El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales

Rafael Jiménez Asensio

RESUMEN

Este estudio analiza el nuevo marco normativo en materia de protección de datos personales y su incidencia sobre el gobierno local. En particular, este trabajo tiene por objeto identificar cuáles son los elementos básicos del sistema de gestión de protección de datos personales que se deben implantar las Administraciones Locales como consecuencia de las reglas establecidas en el nuevo marco normativo (RGPD y LOPDGDD). Asimismo, se lleva a cabo un análisis crítico de algunas dificultades que presenta la implantación de ese sistema en determinados gobiernos locales y también se tratan críticamente aspectos relativos a la regulación realizada por el legislador interno.

Palabras clave: Protección de Datos personales, Administración Local, Delegado de Protección de Datos.

ABSTRACT

This study analyzes the new normative framework regarding the protection of personal data and its impact on local government. In particular, this work aims to identify what are the basic elements of the personal data protection management system that Local Administrations must implement as a result of the rules established in the new regulatory framework (RGPD and LOPDGDD). As well, a critical analysis of some difficulties presented by the implementation of this system in certain local governments is carried out, and aspects relating to the regulation carried out by the internal legislator are also critically treated.

Key words: Protection data rights, Local Government, Data Protection Officer.

SUMARIO

I. PRELIMINAR

1. El nuevo marco normativo del RGPD y de la LOPDGDD como cambio de paradigma

La nota distintiva del actual marco normativo, comprendido por el binomio RGPD/LOPDGDD frente al anteriormente existente (Directiva-LOPD) reside en que el nuevo modelo transita *desde un planteamiento reactivo a otro 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. 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 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 también a las Administraciones Locales (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 de protección de datos, 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 regula minuciosamente en el RGPD y 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, que se puedan ver involucrados por conexión o consecuencia.

Como se ha venido reconociendo, también por la Agencia Española de Protección de Datos (Informe sobre el anteproyecto 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, también en el sector público.

Pero el RGPD se enmarca en un contexto ineludible de economía digital, en la que el dato es el elemento sustantivo. Y no pretende, en ningún caso, obstaculizar ese desarrollo. A tal efecto, uno de los objetivos del RGPD es también establecer «las normas relativas a la libre circulación de datos personales». Por tanto, como también prevé el art. 1.3 RGPD: «la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados son la protección de las personas físicas en lo que respecta a la protección de datos personales».

Ambas ideas citadas tienen perfecto reflejo en los Considerandos 7 y 101 del RGPD. La Unión Europea ha sido la primera instancia que se ha inclinado por una regulación «regional» (superando así el estrecho marco de actuación estatal) de la protección de datos personales y por exigir a todas esas grandes empresas tecnológicas (así como al resto de sujetos obligados, entre ellos a las Administraciones Públicas) el cumplimiento de una exigente normativa.

El nuevo marco normativo se asienta sobre una serie de principios que todos los responsables y encargados del tratamiento deben respetar, algunos de tales principios han sido redefinidos. Y, junto a tales principios, se ha configurado un nuevo catálogo ampliado de dimensiones de derechos específicos vinculados con ese *derecho racimo* que es la protección de datos personales. El dato importante a nuestros efectos es que tales derechos deberán ser garantizados en su ejercicio a las personas físicas 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. Sobre ellos nos detendremos brevemente más adelante.

La Administración Local, a través de los responsables y encargados del tratamiento, debe cumplir fielmente los principios relativos al tratamiento, debiendo informar toda la actuación pública en cualquier tratamiento de datos personales (art. 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 el consentimiento del afectado sea una base legítima de tratamiento en el sector público. Por tanto, de aceptarse esta tesis, solo 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 (art. 6 RGPD, letras c) y e), serían bases jurídicas del tratamiento de datos en las Administraciones Públicas. 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 Local 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.

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. Si bien cabe constatar que, al menos en la adaptación llevada a cabo por el legislador orgánico de las previsiones del RGPD, tales medidas sancionadoras se diluyen casi completamente cuando de aplicarlas a las Administraciones Locales y a sus entidades del sector público se trata, tal como ha quedado regulado el art. 77 de la LOPDGDD. Este último precepto 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 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 RGDP/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. Particularmente 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 (*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 (AEPD/AVPD/adpCAT) 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 el art. 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 y por las entidades de su sector público (con las matizaciones que se harán en su momento). Sin duda, el reto es importante. Y no cabe orillar que el proceso de adaptación de las estructuras organizativas de las Administraciones Locales y de sus entidades del sector público será lento y gradual, más aún cuando los incentivos para ese proceso de adaptación son pocos y las sanciones enormemente blandas, lo que puede generar aplicaciones lentas o, incluso, poco efectivas en el sector público. Especialmente complejo será ese proceso de cambio en los municipios o entidades locales que no dispongan de capacidad de gestión o de recursos al efecto. Hay, como se señala luego una suerte de ficción a la hora de considerar que cualquier «organismo o autoridad pública» está en condiciones de llevar a cabo semejante adaptación en los plazos que marca la legislación vigente.

En verdad, la adaptación de la gestión de protección de datos al nuevo modelo dibujado por el RGPD debería implicar, 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. Algo que, insistimos, no resultará fácil en las entidades locales de pequeñas o medianas dimensiones.

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 Locales (menos aún por lo ya expuesto: las obligaciones de implantar el nuevo modelo en el sector público no vienen

acompañadas de las exigencias sancionadoras que se aplican al sector privado). 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 (art. 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». También la Administración Locales 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 RGPD y en la LOPDGDD. En ese justo y complejo equilibrio es en el que deberá moverse la acción de los poderes públicos.

Ni qué decir tiene que la Administración Local que haya invertido más en ese proceso de adaptación al binomio normativo RGPD/LOPDGDD y sobre todo haya interiorizado su propia filosofía dispondrá de mejores recursos para poder enfrentarse a esos acelerados cambios que se advierten en un horizonte que no va más allá de los 5-10 años. Posiblemente muchas organizaciones y entidades del sector público local se despierten tarde en ese proceso de necesaria adaptación, tal como pasó con la implantación de las previsiones del RGPD: el 25 de mayo llegó y poco o nada se había hecho. El 7 de diciembre de 2018 ha llegado y ha sucedido lo mismo. Pero, sea cual fuere la situación, lo que sí parece obvio es que el sector público seguirá teniendo retos ineludibles que cumplir en ese largo, pero necesario, camino de implantación de esa nueva concepción de defensa de los derechos fundamentales de las personas físicas a través de la protección de los datos de carácter personal. El cambio de paradigma abierto por el RGPD se ha cerrado con la LOPDGDD. Y los retos a abordar son muchos y de gran calado. Hay, pese a que no se perciba todavía de forma generalizada, mucho en juego.

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

Tras más de un año de tramitación parlamentaria, el *BOE* del 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 13 de diciembre de 1999 (LO 15/1999), y asimismo derogó el más reciente Real Decreto Ley 5/2018, de 27 de julio, 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 [...]»). Mediante tales derogaciones expresas se daba cumplimiento, así, a la necesaria adaptación normativa del Derecho interno a las previsiones del RGPD.

Este breve apartado tiene como única pretensión resaltar telegráficamente algunos de aquellos aspectos que, por lo que afecta a la Administración Local y a su sector público institucional, 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 solo con 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) se configuró como la norma que desarrolla y concreta 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[1]. 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

1 Ver: RODRÍGUEZ ÁLVAREZ, L.: «Artículo 18.4 CE», *Comentarios a la Constitución de 1978. Libro Homenaje al Profesor Luís López Guerra*, Valencia, Tirant lo Blanch, 2018.

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.

Este nuevo marco normativo ha venido además adornado por la inclusión (estirando hasta el infinito el art. 18.1 y 4 CE) de los denominados *derechos digitales,* cuyo parentesco con el objeto de la Ley se visualiza exclusivamente en la propia digitalización y 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 lo «digital» o 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 en su día 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 es objeto de este trabajo el estudio de tales derechos digitales, algo que, de forma genérica, ya la abordé en un comentario anterior[2]. Sobre los derechos digitales han reflexionado recientemente diferentes autores en distintos espacios abiertos, como por ejemplo lo siguientes: Eduardo Rojo Torrecilla, por lo que afecta al campo de los derechos digitales en el ámbito laboral[3]; o Concepción Campos Acuña, desde una óptica más general[4], entre otras muchas referencias que se podrían traer a colación. No cabe ocultar que su inserción en

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

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

4 Ver: http://concepcioncampos.org/10-puntos-que-debes-conocer-ya-de-la-nueva-lopd-y-gdd/

el proyecto de LOPD fue promovida por un parlamentario socialista, Artemi Rallo Lombarte, que unía a esa condición la de Catedrático de Derecho Constitucional y ex Director de la AEPD. Sus trabajos sobre estos temas ya anunciaban su inquietud por el campo de los derechos digitales, donde ya apostaba por la constitucionalización de tales derechos digitales, si bien, por razones pragmáticas, ese reflejo constitucional se ha visto aplazado y se han proyectado sobre una regulación en la Ley Orgánica de Protección de Datos (ahora también de «Garantías de los derechos digitales»)[5]. 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, incluso, que se difieren en su concreción posterior a normas jurídicas de distinto carácter o a propias normas convencionales.

Por tanto, lo que ahora nos interesa es una mera identificación de algunos aspectos importantes que pueden tener interés de la nueva regulación (LOPDGDD) en cuanto que innovan determinadas cuestiones en relación con la normativa anteriormente vigente, como consecuencia de la necesaria adaptación al RGPD. 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 cuestiones que se pueden extraer del articulado, teniendo como foco de atención la Administración Pública y, en particular, sus posibles impactos sobre las entidades locales.

Del 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 art. 18.4 CE (una auténtica percha de dimensiones descomunales a partir de esta ley de donde cuelgan implícitamente, junto con el art. 18.1 CE, un número desorbitado de derechos digitales, diecinueve concretamente; aparte del propio derecho a la protección de datos personales, esta vez por decisión del legislador y no de la jurisprudencia constitucional). Allí se reitera la jurisprudencia más significativa del Tribunal

5 Ver, por todos, su trabajo: «De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)», *Revista de Derecho Político*, 100, UNED (septiembre-diciembre de 2017), pp. 639-669.

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 RGPD. 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 que lleva a cabo 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, LTAIBG, 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 ma-

yor 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. NUEVO SISTEMA INSTITUCIONAL Y DE GESTIÓN DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA

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 Locales. 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» (art. 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 este enfoque de riesgos y preventivo implica un cambio frontal de cultura organizativa 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, pues la protección de datos de las personas físicas es un bien a proteger especialmente por lo que a la afectación a los derechos fundamentales respecta.

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, así como las distintas Guías y materiales que ponen en marcha y elaboran estas autoridades de control (AEPD y las autonómicas), junto con las propias Administraciones Públicas, son 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, especialmente en el sector público local. 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 debía 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 dos años su aplicabilidad precisamente para garantizar su efectividad y llevar a cabo tal proceso de adaptación. Pero aún así todavía pesa mucho la cultura jurídica que vive apegada al *BOE* y sigue teniendo una percepción relativa 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. En efecto, hasta la publicación de la LOPDGDD buena parte de la comunidad jurídico-operativa del sector público local no fue plenamente consciente de que las cosas han cambiado de forma radical. Sin duda, ese cambio de escenario ya no tiene vuelta de hoja y habrá de aclimatarse a sus inevitables incidencias.

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, así como de las referencias a los tratamientos especiales (Función Estadística Pública, Archivos de interés público, etc.), 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 Y EN LA LOPDGDD
Responsables/Encargados del tratamiento	Capítulo IV RGPD (arts. 24-29) Arts. 28, 29, 30, 33 y DTR 5ª LOPDGDD
Registro de las Actividades de tratamiento	Art. 30 RGPD Art. 31 LOPDGDD
Seguridad de los datos personales	Arts. 32-34 RGPD Art. 32 LOPD
Análisis de Riesgos	Proceso previo, en su caso, a la evaluación de impacto (Art. 24-25 y 35-36 RGPD y 28 LOPDGDD)
Evaluación de impacto relativa a la protección de datos	Arts. 35-36 RGPD
Delegado de Protección de Datos	Arts. 37-39 RGPD Arts. 34-37 LOPDGDD
Códigos de Conducta	Arts. 40-41 RGPD Art. 38 LOPDGDD
Mecanismos de Certificación	Arts. 42-43 Art. 39 LOPDGDD
Autoridades de Control (AEPD/ACPD)	Arts. 51-59 (especialmente) Títulos VII y VIII LOPDGDD
Régimen de Sanciones	Capítulo VIII RGPD Título IX LOPDGDD
Tratamientos concretos (Videovigilancia, Sistema de denuncias internas, Función estadística pública, Archivos de interés público, Infracciones y sanciones administrativas)[6]	RGPD: referencias por buena parte del articulado Título IV LOPGDD

6 Sobre estas cuestiones puede consultarse, MORO CORDERO, M.A. Ascensión: «Tratamientos concretos en el ámbito local: la función estadística, con fines de archivo e infracciones y sanciones», en CAMPOS ACUÑA, C. (dir.): *Aplicación práctica y adaptación de la protección de datos en el ámbito local. Novedades tras el Reglamento Europeo,* Wolters Kluwer, 2018, pp. 175 y ss.

El objeto, por tanto, de esta segunda parte del trabajo 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.

En cualquier caso, tiempo habrá de profundizar en todos y cada uno de los elementos citados[7]. Sin duda, el análisis puntual de todos y cada uno de los elementos citados debe tener especialmente en cuenta en estos momentos la regulación llevada a cabo por la LOPDGDD, que adapta y desarrolla algunos de los elementos de ese Sistema de Gestión de Protección de Datos personales.

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

A. Responsable de tratamiento: regulación en el RGPD

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».

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. Junto a esta figura también se encuentra otra que es la del «encargado del tratamiento» (que ha sido objeto de algunas modificaciones importantes en su régimen jurídico, tal como se verá), ambas deben estar condiciones de cumplir sus obligaciones en materia de protección de datos. Y, además, 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.

7 En algún caso, como es la figura del Delegado de Protección de Datos, ya lo hemos hecho en un trabajo previo; véase: http://laadministracionaldia.inap.es/noticia.asp?id=1508368. Asimismo, con carácter general, puede consultarse nuestra reciente monografía *Introducción al nuevo marco normativo de la protección de datos personales en el sector público* (IVAP, Oñati, 2019), en la que se desarrollan con mas detalle algunas cuestiones que aquí se tratan en estas líneas de forma más epidérmica.

El responsable del tratamiento es quien determina, según la definición del art. 4, los fines y medios del tratamiento. La regulación específica de la figura del responsable de tratamiento se halla en los arts. 24 a 27 RGPD, si bien el Reglamento está plagado de referencias permanentes a esta figura, que se transforma 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 Esta idea se refleja perfectamente en el art. 24 RGPD, cuyo apdo. 1 expone, por ejemplo, lo siguiente: «Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario».

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 art. 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».

B. **Responsable de tratamiento: regulación en la LOPDGDD**

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 art. 28, especialmente por lo que se refiere a los criterios para determinar los mayores riesgos en la adopción de las medidas organizativas y técnicas (arts. 24 y 25 RGPD; art. 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 que se recogen en tal precepto.

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. Todo ello no deja de ser una ficción jurídico-organizativa en cuanto que tales responsables políticos rara vez son conscientes de las exigencias y obligaciones que se le anudan a esa función de responsable del tratamiento.

En efecto, esta caracterización de un órgano de naturaleza política como responsable del tratamiento (de cualquier tratamiento) se transforma fácilmente en una suerte de (auto) engaño, 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 para la mayor parte de las entidades del sector público y de «sus» responsables (art. 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 (sobre todo cuando suceda algo grave, que alguna vez acaecerá) 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 o de responsabilidades «difusas» sería razonable que las Administraciones Locales regulasen por medio de la potestad normativa local qué es responsabilidad de los responsables, cuál es el papel 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).

C. **El encargado del tratamiento en el RGPD**

Su regulación en el RGPD se encuentra recogida en los arts. 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 disposición normativa 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. De ahí que la regulación de esta figura se prevea con cierto detalle.

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

- El apdo. 1 expone lo siguiente: «Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este 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.»
- En el apdo. 2 se regula que 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 art. 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 (art. 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 art. 28.1 a 4.
- Y, en fin, se incorpora una importante cláusula de desplazamiento de la responsabilidad en determinados supuestos (art. 28.10).

D. **El encargado del tratamiento en la LOPDGDD**

Por lo que afecta a la LOPDGDD, la figura del encargado del tratamiento se regula específicamente en el art. 33, con una mención expresa (e importante) a la proyección estructural de la figura en las Administraciones Públicas (33.4); esto es, a partir de la LOPDGDD queda meridianamente claro (por si no lo estaba an-

tes) que pueden atribuirse las competencias propias de un encargado a un determinado órgano de la Administración Local mediante la adopción de un norma reguladora, lo que facilita la distinción estructural entre quién es responsable y quién deba asumir aquellas 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. Ello justifica más aún la necesidad objetiva de aprobar una normativa local que deslinde con claridad las funciones del responsable y del encargado, así como el rol específico que deben tener los distintos actores que actúen en el Sistema interno de Gestión de Protección de Datos en cada nivel administrativo (DPD, funcionarios, externos, etc.).

Las notas más relevantes de esta figura de encargado tal como aparecen recogidas en el art. 33 de la LOPDGDD. Y allí nos remitimos para su correcta comprensión y alcance. Sí que merece atención especial, en relación con los contratos del encargado de tratamiento, 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, que además de prever la vigencia de los contratos hasta 2022, establece que cualquiera de las partes podrá exigir la modificación de tal contrato a fin de que el mismo resulte conforme a lo dispuesto en el art. 28 del RGPD y en el Capítulo II del Título V de la LOPDGDD. Aunque tal previsión se revista de modo facultativo, debe defenderse la tesis de que las Administraciones Públicas, con el fin de salvaguardar los derechos fundamentales de las personas físicas que se pretenden garantizar con el binomio normativo RGPD/LOPDGDD, tienen la obligación de proceder a esa adaptación, dado que si no la normativa de protección de datos quedaría absolutamente suspendida en esos casos hasta 2022, lo cual no sería ajustado a las finalidades del RGPD.

3. Registro de las Actividades de tratamiento

A. El Registro de Actividades de Tratamiento en el RGPD

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. Y esta diferencia es sustantiva.

El marco regulatorio viene establecido por el art. 30 RGPD, donde se establece la obligación de que cada responsable llevará un registro de actividades de tratamiento *efectuadas bajo su responsabilidad* en el que deberá constar la información que se recoge en el art. 30.1 RGPD. Esa misma obligación de llevanza del registro de actividades se recoge en el art. 30.2 RGPD.

En todo caso, 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 asimismo los apdos. 1 (Responsable) o 2 (Encargado) del art. 30 RGPD. Veamos sucintamente en qué se diferencian tales obligaciones por lo que afecta al contenido del registro de actividades y, por tanto, de lo que en este se debe recoger:

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

B. **El Registro de Actividades de Tratamiento en la LOPGDD**

En lo que afecta a la regulación del Registro de Actividades de Tratamiento en la LOPDGDD, cabe tener en cuenta que el art. 31 LOPDGDD, que reenvía a lo establecido en el art. 30 RGPD, regula también el Registro de Actividades de tratamiento.

Cabe dejar constancia que el art. 31 LOPDGDD establece una serie de peculiaridades o aspectos complementarios a la regulación prevista en el RGPD (por ejemplo, entre otras, que el Registro podrá organizarse en torno a conjuntos estructurados de datos o que cualquier adición, modificación o extinción del contenido del registro se deberá comunicar al DPD, figura que en las Administraciones Públicas es de carácter obligatorio, conforme prevé el art. 31.2). Tal

como ha sido expuesto por Lluís Sanz Marco[8], el Registro de Actividades de Tratamiento es la «piedra angular del principio de responsabilidad proactiva y *accountability*», puesto que en cierta medida resume la capacidad del responsable de la organización y es capaz, así, «de demostrar y proporcionar evidencias del cumplimiento del RGPD en todo momento».

Debe tenerse en cuenta en todo caso que el incumplimiento de la obligación de disponer de un Registro de Actividades de Tratamiento es una infracción grave, aunque el régimen sancionador blando establecido por el art. 77 LOPDGDD no incentive –tal como venimos reiterando– precisamente su cumplimiento.

También debe destacarse que la LOPDGDD establece asimismo unas obligaciones de Transparencia-Publicidad Activa en relación con el Registro de Actividades de Tratamiento que todas las Administraciones Públicas deberán satisfacer.

A tal efecto, se debe resaltar únicamente ahora que la disposición final undécima modifica la Ley 19/2013, de 9 de diciembre (LTAIBG), incorporando un art. 6 bis, donde se establece precisamente que los sujetos enumerados en el art. 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 art. 31 de la citada Ley Orgánica».

4. Seguridad de los datos personales

A. Seguridad de datos personales en el RGPD

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. El marco regulatorio es muy preciso, y se recoge en los arts. 32, 33 y 34 del RGPD.

En función de una serie de variables que se enuncian en el art. 32.1 RGPD, «el responsable y el encargado del tratamiento aplicarán medidas técnicas y

8 Ver su trabajo: «Medidas Organizativas para la implantación del marco legal de protección de datos personales. El Registro de Actividades de Tratamiento», en CAMPOS ACUÑA, C.: *op. cit.*, p 251.

organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Las violaciones de la seguridad de los datos representan también una importante novedad del RGPD. Se regulan en los arts. 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.

Hay, por tanto, una obligación institucional doble (de notificación a la autoridad de control y de comunicación a los interesados o afectados), y por tanto está detrás de esta regulación asimismo un *derecho de la persona física a ser informado de las violaciones del sistema de seguridad que entrañen alto riesgo para los derechos y libertades de las personas físicas, que solo puede ceder o modularse en circunstancias tasadas.* El encargado, siempre que se produzca esta circunstancia, debe ponerla de inmediato en conocimiento del responsable.

B. **Seguridad de datos personales en la LOPDGDD**

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 art. 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.

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 (art. 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.

Tal como ha sido expuesto por la doctrina, «el RGPD exige a las Administraciones Públicas la adopción de medidas de seguridad en orden a la protección de los datos de carácter personal, con el objetivo –entre otros– de tratar los riesgos que presente el tratamiento 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 (art. 32 RGPD)»[9]. Por consiguiente, es obvio que tales medidas de seguridad deben ser adoptadas en el marco del Esquema Nacional de Seguridad, en todo lo que concierne a los sistemas de información que tratan datos personales[10].

Asimismo, en esta materia se debe tener en cuenta lo establecido por la disposición adicional novena de la LOPDGDD, en lo que afecta a la notificación de incidentes de seguridad.

5. Análisis de Riesgos

A. Análisis de riesgos en el RGPD

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 art. 32.2 RGPD de forma diáfana.

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.

9 Ignacio Alamillo Domingo, «Esquema Nacional de Seguridad: la Administración electrónica y la seguridad de la información», en CAMPOS ACUÑA, C.: *op. cit.*, pp. 503 y ss.

10 Sobre el Esquema Nacional de Seguridad, por todos, ver FONDEVILA ANTOLÍN, J.: «Sguridad en la utilización de medios electrónicos. El Esquema Nacional de Seguridad, en GAMERO, E. (dir.): *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Valencia, Tirant lo Blanch, 2017.

El modelo del RGPD basado en un enfoque de riesgos se despliega con un carácter preventivo con una finalidad muy precisa: garantizar los derechos y libertades de los interesados desde la definición de una actividad de tratamiento hasta su desarrollo ulterior. Y, a tal efecto, cabe tener en cuenta lo establecido en el art. 25 RGPD, donde se recoge una importante regulación de lo que se enuncia como «Protección de datos desde el diseño y por defecto».

B. **Análisis de riesgos en la LOPDGDD**

Este importante elemento del nuevo modelo de gestión de datos personales no tiene un tratamiento individualizado en la LOPDGDD, pero está presente de forma transversal en buena parte de su contenido. Particularmente importante a estos efectos es la regulación del art. 28 de la LOPDGDD, una cuestión ya analizada en momentos anteriores de este trabajo (véase, el epígrafe relativo a la figura del responsable del tratamiento y de los propios encargado), pues sobre esas figuras recae la necesidad de valorar si procede o no la evaluación de impacto de la protección de datos en función de una serie de elementos que deberán ser tenidos en cuenta en todo caso, tal como prevé el ya citado art. 28.2 LOPDGDD.

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

A. **Evaluación de Impacto en el RGPD**

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. En suma, 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.

La EIDP en los tratamientos de alto riesgo debe llevarse a cabo de acuerdo con los postulados conceptuales establecidos en el Considerando 84 del RGPD y, asimismo, de conformidad con lo previsto en el Considerando 89 *in fine*. El Considerando 90, por su parte, detalla qué son «operaciones a gran escala» y en qué otras operaciones (a raíz, por ejemplo, del tratamiento de «datos de categorías especiales») se requiere EIPD.

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

Por su parte, el art. 35.3 determina en qué casos la EIPD es necesaria en todo caso en los tratamientos:

a) «Evaluación sistemática y exhaustiva de aspectos personales en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar».

b) «Tratamiento a gran escala de categorías especiales de datos»

c) «Observación sistemática a gran escala de una zona de acceso público»

Cabe asimismo hacer referencia a otras cuestiones vinculadas con la EIDP. A saber:

- Para llevar a cabo la EIPD el responsable contará siempre con el asesoramiento de la figura del Delegado de Datos Personales (art. 35.2).
- Hay que tener en cuenta en esta materia las facultades de las autoridades de control (art. 35, apdos. 4, 5 y 6)
- El cumplimiento de códigos de conducta se tendrán debidamente en cuenta al evaluar las repercusiones de las operaciones realizadas por los responsables o encargados (art. 35.8 RGPD).

B. **La evaluación de impacto en la LOPDGDD**

En este punto tampoco hay una regulación específica en la LOPDGDD, por lo que se aplica sin matices lo expuesto en el RGPD, aunque también se trata de una materia transversal. Tal como hemos expuesto, la regulación aplicable en esta materia se recoge en torno a las obligaciones de los responsables y encargados del tratamiento, donde se reitera la necesidad de que tales figuras establezcan las medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento se lleva a cabo de conformidad con lo establecido en el RGPD (art. 28.1 LOPDGDD).

En ese marco, tal como se viene reiterando, son los responsable y encargados quienes deben evaluar si procede o no la evaluación de impacto de protección de datos y, en su caso, la consulta previa establecida en el RGPD.

Y para ello se determinan una serie de supuestos en los que cabe presumir que, aparte de los casos establecidos en el RGPD, se pueden plantear «mayores riesgos», tal como se ha visto. Por su importancia, conviene resaltar de nuevo tales supuestos de forma explícita.

7. El Delegado de Protección de Datos

A. Introducción

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 binomio normativo RGPD/LOPDGDD. De hecho, puede afirmarse que resulta muy complejo implantar todas y cada una de las medidas contenidas en ese marco normativo sin el apoyo activo y la supervisión del DPD, que se transforma de ese modo en una palanca de cambio de notable importancia, por lo que la elección de la persona para el desempeño de tal puesto singular se torna una de las decisiones más relevantes de cualquier Administración Pública o entidad del Sector Público.

Para las Administraciones Públicas, cualesquiera que estas fueran (también, obviamente, las Administraciones Locales), la nota más importante es la obligatoriedad que establece el binomio normativo RGPD/LOPDGDD: 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 (por ejemplo, sector salud) 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, también por las entidades locales o entidades del Sector Público de escasas dimensiones o tamaño, lo cual no deja de ser un tanto cuestionable.

Hay que insertar, por tanto, 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 deber ayudar a ese proceso de transformación organizativa y al cambio en los tratamientos que el binomio normativo RGPD/LOPDGDD exige.

B. La figura del Delegado de Protección de Datos en el RGPD

En ese contexto sumariamente descrito, no cabe duda que 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 y las entidades de su Sector Público.

Pero, además, el DPD es importante que –tal como se exige en la normativa actual– la persona que ocupe ese puesto debe acreditar conocimientos especializados y cualificación pertinente, pues es el punto de apoyo principal del res-

ponsable 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 y aconsejara las medidas técnicas y organizativas que deban adoptarse en todo caso. Especialmente importante es su papel en los procesos de Evaluación de Impacto de la protección de datos, pero asimismo en toda la fase previa. Por parte de la doctrina autorizada, como es el caso del profesor Eduardo Gamero, también se ha resaltado el papel de *Ombudsman* de esta figura, por lo que afecta a la protección de datos de las personas físicas en las Administraciones Públicas[11].

Es en el considerando 97 dónde se dibujan las líneas maestras de esa nueva figura del DPD, que luego serán desarrolladas por los arts. 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*.
4. El DPD *ejerce sus funciones y cometidos «de manera independiente»*

El RGPD utiliza *la expresión «autoridad y organismo público»* a la hora de atribuir la exigencia de crear necesariamente la figura del DPD. La pregunta es obvia: ¿Y qué cabe entender por «autoridad y organismo público» según el RGPD? Esta es una noción que, como expuso el Grupo de Trabajo del Art. 29[12], reenvía al Derecho interno de los Estados miembros. Y, por tanto, tendría que ser la LOPDGDD la norma que precisara su perímetro. Algo que, una interpretación conjunta de los arts. 34.1 y 77.1 LOPDGDD no deja claro, al menos si las sociedades mercantiles de capital público deben disponer o no obligatoriamente de DPD. 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 art. 37.2 RGPD,

11 Ver, su trabajo: «El Delegado de Protección de Datos en las Administraciones Públicas: Ombudsman de datos personales» (http://laadministracionaldia.inap.es/noticia.asp?id=1509261)

12 Ver el documento elaborado por el citado Grupo del Artículo 29: *Directrices sobre los delegados de protección de datos*.

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 arts. 37 a 39 RGPD. El art. 37, dedicado a «la designación» del DPD, que prevé la designación preceptiva: en caso de las autoridades y organismos públicos . También afronta la cuestión de si cabe nombrar uno o varios DPD (por grupo de empresas o autoridad u organismo público, atendiendo a «su estructura organizativa y su tamaño» (art. 37.2 y 3 RGPD), así como la acreditación de competencias profesionales (art. 37.5 en relación con art. 39 RGPD). Y, en fin, de si el DPD debe ser interno o externo; esto es, formar parte de la plantilla o ser un externo a la organización (contratación de servicios) (art. 37.6 RGPD). Por parte de la regulación de la LOPDGDD se añade que el responsable o encargado publicarán los datos de contacto del DPD y los comunicarán a la AEPD.

Por su parte, el art. 38 tiene como objeto «la posición» del DPD en relación con el responsable o encargado del tratamiento. Allí se recogen cuestiones tales como su configuración como colaborador necesario en «todas las cuestiones relativas a la protección de datos personales» (art. 38.1 RGPD); la obligación de que la Administración debe facilitar al DPD los recursos necesarios para el desempeño de sus funciones y para el mantenimiento de sus conocimientos especializados (art. 38.2 RGPD); se determina su estatuto de independencia, en el sentido 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 (art. 38.3 RGPD); se prevé su configuración como punto de contacto, por lo que los interesados podrán acudir al DPD en todo lo relativo a sus datos personales y al ejercicio de sus derechos (art. 38.4 RGPD); también se establece el régimen de confidencialidad del DPD, en cuanto a que está obligado a mantener el secreto o confidencialidad por el desempeño de sus funciones (art. 38.5 RGPD); y, en fin, se recoge la figura del DPD «a tiempo parcial», puesto que podrá desempeñar otras funciones siempre que no den lugar a conflictos de interés (art. 38.6 RGPD)

El art. 39 RGPD define cuáles son, como mínimo, las funciones del DPD, vinculándolas todas ellas especialmente a «los riesgos asociados a las operaciones de tratamiento» (art. 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.

C. **La figura del Delegado de Protección de Datos en la LOPDGDD**

La figura del DPD está regulada en sus rasgos centrales por el RGPD, no teniendo la Ley Orgánica excesivo margen de configuración o de innovación sobre cuál es su perfil o su sentido, pero aún así la LOPDGDD ha establecido una serie de reglas de carácter complementario que terminan por perfilar más cerradamente la naturaleza de esa figura y le dotan de un carácter singular, sobre todo (aunque no solo) por el papel que cumple el DPD como «filtro» en materia de reclamaciones ante la autoridad de control respectiva en materia de protección de datos de carácter personal y, particularmente, en relación con los derechos recogidos en el binomio RGPD/LOPDGDD.

El Preámbulo de la LOPDGDD incorpora una serie de motivaciones a raíz de las cuales se justifican las novedades que se incorporan en el citado texto normativo en relación con la regulación ya establecida en el RGPD.

La regulación de la figura del DPD en la LOPDGDD, por su parte, reitera algunas de las características recogidas en el RGPD (arts. 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 y en las entidades de su sector público se deriva del propio RGPD. No se establece, por tanto, ninguna especificidad al respecto, ni tampoco la Ley Orgánica nos ayuda a identificar en qué entidades del sector público es preceptivo el nombramiento del DPD (si es en todas o solo en parte).
- 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 (art. 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 (art. 34.5)
- El DPD tiene 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, másteres 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 art. 37.5 RGPD

- Se prevé, también en línea con el RGPD, la garantía, siempre que se trate de persona física, de no remoción (salvo supuestos de dolo o negligencia grave) 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. Lo dicho anteriormente, tal vez 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. Según hemos visto, la figura del DPD tampoco puede coincidir con la de responsable de seguridad.
- El DPD tiene la facultad de inspeccionar los procedimientos relacionados con el objeto de la Ley y emitir recomendaciones (art. 36)
- El DPD tiene, asimismo, la facultad de documentar y comunicar a los órganos competentes la existencia de una vulneración relevante en materia de protección de datos.
- Y debe destacarse, como gran novedad de la LOPDGDD en lo que a perfil funcional de la figura respecta, el régimen de intervención del DPD en los supuestos de reclamaciones ante las autoridades de control (art. 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 tampoco se tratan en la LOPDGDD (pues la normativa es de aplicación general tanto para el sector público como para el privado).
- 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 (art. 65.3 LOPDGDD).

Aparte de esas referencias normativas recogidas en el Capítulo III del Título V de la LOPDGDD, que determina el régimen complementario a la regulación del RGPD por lo que afecta al DPD (así como lo establecido en el art. 65.3 LOPDGDD ya citado), deben tenerse en cuenta otra serie de exigencias adicionales que en torno a esta figura se establecen en otros pasajes de ese nuevo marco normativo establecido en la LOPDGDD y que impactan sobre aspectos puntuales del tratamiento de datos personales y, en particular, sobre la figura del DPD. A saber:

- El art. 31.1, párrafo tercero, prevé expresamente lo siguiente: «Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro (se refiere al Registro de Actividades de Tratamiento).
- El art. 70.2 prevé lo siguiente: No será de aplicación al delegado de protección de datos el régimen sancionador establecido en el Título IX de la LOPDGDD.
- Por su parte, en materia de régimen sancionador, se establecen las siguientes infracciones y una previsión en materia de graduación de sanciones que no resulta, en principio, de aplicación al sector público (salvo que a las empresas públicas no se entienda que es exigible el nombramiento de DPD):
  - Tendrá la consideración de infracción grave, según el art. 73.v): «El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el art. 37 del Reglamento (UE) 2016/679 y el art. 34 de esta ley orgánica».
  - Asimismo, también tendrá la consideración de infracción grave, según el art. 73.w) LOPDGDD: «No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones».
  - Tendrá la consideración de infracción leve, según se prevé en el art. 74.p) LOPDGDD: «No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el art. 37 del Reglamento (UE) 2016/679 y el art. 34 de esta ley orgánica.»

- Y, en fin, el art. 76.2, en lo que afecta a la graduación de sanciones, establece que se tendrá en cuenta disponer, cuando no fuera obligatorio, de la figura del delegado de protección de datos.
- En todos estos supuestos, como es ya conocido, se debe resaltar que el régimen sancionador aplicable a las Administraciones Públicas y a la mayor parte de las entidades del sector público (salvo las empresas públicas) es un *sistema blando* o mucho más benevolente que el que se aplica a los responsables y encargados del tratamiento del sector privado, tal como prevé el art. 77 LOPDGDD (sanciones de apercibimiento y, en determinadas circunstancias, publicidad de las sanciones).

8. Códigos de Conducta y Mecanismos de Certificación

A. **Introducción**

Los códigos de conducta y los mecanismos de certificación son dos instrumentos que entroncan perfectamente con el enfoque «proactivo» que imprime el binomio normativo RGPD/LOPDGDD y van encaminados a salvaguardar la política de cumplimiento en la que se inspira ese nuevo marco de disposiciones aplicables en esta materia. Tienen, por tanto, una orientación preventiva o anticipatoria.

Asimismo son herramientas de carácter voluntario, pero que en el caso de los Códigos de Conducta, una vez asumidos por quienes se adhieran a los mismos tendrán carácter vinculante. Por tanto, caso de suscribirse, implican un compromiso que, en el ámbito del sector público, debiera ser una línea por la implantación y mejora efectiva de ese nuevo modelo de gestión de protección de datos del que venimos hablando en estas páginas.

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 Pública, así como en sus entidades del sector público), también de la Administración Local.*

B. **Códigos de conducta**

a) ***Regulación de los códigos de conducta en el RGPD***

Los rasgos del sistema preventivo y de cumplimiento son evidentes en ciertos pasajes del RGPD. Tal como prevén los arts. 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 art. 32.1 RGPD (art. 32.3 RGPD).

Cabe también tener en cuenta (y este es un punto muy importante por lo que afecta al sector público) que el art. 41 RGPD («Supervisión de los códigos de conducta aprobados»), así como por conexión el art. 40.4 del RGPD, no se aplicarán a los tratamientos realizados por autoridades y organismos públicos (art. 41.6 RGPD: «El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos»)

El RGPD regula en los arts. 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).

b) ***Regulación de los códigos de conducta en la LOPDGDD***

La regulación de los códigos de conducta en la LOPDGDD se contiene en su art. 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 art. 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). También, cabe presumir, se podrán promover por las asociaciones de municipios o entidades locales (por ejemplo, FEMP).
- Ante la inaplicación al sector público (autoridades y organismos públicos) del art. 41 RGPD (organismos o entidades de supervisión), el art. 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 art. 37 LOPDGDD.
- Los códigos serán aprobados por las autoridades de control competentes en cada caso (38.3)
- 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 art. 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 art. 3º LOPDGDD, de conformidad con el reiterado art. 41 RGPD.

C. **Mecanismos de certificación**

a) **Los mecanismos de certificación en el RGPD**

Los arts. 42 y 43 RGPD regulan los mecanismos y organismos de certificación. En el art. 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 (art. 42.3 RGPD).
- La certificación no limitará las responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento (art. 42.4 RGPD)
- Será expedida por los organismos de certificación regulados en el art. 43 RGPD o por la autoridad de control competente, sobre la base de criterios aprobados por dicha autoridad en los términos establecidos en el art. 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 (art. 42.6 RGPD)

b) **Los mecanismos de certificación en la LOPDGDD**

El art. 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.

Ver, asimismo, art. 35 («Cualificación del delegado de protección de datos»), por sus evidentes conexiones con el sistema de mecanismo voluntario de certificación.

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 art. 40 RGPD en el plazo de un año.

9. Autoridades de control independientes: Idea general

A. Introducción

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

No es objeto de este trabajo, por sus especiales características, analizar el papel y funciones de tales autoridades de control, a las que el binomio normativo RGPD/LOPDGDD dedican un buen espacio regulador. En estas páginas solo interesa destacar brevemente cuál es la finalidad de tales autoridades de control, en especial de la AEPD, 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 Públicas 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 que lleven a cabo en este caso las Administraciones Locales.

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 finali-

dad 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».

B. **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 diferentes ámbitos materiales que ahora no interesan; por ejemplo, el Estatuto de independencia de tales (art. 52 RGPD) o las funciones (art. 57 RGPD) o poderes, que se desdoblan en poderes de investigación, correctivos o de autorización y consultivos (art. 58 RGPD). Estas últimas atribuciones son las de mayor importancia a efectos del análisis de las Administraciones Públicas.

C. **Regulación de las autoridades de control en la LOPGDD**

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.

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 (art. 48).
- Se modifica la composición del Consejo Consultivo de la Agencia (art. 49)
- En cuanto a publicidad, serán públicas las resoluciones de la Presidencia que sanciones con apercibimiento a las entidades a que se refiere el art. 77.1 de esta ley orgánica (art. 50).
- En el ámbito de las potestades de investigación y planes de auditoria preventiva hay que tener en cuenta lo dispuesto en el art. 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 art. 52.
- Hay unas importantes reglas sobre el alcance de la investigación (art. 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»

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 arts. 37 y 38.2 de la LOPDGDD (art. 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 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. 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 poner el foco de atención en la aplicación de ese régimen sancionador al ámbito de las entidades locales y de su sector público, que 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.

A. Regulación del régimen sancionador aplicado al Sector Público en el RGPD

El Capítulo VIII del RGPD se enuncia del siguiente modo: «Recursos, responsabilidad y sanciones». De esa amplia y detallada regulación (con un significado endurecimiento del régimen sancionador, tal como ya se ha dicho), solo nos interesa particularmente lo que tiene que ver con la previsión puntual del régimen sancionador para las autoridades y organismos públicos prevista en el art. 87.3 RGPD: «7. 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».

B. **Regulación del régimen sancionador aplicado al Sector Público en la LOPDGDD**

El Título IX del LOPDGDD trata del Régimen sancionador. Y muy brevemente nos interesa hacer mención a la previsión recogida en el art. 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 art. 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 art. 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 (en cuanto personas físicas que desempeñan un cargo o responsabilidad de carácter público), 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. 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 como está actualmente considerado el derecho de acceso a la información pública.

Este *régimen blando en materia sancionadora* se caracteriza por los siguientes elementos:

- El ámbito de aplicación de ese régimen excepcional o singular 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 art. 77 LOPDGDD
- Si la autoridad competente es la Agencia Española de Protección de Datos se procederá a publicar la resolución referida en el art. 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 no se aprueban las leyes autonómicas respectivas (de Cataluña y del País Vasco, así como, en su caso, de Andalucía), lo que a corto plazo no parece muy viable.

Teniendo en cuenta la importancia aplicativa que tiene ese art. 77 LOPDGDD para las Administraciones Públicas y entidades de su sector público, consideramos oportuno por su innegable importancia en su aplicación al sector público local reproducirlo en estas páginas:

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apdo. 1 cometiesen alguna de las infracciones a las que se refieren los arts. 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

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

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apdo. 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

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

Por tanto, en lo que afecta a la Administración local y a las entidades de su sector público debe quedar claro que se este régimen excepcional de sanciones, tal como está regulado en el art. 77 LOPDGDD se aplica a las entidades locales, a los organismos públicos dependientes de estas, a las fundaciones y consorcios adscritos a tales entidades locales, pero no a las empresas públicas de capital total o mayoritariamente local. Asimismo, es a esas entidades citadas, así como específicamente a los responsables y encargados del tratamiento y al personal funcionario o empleado público que lleve a cabo, en su caso, tales operaciones de tratamiento, a las que se les aplican las reglas específicas establecidas en los apdos. 2 a 6 de ese mismo art. 77.

III. **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 local. 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 en-

tidades 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 LOPD-GDD un régimen de sanciones «blando» para la mayor parte de las entidades del 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 lo que afecta a 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/LOPD-GDD) 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* (aunque también completado por un régimen sancionador endurecido, no para las Administraciones Públicas) 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 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 (art. 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»; art. 5.2 RGPD).
- 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 o riguroso si lo que se pretende es 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 casos no hay procedimiento sancionador previsto en las Leyes 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.

5. La implantación de este nuevo modelo de gestión comportará necesariamente, tal como se viene insistiendo, 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 finalida-

des, 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.

6. 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.

7. 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 sin posibilidad alguna de modulación normativa 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, sistema de seguridad, 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 (como es el supuesto de Aragón o de Cataluña) tienen para asistir técnicamente a tales municipios y dotarles, así, de las herramientas básicas que puedan representar un cumplimiento de mínimos de las obligaciones normativas, sobre todo teniendo en cuenta que el fin de tal marco normativo no es otro (algo que no conviene olvidar) que proteger adecuadamente los datos personales y los derechos fundamentales de la ciudadanía.