema comporta. Por tanto, mucha formación seguida por una formación reforzada para aquellos puestos de trabajo que vayan a tratar datos personales, especialmente de aquellos que traten categorías especiales de datos o datos masivos. Y sobre todo planificar bien la puesta en marcha de los diferentes elementos del modelo de gestión antes expuesto.

6.- Y, en fin, ya por lo que concierne a entidades de pequeñas dimensiones, especialmente en el mundo local, hay que partir del enfoque de irrealidad del que partió el RGPD y que se traslada después a la LOPDGDD, sobre todo a la hora de pretender que ese modelo de gestión de protección de datos y de los diferentes elementos que lo componen (por ejemplo, registro de actividades, Delegados de Protección de Datos, códigos de conducta y mecanismos de certificación, etc.) puedan ser aplicados a corto o medio plazo por los municipios, entidades locales u organizaciones públicas que no disponen ni de recursos ni de capacidad de gestión para llevar a cabo tales tareas. Es fácil, en efecto, legislar de espaldas a la realidad. Ciertamente el RGPD no es culpable de que en España la planta local esté absolutamente atomizada, pero sería razonable que el legislador interno cuando desarrolla tales previsiones tuviera en cuenta estos elementos determinantes del contexto. Se impone, por tanto, una aplicación pragmática de las exigencias de tal normativa en tales instituciones y, en todo caso, que se haga uso de las competencias que tanto las Diputaciones provinciales como en algún caso las comarcas tienen para asistir técnicamente a tales municipios y dotarles de las herramientas básicas que puedan representar un cumplimiento de mínimos de las obligaciones normativas, cobre todo teniendo en cuenta que el fin de tal marco no es otro que proteger adecuadamente los datos personales y los derechos fundamentales de la ciudadanía.

**ANEXO 1: DERECHOS QUE SE ALOJAN EN EL "DERECHO RACIMO" *A LA PROTECCIÓN DE DATOS PERSONALES* SEGÚN EL RGPD Y LA LOPDGDD (Y QUE LAS ADMINISTRACIONES PÚBLICAS DEBEN RESPETAR EN SUS TRATAMIENTOS DE DATOS Y EN SUS ACTIVIDADES QUE TENGAN CONEXIÓN CON LOS DATOS PERSONALES)**

| **Derechos** | **RGPD** | **LOPDGDD** |
|---|---|---|
| *Transparencia Información/Información y acceso datos personales* | Artículos 12-14 | Artículo 11 |
| *A solicitar acceso a los datos* | Artículo 15 | Artículo 13 |
| *De rectificación* | Artículo 16 | Artículo 14 |
| *De supresión ("el derecho al olvido")* | Artículo 17 | Artículo 15 (Ver asimismo artículos 93 y 94) |
| *A la limitación del tratamiento* | Artículo 18 | Artículo 16 |
| *Obligación responsable del tratamiento de notificación de la rectificación o supresión de datos personales o limitación del tratamiento* | Artículo 19 | |
| *A solicitar a un proveedor de servicios que transmita sus datos personales a otro o se los provea (A la portabilidad de los datos)* | Artículo 20 | Artículo 17 (Ver asimismo artículo 95) |
| *De oposición y decisiones individuales automatizadas* | Artículo 21 | Artículo 18 |
| *Al consentimiento expreso* | Artículos 4.11, 6 y 7 | Artículo 6 y 7 |
| *A ser informado sin dilación indebida, si sus datos se pierden o son robados: obligación responsable del tratamiento (excepciones)* | Artículos 33-34 | |
| *A la protección en línea para los menores* | Artículo 8 | Ver, asimismo, artículos 84 y 92, así como la disposición adicional 18ª |

**ANEXO 2: Derechos digitales. Cuadro-resumen orientativo de los derechos digitales en la LOPDGDD**

(Ver, en relación con el carácter de estos derechos digitales, epígrafe IV preámbulo y artículo 79: "Los derechos en la Era digital)

| **Artículo/Derecho** | **Reserva Ley Orgánica o Ley ordinaria** | **Observaciones** |
|---|---|---|
| *Artículo 80: Derecho a la neutralidad de Internet* | Ley ordinaria | Declarativo |
| *Artículo 81: Derecho de acceso universal a Internet* | Ley ordinaria | Programático. Requiere medidas complementarias (y presupuestarias) para aplicarse |
| *Artículo 82: Derecho a la seguridad digital* | Ley ordinaria | Declarativo, no anuda consecuencias al incumplimiento |
| *Artículo 83: Derecho a la educación digital* | Ley Orgánica | Muy importante y necesario. Test aplicativo. Competencias digitales del profesorado. ¿Inclusión en temarios? Problema: ¿cómo se acreditan las competencias).<br><br>Ver, artículo 92.<br><br>Ver asimismo DA 21ª (Educación digital); DF 8ª "Modificación LOU"; DF 10ª ("Modificación LOE"): inserción del alumnado en la sociedad digital |
| *Artículo 84: Protección de los menores en Internet"* | Ley Orgánica | Muy importante. Programático en su primer apartado y preventivo/sancionador en el segundo (Ministerio Fiscal)<br><br>Ver, asimismo, DA 18ª: "Derechos de los menores ante Internet", elaboración en el plazo de 1 año de un proyecto de ley en la materia |
| *Artículo 85: Derecho de* | Ley Orgánica | Importante: Regula el derecho de rectificación |

| | | |
|---|---|---|
| *rectificación en Internet* | | en Internet, complementa la normativa vigente y cubre un hueco |
| *Artículo 86: Derecho a la actualización de informaciones en medios digitales* | Ley Orgánica | Importante: Una suerte de derecho de rectificación y actualización de la información, para evitar perjuicios al afectado |
| *Artículo 87: Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral* | Ley Orgánica | Conexión con la intimidad y la propia imagen. Establecimiento de criterios. Participación de los representantes de los trabajadores. Usos para fines privados. Ver DF 13ª, incorporación nuevo artículo 20 bis ET<br><br>Ver: DF 14ª Modificación artículo 14 TREBEP |
| *Artículo 88: Derecho a la desconexión digital en el ámbito laboral* | Ley ordinaria | Mucho impacto mediático: modalidades de ejercicio se sujetan a negociación colectiva o, en su defecto, a acuerdo en la empresa. Empleador debe elaborar una política interna. Evitar riesgo de fatiga electrónica.<br><br>Ver DF 13ª, incorporación nuevo artículo 20 bis ET<br><br>Ver: DF 14ª Modificación artículo 14 TREBEP |
| *Artículo 89: Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo* | Ley Orgánica | Protección intimidad<br><br>Funciones del artículo 20.3 ET.<br><br>Ver DF 13ª, incorporación nuevo artículo 20 bis ET: "Derechos de los trabajadores a la intimidad en relación con el entorno digital y la desconexión"<br><br>Ver: DF 14ª Modificación artículo 14 TREBEP |

| | | |
|---|---|---|
| *Artículo 90: Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral* | Ley Orgánica | Protección de datos: Información del empleador de tales dispositivos<br><br>Ver DF 13ª, incorporación nuevo artículo 20 bis ET.<br><br>Ver: DF 14ª Modificación artículo 14 TREBEP |
| *Artículo 91: Derechos digitales en la negociación colectiva* | Ley Orgánica | Convenios colectivos: garantías adicionales |
| *Artículo 92: Protección de datos de los menores en Internet* | Ley Orgánica | Obligación centros educativos. Difusión a través de redes sociales o servicios equivalentes: consentimiento menor o de sus representantes legales.<br><br>Ver, asimismo, artículo 84 y disposiciones allí citadas |
| *Artículo 93: Derecho al olvido en búsquedas de Internet* | Ley Orgánica | Complemento de lo dispuesto en el Capítulo II del Título III |
| *Artículo 94: Derecho al olvido en servicios de redes sociales y servicios equivalentes* | Ley Orgánica | Derecho a supresión de datos facilitados para su publicación por servicios de redes sociales y servicios de la sociedad de la información |
| *Artículo 95: Derecho de portabilidad en servicios de redes sociales y servicios equivalentes* | Ley ordinaria | Reglas para el acceso a los contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. |
| *Artículo 96: Derecho al testamento digital* | Ley ordinaria | Complementa los previsto en el artículo 17 |
| *Artículo 97: Políticas de impulso de los derechos digitales* | Ley ordinaria | Programático |
| *Disposición Final 13 ª: Modificación del ET.* | Ley ordinaria | Derecho a la intimidad en uso de dispositivos digitales , videovigilancia |

| | | |
|---|---|---|
| *Nuevo artículo 20 bis* | | y geolocalización y desconexión. |
| *Disposición Final 14ª: Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público* | Ley ordinaria | Derecho a la intimidad en uso de dispositivos digitales , videovigilancia y geolocalización y desconexión.<br><br>(reitera artículo 20 bis ET y se aplica a los mismos supuestos |