LA FIGURA DEL *DELEGADO DE PROTECCIÓN DE DATOS*: PERFIL Y ENCUADRE EN LAS ORGANIZACIONES PÚBLICAS (EN ESPECIAL EN LOS ENTES LOCALES). (Ponencia presentada al Seminario de Actualización de Función Pública de la FMC, Barcelona, marzo de 2018)[1]

Rafael Jiménez Asensio
Consultor de Instituciones Públicas y Catedrático (acreditado) de Universidad
Donostia-San Sebastián/Barcelona
https://rafaeljimenezasensio.com/
https://estudiosectorpublico.com/

"Los datos son el eje de todo y supondrán un desafío para nuestras instituciones e incluso para nuestro sentido de la identidad" (p. 233)

"No existen métodos infalibles que nos preparen plenamente para el mundo de los datos masivos; tendremos que establecer principios nuevos para nuestro autogobierno. Tenemos que proteger la privacidad desplazando la responsabilidad de los individuos hacia los usuarios de datos: es decir, que rindan cuentas por su uso. La sociedad debe diseñar salvaguardias para permitir el surgimiento de una nueva clase profesional de 'algoritmistas' que evalúen la analítica de datos masivos" (p. 236)

(Mayer-Schönberger, K. Cukier, Big Data. La revolución de los datos masivos. Turner, 2013)

Introducción

Faltan poco más de dos meses (el 25 de mayo de 2018) para la plena aplicabilidad del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril (en lo sucesivo RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Mientras tanto, en paralelo, la tramitación en el Congreso de los Diputados del Proyecto de Ley Orgánica de protección de datos de carácter personal (BOCG; Congreso de los Diputados, de 24 de noviembre, núm. 13-1; PLOPD, en lo sucesivo), que adapta (o, al menos, eso pretende) la Ley Orgánica anterior (15/1999, de 13 de diciembre) al nuevo marco normativo establecido en la Unión Europea, sigue su curso. Aunque todo apunta que no podrá estar aprobada esta Ley antes del 25 de mayo del presente año, pues cuando esto se escribe no han sido aceptadas las enmiendas a la totalidad en el debate al efecto que se ha realizado en el Congreso de los Diputados y aún se está en el trámite de presentación de enmiendas (con ampliación reiterada del plazo para presentar las mismas)[2], quedando pendiente su tramitación y aprobación en esta Cámara y la subsiguiente intervención del Senado (y, en su caso, el retorno otra vez a la Cámara baja). Poco tiempo para que vea la luz antes de la fecha indicada. Por tanto, el presente trabajo se centrará en la regulación del RGPD y hará alguna mención circunstancial al PLOPD, con la advertencia que la redacción final de la Ley que aprueben las Cortes Generales puede variar notablemente algunas partes de su contenido.

[1] El presente texto es la Ponencia que, sobre el mismo tema, ha sido remitida al Seminario de Actualización de Función Pública organizado por la *Federació de Municipis de Catalunya*, y que tendrá lugar el día 20 de marzo en el IDEC-UPF, en Barcelona. Agradezco al Secretario General de la FMC, Juan Ignacio Soto, así como a la Coordinadora del Seminario, Carme Noguer, la amabilidad que han tenido al permitir la difusión de esta Ponencia a través de otros medios.

[2] Véase: *Diario de Sesiones. Congreso de los Diputados,* núm. 104, 15-02-2018, pp. 28 y ss.

La importancia del RGPD no puede ser puesta en cuestión. Aunque posteriormente pondré de relieve cuáles son algunos de sus precedentes, cabe subrayar ahora que la revolución tecnológica, en la que ya se encuentra inmerso el mundo actual, se caracteriza por la trascendencia que tienen los *datos*, también –aunque no solo- en la propia economía. Se ha dicho, por ejemplo, que los datos son el petróleo de la economía digital, pero eso no es completamente cierto, pues –tal como afirma Franklin Foer, "los datos son infinitamente renovables, no son finitos como el petróleo"[3]. La amenaza a la intimidad por el (mal) uso de los datos es obvia, por tanto. Para entender esa amenaza se pueden traer a colación muchas reflexiones, cada día más abundantes dentro del género de ensayo, pero sin entrar en una larga lista de citas sí que puede ser oportuno en estos momentos recordar lo que dijo en su día uno de los principales asesores de una de las grandes empresas que ejercen el monopolio o cuasi monopolio de Internet. Eric Schmidt, reconocía con toda su crudeza lo siguiente: "Sabemos dónde estás. Sabemos dónde has estado. Podemos saber más o menos lo que estás pensando". El riesgo, por tanto, para la intimidad de las personas que representa esa acumulación de datos y ese cruce casi infinito de los mismos está meridianamente claro. Timothy Garton Ash, en un interesante libro, también nos lo ha recordado recientemente: "Ahora todos somos palomas como transmisor". Y tambien nos recuerda unas palabras del experto en seguridad, Bruce Schneider, que se jactaba de que "la vigilancia es el modelo de negocio de Internet", y concluía del siguiente modo: ""Nosotros construimos sistemas que espían a las personas a cambio de servicios"[4]. Por tanto, queda meridianamente claro que el desafío real y tangible a la privacidad es ya un hecho, que se irá acrecentado con el paso del tiempo. Y las respuestas ante esta amenaza son complejas, pero cualquier solución al problema –como ha recordado recientemente el filósofo Luc Ferry en su última y recomendable obra[5]- pasa inevitablemente por la *regulación*. No hay otra vía. Por eso es de gran trascendencia el alcance que tiene la aprobación del RGPD, que representa un cambio cualitativo en el modo y manera de regular este ámbito de la protección de datos de carácter personal por las instituciones de la Unión Europea, como se verá de inmediato.

No cabe duda, como se ha reiterado hasta la saciedad, que el RGPD supone un auténtico cambio de paradigma en la configuración normativa del problema. Las causas de esta regulación se analizan después, pero están indisolublemente unidas, tal como decía, al desarrollo de la revolución tecnológica, pero también a esa revolución social que ha implicado el desarrollo de Internet y en especial de las redes sociales, aparte de la omnipresencia del buscador de Google, como se ha denominado. Todo ello ha conducido a que "las personas hayan cambiado radicalmente sus hábitos pasando de ser muy celosas de sus datos en los 90 hasta el escenario actual en el que se facilitan abiertamente". Pero el cambio real de paradigma se advierte, tal como se dirá, en una suerte de "responsabilidad proactiva", que representa –como se ha dicho- "nuestra mayoría de edad en lo relativo a la protección de datos personales", puesto que "el nuevo Reglamento deja en nuestras manos el decidir qué medidas implantamos, pero, eso sí, debiendo justificar nuestra elección y, ante todo, acreditar documentalmente su cumplimiento"[6]. El giro en el modelo es, ciertamente, radical; pues se asienta, tal como se verá, en una serie de herramientas de control interno que se ven reforzadas y de las que la figura del Delegado de Protección de Datos es una de las piezas clave, pues por parte de los responsables y encargos del tratamiento hay una obligación de adaptar una política de *privacy by design* y de *privacy by default* cada vez que se vayan a tratar datos personales. Una figura que encontraba alguna referencia incidental en el considerando 49 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, así como en alguna otra práctica tanto de las instituciones europas como de algunos de los Estados miembros, pero aún así su encaje en el modelo final resultante puede considerarse como una de las más importantes novedades de la regulación actual.

---

[3] F. Foer, *Un mundo sin ideas. Las amenazas de las grandes empresas a nuestra identidad*, Paidós, 2017.

[4] Y Schneider, como nos recuerda Timothy Garton Ash, "nos compara con arrendatarios agrícolas en las grandes fincas de Google o Facebook. La renta que pagamos –concluye- son nuestros datos personales" (*Libertad de palabra. Diez principios para un mundo interconectado*, Tusquets, 2017, pp. 387-388).

[5] L. Ferry, *La revolución transhumanista. Cómo la tecnomedicina y la Uberización del mundo van a transformar nuestras vidas,* Alianza Editorial, 2017.

[6] J. L. Rivas López y V. Salgado Seguín, "Hacia la seguridad de los datos después del Reglamento Europeo". Se puede consultar en abierto en Internet.

En efecto, en relación con ese nuevo marco normativo hay una opinión común a la hora de resaltar que una de las novedades más relevantes que se incorporaron a ese RGPD fue sin duda la obligación de que las autoridades u organismos públicos "designen" un *delegado de protección de datos* (DPD, en lo sucesivo; o también denominado por sus siglas en inglés, DPO: *Date Protector Officer*). En efecto, ese cambio de paradigma que se intenta impulsar con el RGPD, y al que también haré referencia en páginas posteriores, no puede realizarse plenamente sin un papel activo y determinante de esta nueva figura que es el DPD, que debe velar por el cumplimiento de la normativa en materia de protección de datos entre otras muchas funciones. La política de *compliance* pide paso también en lo que a protección de datos respecta.

En este trabajo interesa particularmente poner el foco de atención en aquellas cuestiones que afectan al perfil de la figura y a su correcto encuadre en las organizaciones públicas, en especial –dado el foro en el que este trabajo se presenta- a los problemas que se pueden plantear en lo que afecta a su aplicación en las entidades locales. La figura, en cualquier caso, trasciende con mucho los contornos del sector público, para adentrarse con fuerza en el ámbito privado, particularmente empresarial, pero este enfoque no puede ser objeto de análisis en estos momentos. Nos ocupa, por tanto, el impacto de la figura en el sector público. A tal efecto, centraré la atención de modo prioritario en los siguientes puntos:

1) El estatuto de esa figura (lo que el RGPD y el PLOPD califican como "posición").

2) Las funciones del DPD, tal como aparecen recogidas en el binomio RGPD-PLOPD.

3) La proyección orgánica que debe tener ese DPD en la estructura administrativa y qué problemas se plantean al respecto.

4) El sistema de provisión y algunos detalles del régimen jurídico aplicable al DPD en las Administraciones Públicas.

Y, por último,

5) Algunas referencias incidentales, que se recogen a lo largo del texto a las líneas básicas del régimen sancionador aplicable a los responsables y encargados de las Administraciones Públicas y de los organismos y entidades de Derecho Público vinculadas o dependientes de aquellas o en su caso adscritas (Consorcios), así como las que sean aplicable, con carácter general, a los responsables o encargados de las sociedades mercantiles de capital público.

En cualquier caso, lo que sigue no pasa de ser un primer estudio de un problema no exento de notable complejidad y plagado aún (dada su novedad y la impronta singular de la normativa en la que se encuadra) de innumerables incógnitas o dudas aplicativas. A algunas de estas dudas se les intentará dar una respuesta razonable en estas páginas, otras permanecerán abiertas y, en fin, ciertas interpretaciones que aquí de defienden deberán ser contrastadas por su aplicación futura. También veremos hasta qué punto la futura LOPD viene en nuestra ayuda y solventa o no ciertas cuestiones hoy en día abiertas. Por tanto, quedan aún muchas preguntas por responder. Y no pretendo, obviamente, dar solución a todas, sino abrir un camino de reflexión y debate sobre tan importante tema.

No obstante, con carácter previo, conviene llevar a cabo algunas reflexiones de naturaleza introductoria que nos enmarquen con carácter general el problema y, asimismo, nos sitúen en cuáles son las claves generales de por qué se ha aprobado por la Unión Europea esta normativa específica a través de una fuente del Derecho tan reforzada como es la de un Reglamento General de la Unión Europea (al ser obligatorio en todos sus elementos, tener aplicabilidad general y uniforme en todos los países y para todos los ciudadanos y entidades de la UE).

Enmarcando el problema

Resulta oportuno enmarcar, en primer lugar, la figura del DPD en los objetivos generales de la regulación europea. No es adjetivo que el legislador europeo haya optado esta vez por regular esta materia por Reglamento y no por Directiva, como lo fuera antaño (se deroga, así, la Directiva 95/46/CE). Sin entrar en otras consideraciones, el Reglamento UE deja clara la necesidad de "garantizar un nivel uniforme y elevado de protección de las personas físicas", expone que el "tratamiento de dichos datos debe ser equivalente en todos los Estados miembros" y se pretende que la aplicación de las normas en esta materia "sea coherente y homogénea" (Considerando 10).

No es baladí, por tanto, que se haya dado un giro copernicano en el uso del instrumento normativo regulador de la Unión Europea: de una regulación establecida a través de una Directiva en 1995 (Directiva 95/46/CE) se ha pasado a otra, veintiún años después, formalizada por medio de un Reglamento de la Unión Europea (Reglamento UE 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016). En esas dos décadas el mundo de las tecnologías de la información y, por ende, la protección de datos, ha sido objeto de transformaciones espectaculares, por lo que las viejas respuestas frente a un problema que crecía exponencialmente conforme se desarrollaba el mundo tecnológico e Internet, ya no servían.

Esa acelerada transformación tecnológica, unida al fenómeno de la globalización y del aumento de flujos transfronterizos de datos personales, son las causas que desde hace años condujeron a las instituciones europeas a un replanteamiento frontal del problema de la protección de datos que comienza, así, a cuestionar gradualmente los postulados en los que se asentaba la propia Directiva 95/46/CE. El punto de arranque de ese proceso (aunque hay precedentes) puede situarse en el documento de la Comisión de 4 de noviembre de 2010, titulado *Un enfoque global de la protección de datos personales en la Unión Europea*[7]. No es momento para llevar a cabo un análisis del citado documento, pero no cabe duda que en su contenido se advertían ya algunas de las líneas-fuerza de las que se dotará el RGPD de 2016. Allí, por ejemplo, se parte de un claro diagnóstico del problema de la protección de datos, que se sintetiza en los siguientes pasajes. A saber.

Por un lado, se pone de relieve que "la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio y han lanzado nuevos retos en materia de protección de los datos personales (…) Paralelamente, los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad".

Partiendo de ese diagnóstico, el documento establece una serie de "retos específicos" a los que la Unión Europea debe hacer frente:

1. Abordar el impacto de las nuevas tecnologías.
2. Reforzar la dimensión del mercado interno de protección de datos.
3. Hacer frente a la globalización y mejorar las transferencias internacionales de datos.
4. Consolidar las disposiciones institucionales para la aplicación efectiva de las normas de protección de datos.
5. Mejorar la coherencia del marco jurídico que regula la protección de datos.

Y, de acuerdo con este diagnóstico, la conclusión que se extrae es obvia: "Los retos previamente mencionados requieren que la UE elabore un enfoque global y coherente, que garantice el pleno respeto del derecho fundamental a la protección de los datos personales, tanto en la UE como fuera de ésta. El Tratado de Lisboa dotó a la Unión de medios suplementarios para afrontar estos retos: la Carta de los Derechos Fundamentales de la UE - cuyo artículo 8 reconoce un derecho autónomo a la protección de los datos personales – se configuró a partir del TFUE como un texto jurídicamente vinculante, y se ha

[7] Ver, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *"Un enfoque global de la protección de datos personales en la Unión Europea"*, Bruselas, 4.11.2010 COM(2010) 609 final.

creado una nueva base jurídica (artículo 16), que permite la elaboración de una normativa de la Unión global y coherente en materia de protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.". Y, a partir de tales reflexiones, el documento establecía una serie de líneas-fuerza de actuación que, con distinta intensidad y alcance se irán concretando en la normativa que finalmente apruebe la Unión Europea en 2016[8].

La Directiva de 1995 fracasó en su empeño de aproximar las regulaciones de los Estados miembros o quizás se vio desbordada por el acelerado proceso de transformación y uso masivo de los datos personales. Y como reconoció en su momento el dictamen del Consejo de Estado sobre el anteproyecto de Ley Orgánica de Protección de Datos de carácter personal[9], "la necesidad de reducir esas divergencias normativas llevó, por tanto, a la propuesta de aprobación de un Reglamento, norma obligatoria en todos sus elementos y directamente aplicable en todos los Estados miembros (artículo 288 TFUE)". Por consiguiente, a partir de la entrada en vigor (y, sobre todo, desde la fecha de su plena aplicabilidad: 25 de mayo de 2018), el Reglamento (UE) 2016/679 es norma directamente aplicable en todos los países miembros sin que sea necesaria o imprescindible, en principio, ninguna norma de trasposición para que sean plenamente efectivos sus mandatos. La paradoja, de la que se hace eco el propio dictamen del Consejo de Estado, es que "un derecho fundamental protegido por el artículo 18.4 de la Constitución española va a ser directamente y principalmente regulado en una norma europea", con lo que comporta de traslado igualmente del canón de constitucionalidad, que a partir de ahora se regirá, por consiguiente, sin perjuicio de lo que prevé el artículo 18 CE, por lo establecido en la Carta de Derechos Fundamentales de la Unión Europea y por la interpretación que al respecto realice el Tribunal de Justicia del citado RGPD[10].

Sin perjuicio de esa evidente aplicabilidad directa del RGPD, lo que no cabía duda alguna es que la legislación española hasta entonces vigente en la materia (la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, además de toda su normativa de desarrollo) debía adaptarse a lo establecido en el citado Reglamento, pues buena parte de sus previsiones se habían visto plenamente afectadas por la novedosa regulación de la norma europea. En efecto, el hecho de que la Unión Europea hubiese optado por un instrumento normativo de aplicabilidad directa, como es el Reglamento, ello no era óbice para que los Estados miembros debieran complementar o aclarar esa normativa europea a través de instrumentos normativos de su propio ordenamiento jurídico. No en vano, el propio Reglamento (UE) 2016/679 llama en más de cincuenta casos a que lo allí establecido se complemente (o se pueda complementar) por normas de Derecho interno, cuyo rango y procedencia dependerá del sistema constitucional de cada Estado miembro (principio de autonomía institucional en el desarrollo y aplicación del Derecho de la Unión Europea).

---

[8] Entre esas líneas de actuación que entonces ya se identificaban se podían citar, sin ánimo de exhaustividad, las siguientes:

- Proteger los derechos fundamentales de las personas físicas y en particular su derecho a la protección de datos personales, de acuerdo con la Carta Europea de Derechos Fundamentales de la UE.
- Garantizar una aplicación coherente de las normas de protección de datos, habida cuenta de las repercusiones de las nuevas tecnologías sobre los derechos y libertades de las personas.
- Aumentar la transparencia para los interesados.
- Reforzar el control sobre los propios datos (minimización de datos, derecho de acceso, derecho a ser olvidado, portabilidad, etc.).
- Clarificar y reforzar las normas en materia de consentimiento.
- Proteger los datos sensibles.
- Reforzar las vías de recurso y sanciones.
- Reforzar, asimismo, la responsabilidad de los responsables de tratamiento (*accountability*, análisis de impacto, etc.).
- Fomentar incentivos de autorregulación e implantar sistemas de certificación
- Reforzar el marco institucional para una mejor aplicación de las normas de protección de datos.

[9] Dictamen del Consejo de estado de 26 de octubre de 2017, Referencia: 757/2017; asunto: Anteproyecto de Ley Orgánica de Protección de Datos de carácter personal.

[10] STJUE de 26 de febrero de 2013, Melloni, C-399/11.

En cualquier caso, sin adentranos tampoco en este tema, sí que conviene resaltar que el RGPD ha achicado el espacio regulador del legislador estatal, particularmente en este caso por lo que afecta a la reserva material propia del legislador orgánico, produciéndose una enorme paradoja: la Ley Orgánica de Protección de Datos que finalmente se apruebe para adaptarla a lo establecido en la norma de Derecho Europeo, tal como ya se dibuja en el Proyecto de Ley que se está tramitando en estos momentos en el Congreso[11], es una disposición normativa con rango de Ley y con el calificativo de orgánica, pero en verdad en muchos de sus pasajes es una norma de mera "remisión" a lo ya establecido en el propio RGPD, que es finalmente la norma cabecera o principal que regula el alcance y contenido real del derecho fundamental de protección de datos personales, cumpliendo el legislador orgánico una función vicarial y hasta cierto punto de complemento de régimen jurídico o, incluso, de "desarrollo reglamentario" en algunos de sus pasajes, lo que ciertamente devalúa el carácter orgánico de esa regulación, que solo se sostiene por conexión o consecuencia con lo establecido en el artículo 18.4 CE y por la reserva de ley orgánica que "el desarrollo directo" de ese derecho conlleva, aunque en verdad ese desarrollo ha sido regulado primariamente por la norma del Derecho de la Unión Europea, que "seca" o "agota" buena parte de la configuración normativa del derecho fundamental.

Por consiguiente, el operador jurídico español tendrá que actuar en el campo de la protección de datos personales con un binomio normativo de cabecera formado, en primer lugar, por el Reglamento 2016/679 UE y por la futura Ley Orgánica de Protección de Datos, pero teniendo primacía aplicativa el primer elemento normativo de ese binomio en caso de contradicción o antinomia. Y ello se advierte, tal como decíamos, en que la futura Ley Orgánica preverá innumerables reenvíos normativos que requerirán una interpretación integrada (y, en algunos casos, no exenta de complejidad), por mucho que el propio RGPD reconozca que en algunos casos "por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, puedan incorporar a su derecho nacional elementos del presente Reglamento" (Considerando 8). La técnica normativa se entremezcla aquí con la seguridad jurídica y con la calidad regulatoria, ofreciendo un claro ejemplo de regulación primaria de una materia como es la protección de datos a partir de un binomio normativo de procedencia diferenciada en cuanto a los sistema de origen: el Reglamento General de Protección de Datos (Derecho de la Unión Europea), que es la norma principal; y la Ley Orgánica de Protección de Datos (Derecho interno), que resulta la norma complementaria aplicable a nuestro sistema normativo, que desarrolla un derecho fundamental recogido en la Constitución, *pero de acuerdo con los parámetros y contenidos establecidos previamente por el Reglamento Europeo.* Un ejemplo vivo también de la *integración de ordenamientos* o, si se prefiere, de la imposibilidad material de diseccionar tales sistemas normativos que, al fin y a la postre, se integran en uno solo.

Como señalara en su día el Informe de la Agencia Española de Protección de Datos en relación con el Anteproyecto de Ley Orgánica de Protección de Datos Personales elaborado para su adaptación al nuevo marco normativo europeo[12], el Reglamento General de Protección de Datos se adopta con dos claros objetivos:

1) "Por una parte, superar la fragmentación existente en la aplicación de las normas de trasposición de la Directiva 95/46/CE, que ha dado lugar, en la práctica, a la existencia de tantos regímenes de protección de datos como Estados Miembros".
2) Y, por otro, el segundo objetivo "consiste en adaptar las normas de protección de datos a la rápida evolución tecnológica y a los fenómenos derivados del desarrollo exponencial de la sociedad de la información y la globalización que la misma conlleva en el tratamiento de los datos de carácter personal"; dado que, como hemos visto, "fenómenos que en 1995 eran incipientes o ni siquiera se planteaban

[11] Ver: Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, *Boletín Oficial de las Cortes Generales*, Congreso de los Diputados, XII Legislatura, Serie A, 24 de noviembre de 2017, núm. 13-1.

[12] Agencia Española de Protección de Datos, Gabinete Jurídico, *Informe: 0194/2017, sobre Anteproyecto de Ley Orgánica de protección de datos de carácter personal*: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_preceptivos/Administracion_estado/Leyes/index-ides-idphp.php.

ahora son generalmente reconocidos y forman parte del comportamiento diario de todos los operadores involucrados en la normativa de protección de datos".

Todo ello, por tanto, hay que ponerlo en conexión con la finalidad última de la norma de que las personas físicas tengan un control de sus propios datos, así como con la necesidad de "reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas", lo que se manifiesta en un refuerzo también evidente de dos pilares tradicionales en la protección de datos personales: el consentimiento (que siempre habrá de ser expreso) y la información (con una regulación nueva y exigente). Y por una razón de contexto muy obvia, que se expresa con carácter diáfano en el considerando 6 del Reglamento:

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

En efecto, una sociedad globalizada e interconectada de forma intensiva y extensiva abre unos escenarios nuevos a la protección de datos de las personas físicas, dejando añejas determinadas formas de regular esa materia y obligando a afrontar esos problemas con fórmulas nuevas. Los datos personales y, particularmente, la intimidad de las personas físicas, sufre de forma diáfana y cada vez más intensa. Lo que obliga a adoptar medidas especialmente volcadas en identificar riesgos. Y ello es así en toda actividad empresarial. También, como es obvio y por razones lógicas, por lo que afecta al tratamiento de esos datos en el sector público, donde se produce un manejo inusitadamente amplio y extenso de datos personales.

En ese marco es donde hay que incluir ese "nuevo paradigma" en la protección de datos, como acertadamente recoge la AEPD, que transita desde el antiguo modelo de la Directiva 95/46/CE, basado en una serie de obligaciones a las que debían ajustarse los responsables y encargados del tratamiento de datos con el reconocimiento en paralelo "de potestades reactivas", hacia otro modelo (el que se refleja en el RGPD) basado "en lo que se denomina *enfoque de riesgo*; es decir, en la necesaria evaluación por los propios responsables y encargados del tratamiento de los riesgos que su actividad puede generar en el derecho fundamental para que, a partir de esa valoración, adoptar las medidas que resulten necesarias para mitigarlos en todo lo que sea posible". El *principio de responsabilidad activa* toma, así, el testigo y exige de los responsables un cambio de hábitos en cierta medida copernicano: deben aplicar todas aquellas medidas técnicas y organizativas que sean apropiadas para que el tratamiento se lleve a cabo de conformidad con el RGPD. Se instala, como decía, la política de *compliance* (a través, aunque no solo, de la "evaluación de riesgos") en el ámbito de la protección de datos y, por tanto, la cultura de la prevención o, si se quiere, de la anticipación. Y es en este marco dibujado a grandes rasgos dónde la figura del DPD o DPO encuentra su verdadero sentido.

No deja de ser, por tanto, un cambio cualitativo en el modo y manera de enfocar el problema, que –dicho sea de paso- tardará tiempo en arraigar. Bien es cierto que no se abandona, como se verá, la dimensión "reactiva" o "represiva", con el endurecimiento del régimen sancionador (aunque amortiguado en sus efectos por el PLOPD por lo que respecta a las Administraciones Públicas; algo en sí mismo discutible, al menos en su conformación tan blanda), pero sí que hay un cambio de orientación que se manifiesta en la configuración de "un marco modernizado y basado en la rendición de cuentas para la protección de datos en Europa"[13], que se manifiesta asimismo en un modelo que pretende asentarse, como

[13] *Directrices sobre los delegados de protección de datos (DPD),* adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017, Grupo de Trabajo sobre la protección de Datos del Artículo 29. 16/ES WP 243, rev. 1

inmediatamente decía, en una política de cumplimiento, reforzando las responsabilidades y articulando sistemas de autorregulación y de certificación.

Así, ese cambio de paradigma lleva anudado la implantación de ese "modelo de responsabilidad activa" al que hacía referencia, que obviamente representa una alteración profunda del sistema anterior en cuanto que exige una anticipación, así como una actitud activa, del sujeto obligado por la norma, y comportará –como reconoce el Informe de la AEPD- "la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnica y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento".

Y es, efectivamente, en este nuevo escenario que se abre con el RGPD donde encuentra pleno sentido la inserción de esta (relativamente) nueva figura del Delegado de Protección de Datos (DPD, en lo sucesivo). También el Informe de la AEPD lo deja meridianamente claro: "En este modelo, por otra parte, las medidas de carácter organizativo, tales como la designación de un delegado de protección de datos, sobre el que recae la función de asesorar y supervisar las actividades de tratamiento de los responsables o encargados, adquiere un papel fundamental para la salvaguarda del derecho fundamentales de los afectados".

Como también recoge el documento de *Directrices sobre los delegados de protección de datos*, los DPD "serán el elemento central de este nuevo marco jurídico para muchas organizaciones (particularmente para las autoridades y organismos públicos, cuya incorporación de la figura es obligatoria), facilitando el cumplimiento de las disposiciones del RGPD". Ciertamente, esa figura, aunque no reconocida expresamente por la Directiva 95/46/CE, sí que en la práctica se fue desarrollando en varios Estados miembros a lo largo de los años. Y, en palabras del Grupo de Trabajo del Artículo 29, "el DPD es la piedra angular de la rendición de cuentas y el nombramiento de un DPD puede facilitar el cumplimiento", actuando además como intermediario entre las partes interesadas correspondientes: interesados, organismos o unidades de la propia Administración Pública, y autoridades de control. Una triada en la que, más tarde, cabrá detenerse, al analizar la dimensión funcional de tales DPD.

Se abre, por tanto, un enfoque de protección de datos que pretende combinar la prevención con la adopción de mecanismos reactivos. En esta línea cabe incluir, tal como decía, la importante regulación de la evaluación de impacto relativa a la protección de datos (artículo 35 RGPD), que debe poner el foco en aquellos tratamientos que impliquen mayores riesgos; la creación, asimismo, de la figura del Delegado de Protección de Datos; o, en fin, la incorporación de los códigos de conducta como medio de autorregulación para la correcta aplicación del Reglamento (artículos 40 y 41 RGPD), así como la creación de mecanismos de certificación. Y a todo ello se añade una (no tan) nueva arquitectura institucional que sireve de soporte, cuyas mayores innovaciones estriban en la ampliación de las funciones o facultades de las autoridades de control en materia de protección de datos que juegan, así, un rol marcadamente plural de impulsor/supervisor/sancionador.

Se trata, como se señalaba, de articular sistemas que opten por una línea preventiva en aquellos ámbitos que conllevan alto riesgo para los derechos y libertades de las personas físicas, particularmente en aquellas entidades que realizan operaciones de tratamiento de datos a gran escala, algo que habitualmente las administraciones públicas y sus entidades del sector público deben llevar a cabo. Los datos en una sociedad digitalizada e instantánea no pueden detenerse una vez que estos circulan libremente. La seguridad de la información y de los datos es clave en el sector público. Identificar los riesgos y prevenir, así como garantizar los derechos de las personas físicas, son soluciones correctas. En esas coordenadas, aunque no exclusivamente, se debe entender la figura del DPD en las administraciones públicas.

En todo caso, sin ser tampoco objeto de este trabajo, no es indiferente centrar la atención sobre las dificultades implícitas que el nuevo modelo que se pretende implantar representa. No es fácil, en efecto, transitar de una cultura de "cumplimiento reactivo" (es decir, que actúa bajo el imperativo de una norma que, en caso, de transgredirse, conlleva, siempre que se identifique la infracción, sanciones; aunque muy

atenuada una vez más en su aplicación al sector público) a otra de "cumplimiento proactivo", en la cual se emplaza tanto a los responables como a los encargados del tratamiento de datos a que deban tener una actitud siempre alerta para poder identificar aquellos tratamientos de datos en que los riesgos de afectación al derecho fundamental de las personas físicas es más elevado. Y, aunque esa labor de identificación de mayores riesgos y, por tanto, de la necesaria evaluación de estos, es una tarea que es en última instancia obligación de los responsables o encargados del tratamiento, no es menos cierto que el papel del DPD en esas funciones de asesoramiento que a tales figuras debe desarrollar, se convierte en crucial. Más aún si tenemos en cuenta que tales operaciones de identificación y evaluación del riesgo en la afectación al derecho fundamental de protección de datos son tareas absolutamente nuevas, también en las organizaciones públicas, que ofrecerán no pocas dificultades para poderse articular de modo efectivo.

Y aquí, una vez más, entra en juego la figura del DPD, tal como prevé en el artículo 39.2 del RGPD: "Dicho artículo recuerda un principio general y de sentido común, que puede ser pertinente para muchos aspectos del trabajo diario de un DPD (y también, habría que añadir, de un responsable o encargado del tratamiento de datos personales). En esencia, requiere que los DPD establezcan prioridades en lo que respecta a sus actividades y centren sus esfuerzos en las cuestiones que representen mayores riesgos para la protección de datos". Deben, por tanto, focalizar su atención "en los ámbitos de mayor riesgo"[14].

Por tanto, enmarcada la figura del DPP en la finalidad y objetivos de la nueva regulación recogida en el RGPD, estamos ya en condiciones de analizar correctamente el alcance y sentido que el DPD tiene en la estructura y funcionamiento del modelo diseñado en el RGPD de 2016 y que debe ser correctamente aplicado a partir de 25 de mayo de 2018 por todos los Estados miembros y, por lo que ahora respecta, por sus Administraciones Públicas y organismos públicos de ellas dependientes.

Para llevar a cabo este análisis, deberé trabajar no solo con lo que establece el RGPD, sino también con lo que determine en su momento la adaptación del Derecho interno a esas previsiones del legislador europeo mediante la futura Ley Orgánica de Protección de Datos de carácter personal. Al estar este proyecto aún, según decía antes, en fase de tramitación parlamentaria, las referencias que aquí se hagan lo serán siempre al proyecto de Ley presentado por el Gobierno, aunque elaborado –tal como reconoce expresamente el propio Informe de la AEPD ya citado- por una Ponencia creada en el seno de la Sección de Derecho Público de la Comisión General de Codificación de la que formaban parte la Directora de la Agencia Española de Protección de Datos, en su condición de vocal nato de la Comisión y tres vocales adscritos, procedentes de la citada Agencia". De ahí que se pueda reconocer –como indirectamente se advierte en el tono del Dictamen del Consejo de Estado en algunos de sus pasajes- que "la Agencia Española de Protección de Datos ha tomado parte activa (podríamos decir, incluso, que determinante) en la elaboración del Anteproyecto". De ahí también que el propio Informe de la Agencia sea especialmente (auto) complaciente con el contenido del citado Anteproyecto. En cualquier caso, esta es una clave que conviene tener presente a la hora de interpretar el alcance del reglamento y, sobre todo, del Proyecto de Ley en relación con este.

La necesidad de disponer de un DPD por las Administraciones Públicas y sus organismos públicos: cómo delimitar el ámbito de aplicación de esa exigencia.

El artículo 37.1 a) del RGPD establece la obligatoriedad de que siempre que el tratamiento lo lleve a cabo "una autoridad u organismo público" se designe un delegado de protección de datos. A diferencia de lo que sucede con las organizaciones o empresas del sector privado donde el criterio determinante para esa exigencia gira sobre otros parámteros (ver, artículo 37.1, apartados b) y c), del RGPD, así como Considerando 13), en el caso del ámbito público la obligación es directa independientemente del tamaño o número de empleados públicos, así como del tipo de tratamiento de datos que se lleven a cabo. Ello se debe a la presunción de que las Administraciones Públicas y sus organismos autónomos, sean estas cuales fueren, tratan por lo común datos de forma masiva y potencialmente deben aplicar sin

[14] *Directrices sobre los delegados de protección de datos (DPD),* cit., pp. 20-21.

excepciones la normativa europea en toda su plenitud. Por tanto, todas las autoridades y organismos públicos deben disponer de esa figura, en los términos que seguidamente se dirán.

El primer problema surge cuando se trata de delimitar el alcance de la expresión "autoridad u organismo público", pues el RGPD no nos da ninguna pista al respecto, salvo que quedan excluidos de esa doble noción los tribunales de justicia. Como expone razonablemente el Grupo de Trabajo del Arículo 29, "dicha noción debe determinarse en virtud del Derecho nacional"[15]. Según ese documento, la noción incluye con toda claridad a las autoridades nacionales, regionales y locales, así como sus organismos regidos por el derecho público que estén vinculados a tales entidades territoriales. En todos estos casos, independientemente de la entidad, la designación del DPD es obligatoria.

Tal como expone el Grupo, "una labor pública puede llevarse a cabo, y la autoridad puede ejercerse, no solo por las autoridades y organismos públicos sino también por otras personas físicas o jurídicas regidas por el derecho público o privado, en sectores como, según la legislación nacional de cada Estado miembro, los servicios de transporte público, el suministro de agua o energía, las infraestructuras viarias, la radiodifusión pública, la vivienda pública o los órganos disciplinarios de las profesiones reguladas". Tal como se dice en ese documento, "en tales casos, los interesados pueden estar en una situación muy similar a la que se produce cuando una autoridad u organismo público trata sus datos". Por lo que la recomendación de las reiteradas *Directrices* es muy obvia: "Aunque no existe obligación en tales casos, el Grupo de Trabajo del Artículo 29 recomienda como buena práctica que las organizaciones privadas que llevan a cabo una función pública o una función pública designen un DPD".

Por tanto, se debe recurrir para delimitar esos contornos al Derecho interno. Y, por consiguiente, cabrá esperar a cómo se regule definitivamente esta materia en la futura Ley Orgánica de Protección de Datos de carácter personal. En todo caso, en el PLOPD, regula esta cuestión en su artículo 34 mediante la técnica del reenvío a lo establecido en el artículo 37.1 RGPD (lo cual no resuelve nada) y completando esa regulación con la determinación de una serie de entidades en las que, en todo caso, se deberá disponer de tal figura que, en el campo de lo público, salvo en el tema de colegios profesionales y sus consejos generales (en su calidad de corporaciones de Derecho Público). En verdad, esa redacción no añade nada a lo ya establecido en el artículo 37.1 RGPD, salvo las referencias funcionales en las que pudieran estar inmersas algunas entidades del sector público que no tengan en sí mismo la condición de organismos públicos. De hecho, el propio Informe de la AEPD, aún reconociendo el margen de configuración que da el RGPD para ampliar las exigencias de establecer la figura del DPD a otro tipo de entidades, afirma que de tal habilitación no se ha hecho uso. Por tanto, la técnica regulatoria del artículo 34 del PLOPD es altamente discutible y, a nuestro juicio, no sigue plenamente las recomendaciones establecidas por el Grupo de Trabajo del Artículo 29, sobre todo en lo que puede afectar a entidades del sector público con forma de sociedad mercantil, donde la exigencia de la figura parece reenviar a los requisitos establecidos para las empresas con carácter general, sin ser en sí misma obligatoria siempre y en todo caso (lo que no evita que sea recomendable su creación).

Tampoco el artículo 77 del PLOPD resuelve el problema, aunque la materia a la que se refiere no afecta al delegado de protección de datos, sino que se refiere al régimen de sanciones aplicable a determinadas categorías de responsables o encargados del tratamiento de datos. Pero en esa regulación, que podría servir de referencia (o de cierta orientación) para saber en qué casos la noción de autoridad y organismo público se aplica a actividades vinculadas con el ejercicio de autoridad pública o de potestades públicas y exige, por tanto, la creación de un DPD, lo cierto es que allí se entremezclan instituciones y organismos de muy distinta procedencia que se blindan, así, frente al regímen sancionador general (algo que puede ser discutible en términos de efectividad del propio Reglamento), incluyéndose dentro de esas entidades, al margen de órganos constitucionales y estatutarios y autoridades judiciales o autoridades independientes, otras tales como:

[15] *Directrices sobre los delegados de protección de datos,* cit. p. 7. También todas la citas entrecomilladas que aparecen a continuación.

- La Administración General del Estado, las Administraciones de las CCAA y las entidades que integran la Administración Local.
- Los organismos públicos y entidades de Derecho Público vinculadas o dependientes de las Administraciones Públicas.
- Las fundaciones del sector público
- Los Consorcios

Quedan, por tanto, fuera de ese perímetro (que amplía bastante el delimitado formalmente por el todavía vigente artículo 46 de la LOPD 15/1999, de 13 de diciembre) las empresas públicas mercantiles, por lo que parece que también quedan fuera de la exigencia preceptiva de disponer de un DPD, pero no se advierte una correspondencia exacta entre las exigencias de disponer un DPD (artículo 34) y la excepción del régimen sancionador para responsables y encargados del tratamiento (pues en este caso se incluyen, por ejemplo, las Fundaciones del sector público y todos los Consorcios). En cualquier caso, de este breve análisis cabría concluir que, de acuerdo con el artículo 37.1 a) RGPD, entraría plenamente dentro de la noción de "autoridad y organismo público" las Administraciones territoriales y sus entidades u organismos públicos tales como los Organismos Autónomos (y figuras similares) y las Entidades Públicas Empresariales que estén vinculados o dependientes de la administración matriz, así como los Consorcios administrativos adscritos asimismo a una Administración territorial. Parece que igual criterio habría de seguirse con las Fundaciones del Sector Público, aunque su ámbito de actuación puede estar muy alejado de las funciones de autoridad (si no cabe preguntarse qué sentido tiene excluirlas del ámbito sancionador). Todas estas entidades, cabría entender, tendrían la obligación de designar un DPD. No así, en principio, las sociedades mercantiles de capital público, que solo deberían hacerlo en los casos que su actividad de tratamiento de datos se subsuma en alguna de las exigencias previstas en los apartados b) y c) del citado artículo 37.1 RGPD. Parece que la filosofía de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, y su contenido básico, ha podido influir en esa regulación, que no deja de ser muy evanescente y poco precisa.

No obstante, la tesis expuesta anteriormente no es otra cosa que un ensayo de interpretación sistemática para suplir una anomia que el legislador orgánico (al menos en lo que respecta al Proyecto) no ha resuelto adecuadamente. La determinación del correcto alcance de qué se entiende en Derecho interno por "autoridad y organismos públicos" a efectos del nombramiento preceptivo de un DPD, es una cuestión que no está resuelta por la actual redacción del artículo 34 del PLOPD, dejando algunas zonas de sombra que solo pueden desvelarse inicialmente con el régimen de excepción singular que el propio texto del PLOPD establece para la no aplicabilidad del duro régimen sancionador impuesto por el RGPD a las Administraciones Públicas y algunas entidades vinculadas o dependientes de su sector público. Sin duda, el carácter "público" de tales entidades cierra de plano la aplicabilidad de las medidas sancionadoras que se vehiculan a través de multas cuantiosas o de porcentaje sobre el volumen de negocios, pero el legislador del PLOPD podía haber sido más imaginativo en lo que a su aplicación al sector público respecta, pues seguir con el esquema de la LOPD de 1999 puede fomentar el reino de la impunidad en el sector público. Habrá que ver cómo queda definitivamente la nueva LOPD. En cualquier caso, lo más adecuado sería que el propio legislador orgánico definiera con precisión en el artículo 34 del proyecto cuál es realmente el alcance de esa expresión "autoridades y organismos públicos" por lo que a la obligación de designar un DPD respecta.

Tal como decía, el que una empresa pública no tenga la obligación de designar un DPD –de acuerdo con lo que prevé el artículo 37.1 RGPD o el Derecho del Estado miembro- no implica que no pueda hacerlo. En efecto, el artículo 37.4 RGPD establece la posibilidad de esa designación facultativa. Y, de todas formas, puede ser una buena práctica hacerlo, sobre todo en aquellos casos en que se disponga de un holding empresarial público, pues en ese caso se puede acudir asimismo a la fórmula prevista en el artículo 37.2 RGPD (un DPD para un "grupo de empresas"), como se verá a continuación.

Líneas-fuerza de la figura del Delegado de Protección de Datos en los Considerandos del RGPD.

El considerando 97 del RGPD establece con precisión que el DPD es una figura que "ayuda" (*colaborador necesario* lo podríamos denominar) al responsable o encargado de protección de datos en la aplicación efectiva del Reglamento, debiendo ser aquel "una *persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos* si el tratamiento lo realiza una autoridad pública" (con excepción del poder judicial). Es una suerte de "delegado de cumplimiento" del RGPD. La relación entre DPD y la plena efectividad del RGPD en el ámbito público es completa.

Allí también se indica algo que no es menos importante en lo que afecta al estatuto jurídico del DPD. En efecto, su cobertura no solo debe recaer (tal como se verá a continuación) en persona con cualificación acreditada, sino además el propio Reglamento exige que tal figura tenga garantizado un funcionamiento *independiente*, lo cual no es nada adjetivo, sino todo lo contrario. Así, el Considerando 97 concluye del siguiente modo:

"El nivel de conocimiento especializado necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente"

Por tanto, antes de entrar en mayores detalles, hay cuatro notas que el RGPD ha querido remarcar de la finalidad de la figura en los propios Considerandos de la disposición normativa. A saber:

a) Que el DPD es una figura de "ayuda" o de colaboración necesaria (por exigencia normativa) con el responsable o encargado de protección de datos en las funciones de cumplimiento del Reglamento;

b) Que, en todo caso, si el tratamiento de datos lo lleva a cabo una autoridad pública, la persona nombrada como DPD debe acreditar "conocimientos especializados del Derecho y la práctica en materia de protección de datos" (por consiguiente, tales conocimientos se deberían acreditar en un procedimiento objetivo: el PLOPD (en línea con el RGPD) admite, en su artículo 35, la certificación ("entre otros medios") para acreditar tales exigencias[16];

c) Que el DPD puede ser "un empleado" de la Administración Pública o que también cabe la contratación de esos servicios con un profesional o empresa externo;

y d) Que esa figura debe tener un estatuto jurídico que salvaguarde su independencia, lo cual incorpora un elemento existencial y diferencial a lo que sea el DPD en las administraciones públicas y entidades vinculadas o dependientes en relación con otros puestos orgánicos de esas mismas estructuras organizativas. Este es un dato que no conviene perder de vista.

Estatuto jurídico del Delegado de Protección de Datos

[16] Ver, sobre esta cuestión, el Informe de la AEPD al Anteproyecto de la nueva LOPD, donde sobre este tema se indica lo siguiente: "A tal efecto, los esquemas de certificación podrán permitir acreditar los conocimientos de quienes pudieran ostentar esta condición, aunque la certificación no será en ningún caso requisitos imprescindible para acceder a este puesto, dado que el artículo 36 del Anteproyecto los configura como uno de los medios a través de los que podrá acreditarse la posesión de las competencias necesarias". Ver, asimismo: AEPD, *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEP-DPD).* Al parecer se trata –según se ha dicho- "de la primera autoridad europea en desarrollar dicho esquema" (Ver: A. Ortega Giménez y J.J. Gonzalo Domenech, "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", *Revista de la Facultad de Derecho de la Universidad de la República de Uruguay,* núm. 44, 2018.

1) ¿Cuántos DPD debe haber en cada organización? ¿El DPD debe ser una figura interna (insertada en la propia estructura) o externa (contratación de servicios)?

Queda claro, por tanto, que todas las administraciones públicas y organismos públicos vinculados o dependientes de estas deben disponer de modo preceptivo de un delegado de protección de datos. La siguiente pregunta es si debe existir un solo delegado o pueden ser varios, así como si la figura del delegado puede ser asumida por un órgano colegiado o, en cambio, debe tratarse de una figura unipersonal que se manifieste en un órgano de estructura monocrática.

Se ha defendido la posibilidad de que la figura del delegado de protección de datos pueda ser desempeñada por un órgano colegiado y no necesariamente por un órgano unipersonal, sin perjuicio de que ese órgano o unidad del que sea titular se dote después de determinada estructura. En principio, nada parecería impedir ese carácter colegiado de la figura o del órgano que ejerza las funciones de DPD, aunque de la dicción del propio RGPD y del PLOPD parece más bien advertirse que se está pensando en "una persona" y no en un colegio, especialmente en el caso de que se trate de una figura internalizada y no externalizada, pues en este último supuesto (externo) sí que se permite sin ningún problema que pueda ser una empresa la que ejerza tales funciones, aunque al tratarse el DPD de un *punto de contacto* necesario se sugiere –como así lo hizo el Grupo de Trabajo del Artículo 29- que se individualicen esas tareas de asistencia e interlocución.

Los términos del RDPD son bastante contundentes, al exponer en su artículo 37.3 lo siguiente: "Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, *se podrá designar un único delegado de protección de datos* para varias autoridades u organismos, *teniendo en cuenta su estructura organizativa y tamaño*". Del mismo modo, si se toma como referencia la noción de "grupo empresarial", el artículo 37.2 RGPD, como ya se ha visto, indica que "podrá nombrar un único delegado de protección de datos *siempre que sea fácilmente accesible*".

Este atributo de la *accesibilidad* "se refiere a las tareas del DPD como punto de contacto con respecto a los interesandos y a la autoridad de control, pero también internamente dentro de la organización, teniendo en cuenta que una de esas tareas es (como establece el artículo 39.1 a) RGPD) 'informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento'"[17].

Así formulada, la noción de "accesibilidad" debería informar plenamente la arquitectura del diseño de la figura del DPD en aquellas organizaciones públicas que opten por la inserción de una sola figura cuando la estructura de la administración pública o entidad sea suficientemente compleja. *La posición triangular del DPD*, que luego se analizará, determina que la interlocución con los interesados, con la autoridad de control y con sus propios clientes (responsable o encargado y con el resto de empleados públicos) sea o deba ser siempre fluida. Tal como se verá, el DPD actúa como punto de contacto con esas tres instancias o vértices, pero especialmente –dada la finalidad última del RGPD como herramienta normativa para la protección de datos de naturaleza personal- con los interesados. Esta óptica, siempre presente en el Reglamento, se visualiza de modo efectivo en el artículo 38.4, cuando al efecto reconoce lo siguiente: "Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento". La dimensión del DPD como cauce de garantía de los derechos de las personas a sus datos personales parece obvia.

En una organización departamental o sectorial, lo razonable es que haya más de un DPD, salvo que se cumpla ese principio de la "accesibilidad". De hecho, el artículo 37.3 RGPD condiciona la existencia de un único DPD –y no es un dato menor- al hecho de que se tenga "en cuenta su estructura organizativa y tamaño". Una organización departamental de un Ejecutivo autonómico o el del propio Estado, también la de un municipio de gran tamaño, es normal que disponga de varios DPD. Otra cosa es cómo estructurar

[17] *Directrices sobre los delegados de protección de datos*, cit. p. 11.

ese complejo de figuras para adecuarlos a una única forma de actuar. Bajo ese punto de vista se ha barajado también la posibilidad de que existiera un único DPD, pero con "subdelegados" en determinados ámbitos. No es tampoco una opción que quepa descartarla en sí misma, puesto que no está prohibida por el RGPD, y el propio Grupo de Trabajo del Artículo 29 defiende en diferentes pasajes de su documento sobre *Directrices* que ese DPD pueda tener a su cargo personal, inclusive lo considera necesario. La clave está en si existe o no un responsable único o un único encargado o si estos son varios.

Siempre que se haya optado por la internalización de la figura, la primera decisión que se ha de adoptar al respecto es, por tanto, si se crea uno o varios DPD en la estructura administrativa, así como, en su caso, cómo articular la coordinación entre ellos si es que fueran varios, por motivos de coherencia en el funcionamiento interno en lo que a tratamiento de datos y análisis de riesgos, así como al ejercicio de otras funciones, comporta. Se trata de una cuestión abierta, que ni el marco normativo europeo ni la futura LOPD resuelven, sino que entra de lleno en las potestades de autoorganización que las administraciones públicas y las entidades vinculadas o dependientes tienen.

Obviamente en Administraciones públicas, departamentos u organismos públicos de tamaño mediano o pequeño o que no lleven a cabo tratamientos de datos a gran escala, se puede plantear la innecesariedad de tener que disponer de una estructura estable (un puesto de trabajo) a tiempo completo, dado que cabe perfectamente la existencia de un DPD a tiempo parcial, si bien en este supuesto se pueden producir algunos problemas que habrán de resolverse. En este caso, el artículo 38.6 RGPD expone lo siguiente: "El delegado de protección de datos podrá desempeñar otras funciones y cometidos". Pero, una vez reconocida la posibilidad de que exista un DPD con dedicación "parcial", rápidamente advierte que se deberá garantizar por parte del responsable o encargado del tratamiento que el ejercicio de otras funciones o cometidos "no den lugar a conflictos de intereses".

Y esta preocupación del RGPD es normal, sobre todo por el carácter de la figura del DPD como *una suerte de "autoridad (o, si se prefiere, funcionario o estructura orgánica) independiente" dentro del seno de la propia organización*, como seguidamente se verá. En efecto, como enuncia el documento del Grupo de Trabajo del Artículo 29, esa ausencia de conflictos de intereses está estrechamente ligada a la independencia de la figura. Por tanto, atribuir el rol de DPD a determinados puestos de trabajo, siquiera sea como función adicional o adjetiva, puede suponer una vulneración de esa regla recogida en el artículo 38.6 RGPD. Todos aquellos puestos de trabajo que intervengan, directa o indirectamente, en el tratamiento de datos personales, así como tanto los puestos de representación jurídica (en cuanto pueden implicar objetivamente la defensa ante los tribunales de los responsables o encargados) y en especial los puestos de estructura directiva o de jefatura, son ámbitos en los que pueden surgir potencial u objetivamente conflictos de intereses. Lo razonable es no acumular esas tareas con las propias del DPD.

Para facilitar esa delimitación, el documento de *Directrices* establece que "dependiendo de las actividades, tamaño y estructura de la organización, puede ser una práctica recomendable que los responsables y encargados del tratamiento" lleven a cabo, entre otras, las siguientes acciones:

- Determinar los puestos que podrían ser incompatibles con la función de DPD.
- Elaborar normas internas a tal efecto con el fin de evitar conflictos de intereses.
- Incluir una explicación más general (Circular) sobre los conflictos de intereses.
- Declarar que el DPD no tiene conflictos de intereses con respecto a sus funciones como tal, como medio de concienciar sobre ese requisito.
- Incluir salvaguardias en las normas internas de la organización y garantizar que el anuncio de convocatoria para el puesto de DPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de intereses. En este contexto, debe tenerse en cuenta también que los conflictos

de intereses pueden adoptar diversas formas en función de si el DPD se contrata interna o externamente"[18].

Efectivamente, tal como expone el artículo 37.6 RGPD, "el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento *o desempeñar sus funciones en el marco de un contrato de servicios*". Ni que decir tiene que esta opción por la externalización será la preferida por buena parte de las Administraciones Públicas y organismos del mismo carácter, cuando tengan unas dimensiones pequeñas o medianas o se presenten dificultades para poder insertar en la estructura de puestos de trabajo un puesto o estructura de nueva creación (piénsese en las restricciones de carácter presupuestario o en la inexistencia de personas en la organización que reunan el perfil de competencias tan especializado requerido para su desempeño).

En estos casos habrá que acudir a los procedimientos y reglas de contratación pública establecidos en la nueva Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. Pero al margen de las dificultades que conlleva definir cabalmente el objeto de la contratación y sobre todo su ejecución, así como la gestión del propio proceso de contratación pública, habrá que tener especialmente en cuenta las funciones que tales DPD realizan y analizar hasta qué punto esas tareas no pueden representar directa o indirectamente el ejercicio de funciones de autoridad o de potestades públicas. Aparentemente, puede dar la impresión de que las funciones del DPD tienen un contenido muy instrumental o esencialmente técnico, pero tal percepción se desvanece cuando se analizan con detalle tales cometidos funcionales o, al menos, algunos de ellos. Lo veremos más adelante. Si así fuera (esto es, si se advirtiera que el DPD puede realizar, directa o indirectamente, funciones de autoridad), el proceso de externalizar el servicio solo se podría llevar a cabo en la parte más instrumental, debiendo existir siempre un funcionario público que, en su caso, ejerciera en última instancia esas potestades públicas que, en su caso, se pudieran derivar de los procesos de supervisión y, especialmente, de la resolución de aquellas quejas o expedientes que vayan encaminados luego a ser analizados por la autoridad de control.

Una vez más, en este punto el Grupo de Trabajo del Artículo 29 también emitió una serie de criterios. En efecto, el RGPD reconoce que la función del DPD puede ejercerse también en el marco de un contrato de servicios que sea suscrito con una persona física o con una organización ajena a la estructura organizativa del responsable o del encargado del tratamiento. En este caso, el Grupo recomienda que "cada miembro de la organización que ejerza las funciones de DPD cumpla todos los requisitos aplicables de la sección 4ª del RGPD" (artículos 37 a 39). Particularmente hace mención a que ninguna de esas personas que trabaja en la organización pueda tener un conflicto de intereses. Añade la posibilidad de que los distintos miembros que componen esa estructura organizativa que desempeñe el contrato de servicios combinen "capacidades y puntos fuertes individuales para que varios individuos que trabajen en equipo puedan servir a sus clientes de forma más eficaz". El problema consistirá en cómo trasladar estas exigencias al pliego de condiciones administrativas y sobre todo cómo valorarlas en el proceso de licitación, así como supervisar posteriormente la correcta ejecución del contrato.

Y, en este punto, el Grupo de Trabajo finaliza su análisis con una recomendación a tener en cuenta en estos procesos: "En aras de la claridad jurídica y de la buena organización y con el fin de evitar conflictos de intereses de los miembros del equipo, se recomienda asignar claramente las tareas dentro del equipo del DPD y designar una única persona como contacto y (definir la) persona 'a cargo' de cada cliente. Sería también útil, en general, especificar estos puntos en el contrato de servicios"[19].

Sin duda el planteamiento es muy oportuno y lo que nos quiere trasladar es que las Administraciones Públicas que externalicen este servicio en empresas o equipos de profesionales (por ejemplo, despachos colectivos), deberían exigir una individualización de la prestación de los servicios en un miembro de la empresa o del equipo profesional que se singularice como DPD, garantizar que disponga de todas y cada una de las exigencias establecidas en el RGPD y que esa "persona" (no solo la empresa) no incurra en ningún tipo de conflicto de intereses. Y ello tiene su sentido, puesto que la especial posición

[18] *Directrices sobre los delegados de protección de datos*, cit., p. 18.
[19] *Directrices sobre los delegados de protección de datos*, cit. p. 13.

"triangular" del DPD, que no solo interlocuta con la organización contratante y con los responsables o encargados del tratamiento, sino que también proyecta su actividad sobre los interesados (con importantes tareas en este campo) y es asimismo punto de contacto con la autoridad de control, representa con claridad la necesidad objetiva de que se identifique individualmente quién es la personas o personas que ejercen tales funciones de DPD (lo que de paso dificultaría objetivamente que tales funciones se pudieran desarrollar internamente por un órgano colegiado). No en vano el artículo 37.7 RGPD exige por parte del responsable o encargado de protección de datos la publicación de "los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control". Una previsión que parece advertir claramente de la condición individual de la figura de DPD.

2) Perfil de competencias que debe acreditar el DPD

El artículo 37.5 RGPD establece lo siguiente: "El delegado de protección de datos *será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos* y a su capacidad para desempeñar las funciones indicadas en el artículo 39". Se ha venido afirmando, con razón, que de la dicción de esta precepto no se deriva necesariamente la exigencia de que el DPD sea jurista o abogado, puesto que debe combinar adecuadamente conocimientos jurídicos en materia de protección de datos (que deben asimismo extenderse, al menos, al campo de los derechos fundamentales y del Derecho Público, por no añadir otros sectores del ordenamiento jurídico que también se verán afectados en el ejercicio de sus funciones) con conocimientos tecnológicos, especialmente en materia de datos. También se ha venido defendiendo que las empresas de servicios estaban en condiciones mejores para prestar este tipo de funciones ya que podrían aportar un amplio abanico de personas con conocimientos complementarios en ambos campos. Pero, tal como se ha visto, la necesidad (o al menos la recomendación) de que se individualice quién ejerce esa función de DPD rompe relativamente este argumento, aunque es verdad que disponer de un equipo técnico de soporte (especializado en Derecho de protección de datos y en tecnología o seguridad informática o de tratamiento de datos) puede ofrecer más garantías. Lo cierto es que, tras un análisis (como luego se hará) de las funciones atribuidas al DPD no solo por parte del RGPD sino también por el PLOPD, puede convenirse fácilmente que el perfil imperante será el de una persona con formación jurídica pero con buenas herramientas en el plano de la tecnología. Además, un análisis de todas y cada una de las dimensiones puntuales en las que puede intervenir el DPD a lo largo de la regulación recogida en el RPD nos conducen a la tesis de que un alto porcentaje de esas tareas tienen, directa o indirectamente, implicaciones o consecuencias jurídicas (se ha valorado que estas representan en torno a un 80 por ciento), mientras que hay un porcentaje, tampoco despreciable (en torno a un 20 por ciento), que tienen relación estrecha con la seguridad en los tratamiento de datos y, en consecuencia, una dimensión mucho más tecnológica, aunque en ocasiones sea francamente difícil diferenciar ambos planos. En todo caso, es una estimación que, dada la fuente de la que procede (un despacho profesional), probablemente "barra para casa".

En el Considerando 97 del RGPD se establece que el nivel de conocimientos especializados necesario para llevar a cabo las tareas de DPD se debe determinar en función del tipo de entidad sobre el cual proyecte su actividad, especialmente si este proyecta sus funciones sobre una autoridad u organismo público, pues en este caso el perfil de competencias exigido al DPD "para supervisar la observancia interna del presente Reglamento" y proveer de la correspondiente ayuda al responsable o encargado del tratamiento, requiere de una persona que tenga "conocimientos especializados del Derecho y de la práctica en materia de protección de datos".

¿Qué representan realmente esas exigencias? En primer lugar, en cuanto al nivel de conocimientos, es obvio que el Reglamento opta por referencias genéricas que han de concretarse puntualmente y que dependerán necesariamente de la complejidad de la organización y, en particular, del manejo de datos que esa entidad lleve a cabo, así como de si estos se encuadran en "categorías especiales de datos" (o lo que se conoce como datos sensibles). Por tanto, la recomendación del Grupo de Trabajo es que el DPD se elija en función del tipo de organización de que se trate, "teniendo debidamente en cuenta las cuestiones relativas a la protección de datos que surjan en la organización". Las únicas referencias explícitas son las establecidas en el artículo 37.5 RGPD, que reproducen las previstas en el

Considerando 97, y que se despliegan, sobre tres ámbitos de actuación: a) conocimientos especializados en Derecho; b) Práctica en materia de protección de datos; y c) Capacidad para desempeñar las funciones indicadas en el artículo 39 RGPD (que luego tratamos).

Por tanto, se deberían acreditar tales conocimientos especializados, la experiencia en la materia y, asimismo, la capacidad (competencias efectivas) para desempeñar las funciones asignadas. Poca información más nos da el Reglamento. Tampoco nos dice apenas nada sobre esta materia el PLOPD. Así, por tanto, una vez más, es oportuno detenerse en las reflexiones que el Grupo de Trabajo del Artículo 29 expuso en su día.

En el documento sobre *Directrices* se recogen algunas pautas que podrían ser tenidas en cuenta para designar al DPD. Y, entre ellas, se considera "un factor importante" que el DPD "tenga *conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD*". Luego el documento recoge asimismo que "resulta también de utilidad que las autoridades de control promuevan una formación adecuada y periódica para los DPD". Asimismo, y no es un dato en nada menor, el documento hace hincapié en una idea relevante: "En el caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización". Por consiguiente, aparte de las exigencias de conocimientos especializados, el DPD en el contexto público debe acreditar igualmente que dispone de un "conocimiento sólido" del ordenamiento jurídico-público y de los procedimientos administrativos, lo que claramente nos conduce a un profesional (o empresa de servicios profesionales) que vuelca su foco de atención sobre el Derecho Público y el Derecho de las Tecnologías de la Información y de las Comunicaciones, con especial atención a los procedimientos administrativos.

Así las cosas, el primer problema que se plantea en una Administración Pública o entidades dependientes o vinculadas a esta, es a través de qué medios se podrán comprobar esos conocimientos y esa "profunda comprensión del RGPD" que el Grupo de Trabajo sugiere como medio de acreditar las cualificaciones profesionales. Si se trata de una provisión interna se deberán evaluar los programas formativos a los que la persona que concurse ha participado, los trabajos o proyectos realizados, la formación impartida en su caso sobre esta materia y, en fin, las publicaciones que al respecto haya podido elaborar en relación con este tema, pudiendo, en su caso, realizar alguna prueba de conocimientos al efecto de poder acreditar de forma más fehaciente si se dispone o no de esa profunda comprensión exigida. Todo dependerá, una vez más, del puesto de trabajo de DPD, que está directamente relacionado con el tipo de organización. En estos casos cabe presumir que esas personas que concursan disponen de "conocimientos sólidos" por lo que respecta a "las normas y procedimientos administrativos de la organización", pero no estaría de más incorporar algún medio de comprobación de tales exigencias, como por ejemplo cursos de postgrado, cursos de formación evaluados o no evaluados, planes de mejora, programas de formación impartidos sobre esas materias, publicaciones, etc.

Si la provisión es externa, será importante reflejar en los pliegos cómo se acreditarán esos conocimientos. Pero las exigencias allí recogidas no pueden variar mucho de las que ya se han visto para una provisión interna, con la dificultad en este caso de que no pueden incorporarse pruebas de conocimiento y que, por tanto, se deben exigir méritos objetivos a través de los cuales se pueda deducir cuál es el nivel de conocimiento del RGPD (y su práctica en esta materia) por parte de cada licitador: formación, impartición de cursos, proyectos realizados o publicaciones sobre ese ámbito. Parece importante, asimismo, establecer algún medio de comprobación objetivo para garantizar que los licitadores (y obviamente el profesional o empresa que resulte adjudicatario del contrato de servicios) acredite "un conocimiento sólido de las normas y procedimientos administrativos de la organización". Para ello, una vez más, lo procedente sería establecer criterios que puedan medir objetivamente ese conocimiento: años de experiencia en relación con la aplicación de normas y procedimientos administrativos sobre la organización, formación recibida e impartida, proyectos profesionales en los que se ha participado, titulaciones universitarias complementarias (por ejemplo, Doctorado o Masters en estas materias), publicaciones, etc. Obviamente, habría que diferenciar si quien licita es empresa o profesional individual. Si fuera empresa o equipo de profesionales, es importante, tal como se decía, que en los propios pliegos se exija la individualización de quién va a ser DPD y, por tanto, que aparte de que

la empresa acredite trayectoria profesional en ese campo, la deba acreditar asimismo individualmente la persona que hará de "punto de contacto". En el supuesto de que fuera un profesional individual el problema resulta mucho menor, pues debe ser él quien acredite poseer las competencias requeridas para el desempeño del servicio de DPD. Esta "individualización" del DPD en el ámbito de empresas de servicios o de equipos profesionales (despachos) puede conllevar también un control indirecto por parte de autoridad de control (a través del registro de tales DPD) del tiempo que se dedican a estas actividades en función del número de Administraciones Públicas u organismos públicos a los cuales se asiste profesionalmente. Un aspecto nada baladí para evitar la concentración de funciones de DPD en una serie de personas que objetivamente no podrán ofrecer sus funciones de punto de contacto de modo idóneo.

Todas estas exigencias conducirían a que, en estos casos y salvo excepciones puntuales (municipios de escaso tamaño o entidades del mismo carácter) si bien con las observaciones que seguidamente se formulan, sea difícil recurrir al procedimiento de contratación menor. Aunque nada legalmente impediría su uso, lo cierto es que si la adjudicación es directa y sin determinar previamente las condiciones de licitación y de su ejecución, no parece que sea un procedimiento que pueda respetar las exigencias mínimas del RGPD, tal como han sido interpretadas en el citado Documento de *Directrices*. Tal vez la solución estribe en abrir esos contratos menores a licitación (o, al menos, solicitar tres ofertas) junto con unas mínimas prescripciones de los requisitos y exigencias que deberá disponer el adjudicatario del contrato (con referencia a las cualidades profesionales antes expuestas). Se cumplirían así plenamente con los principios de la contratación pública. Con ello se podría salvar que se utilizara esta modalidad específica de contratación pública en relación con este objeto (solo aplicable en principio a entidades de pequeño o mediano tamaño y que no traten datos sensibles o datos a gran escala). Pero esta es una cuestión que excede del presente objeto y requeriría un detenido análisis –que ahora no puede hacerse- desde el punto de vista de la contratación pública, un aspecto que se antoja necesario para enmarcar correctamente la figura del DPD en el sector público a través de figuras externas.

Tal como se ha visto, si el DPD desarrolla su actividad en el marco de un contrato de servicios que esté suscrito con persona física o jurídica ajena a la organización del responsable o encargado del tratamiento, es fundamental que no se incurra en conflicto de intereses, pues –como se verá de inmediato- las cualidades profesionales hay que enmarcarlas no solo en conocimientos y experiencia, sino también "deben incluir, por ejemplo, la integridad y un nivel elevado de ética profesional". Asimismo, en estos casos, como vengo insistiendo, es importante que la empresa de servicios profesionales determine quién es la persona que, en relación con esa organización pública concreta, llevará a cabo las funciones de DPD, para lo cual es relevante incluir en los pliegos este tipo de exigencias.

En efecto, dentro de lo que se denomina la "capacidad para desempeñar sus funciones", cabe poner de manifiesto que tal exigencia debe ponerse necesariamente en relación con la necesidad de cumplimiento del RGPD que debe salvaguardar el DPD. Y, sobre este punto, atendiendo al "papel fundamental en la promoción de la cultura de la protección de datos dentro de la organización" que tiene el DPD, es imprescindible incluir dentro de "las cualidades personales" que debe acreditar la persona, profesional o empresa que desarrolle ese tipo de funciones, "la integridad y un nivel elevado de ética profesional", algo que será más difícil de medir objetivamente en sistemas de provisión de puestos de trabajo o en los procesos de licitación en materia de contratación pública, pero que también pueden existir algunos criterios que den pautas u orientaciones para saber si se cumplen o no tales exigencias (aparte de la hipotética inserción de códigos o prescripciones éticas o de conducta, también en la ejecución): procedimientos sancionadores, formación sobre estas materias, experiencia profesional en el ámbito de la integridad y de la ética pública, proyectos profesionales en los que se ha participado y resultados de los mismos, publicaciones, etc.

En todo caso, no cabe ocultar que los municipios pequeños y medianos, así como otras entidades locales del mismo carácter, pueden tener problemas efectivos para incorporar esta figura a sus plantillas

o incluso para externalizar este tipo de servicios. Por ello, tal como ha defendido Campos Acuña[20], puede ser un instrumento operativo que las propias Diputaciones provinciales puedan crear, en uso de sus competencias de cooperación y asistencia técnica a los municipios, una figura de DPD que pueda prestar servicios a diferentes entidades, ya sea de carácter interno o externo. En todo caso, se deberían cumplir las exigencias antes establecidas de acreditación de competencias profesionales y de estándares éticos (o de no incurrir en conflictos de intereses), individualizando asimismo quién será el DPD que actuará en cada ayuntamiento. La forma más correcta de articular este proceso debería ser mediante convenio entre la respectiva entidad local y la propia Diputación, y en este documento se deberían incorporar todas las exigencias antes expuestas, pues el responsable o encargado de tratamiento es una autoridad o funcionario de la entidad local y el DPD debe ser designado por estos y ayudarles en el ejercicio de sus funciones sirviendo de punto de contacto, por lo que se debería mostrar el consentimiento a que la designación o contratación pública se llevara a cabo por la propia Diputación. Estos convenios, salvo que se configuraran como encomiendas de gestión (aunque caben algunas dudas de que se pueda acudir a esta fórmula, por el cometido funcional del DPD), deberían estar sometidos al régimen jurídico establecido en el capítulo VI del título preliminar de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

Estatuto de* independencia *de la figura del DPD: notas características. La "posición" del DPD en la estructura organizativa.

El artículo 38 RGPD establece una serie de principios y reglas que configuran lo que cabe denominar –en terminología del propio Reglamento y del PLOPD- como la "posición" del delegado de protección de datos en la estructura organizativa. Sin duda se trata de una serie de decisiones normativas que ayudarán a perfilar qué tipo de figura orgánica y qué clase de puesto de trabajo representa el DPD, así como también facilitará el encuadre de esa misma figura cuando se acuda a un proceso de externalización de tales servicios profesionales.

La primera regla del citado artículo 38 RGPD es muy precisa pues atribuye al responsable o encargado del tratamiento la obligación de garantizar que el DPD "participe *de forma adecuada y en tiempo oportuno* en todas las cuestiones relativas a la protección de datos". Por tanto, en este artículo 38.1 RGPD se contienen al menos tres exigencias: a) Que el responsable o encargado del tratamiento *garantice* la participación del delegado en esos procesos; b) Que esa participación se articule *de forma adecuada y en tiempo oportuno*; y c) Que se proyecte, en principio, sobre *todas las cuestiones* relativas a la protección de datos (aunque, como se ha visto, esa vocación de universalidad deberá ser selectiva en función de aquellos tratamientos que impliquen riesgos o afecten a los derechos fundamentales de la persona). En cualquier caso, parece obvio resaltar que su participación debe ser efectiva, y que no puede ser orillada nunca tal actuación, si así lo requiere el propio DPD, en tales procesos de tratamiento de datos.

El Grupo de Trabajo del Artículo 29 aportó en su día algunas claves interpretativas de esa participación del DPD en tales procesos. Así, se subraya que resulta "fundamental que el DPD, o su equipo, *participen desde la etapa más temprana posible* en todas las cuestiones relativas a la protección de datos". Algo que, el propio RGPD, establece en los casos de que se deban realizar "evaluaciones de impacto", pues en tales supuestos el responsable del tratamiento debe recabar necesariamente el asesoramiento del DPD, siempre que este haya sido nombrado (artículo 35.2 RGPD). Y esta intervención temprana del DPD en todo tipo de procesos de tratamiento de datos, debería ser considerada como "un procedimiento estándar en la gobernanza de la organización", recomendándose que el DPD "forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización".

Así, el documento de *Directrices* hace hincapié en que la organización (en este caso la Administración Pública y sus entes dependientes o vinculados) debería garantizar, entre otras cosas, lo siguiente:

[20] C. Campos Acuña, "Los 7 'imprescindibles' en la protección de datos en el ámbito local (RGPD y PLOPD)", *El Consultor de los Ayuntamientos y Juzgados,* 2018.

- Que se convoque al DPD para que participe con regularidad en reuniones de cuadros directivos altos y medios.
- Se recomienda que esté presente cuando se tomen decisiones con implicaciones para la protección de datos, trasladándosele a su debido tiempo (por tanto, con carácter previo) toda la información para que pueda prestar asesoramiento adecuado.
- Asimismo, se deberá tener debidamente en cuenta la opinión del DPD. Y, en caso de desacuerdo, se recomienda, como buena práctica, que se documenten los motivos por los cuales no se sigue el consejo del DPD.
- Y, en fin, en los supuestos de que se haya producido una violación de la seguridad de los datos o de cualquier otro incidente, se debe consultar al DPD "con prontitud"[21].

No cabe duda que todas esas recomendaciones están articuladas principalmente en torno a que el DPD esté vinculado orgánicamente con la organización, pues si fuera un externo en el caso de las Administraciones Pública se podrían plantear algunos problemas en la participación en determinadas reuniones de órganos colegiados o en aquellos ámbitos donde se adopten decisiones estratégicas con implicaciones para la protección de datos. Sin perjuicio de que en determinadas estructuras organizativas u órganos colegiados "el DPD externo" pueda participar como "asesor" en aquellos asuntos que afecten a su ámbito de competencia, no es menos cierto que su encaje en ciertos órganos administrativos (como miembro de pleno derecho) tal vez podrá ser más complejo, salvo que se trate de "reuniones informales" de nivel alto o medio. No es, por tanto, un asunto menor cómo ensamblar en la organización administrativa y en el funcionamiento de determinados órganos colegiados la figura de un DPD "externo".

En línea con lo anterior, sobre todo si se pretende una participación efectiva del DPD en todos estos procesos de tratamiento de datos, resulta imprescindible que la Administración Pública o el órgano (departamento o entidad) a la que se adscriba el DPD *facilite "los recursos necesarios para el desempeño de dichas funciones* y el acceso a los datos personales y a las operaciones de tratamiento (…)" (38.2 RGPD). En suma, esa dotación de recursos debe ser asimismo efectiva si se trata de un DPD interno para el correcto cumplimiento de sus funciones, lo que implica dotarle de medios personales (si fueran necesarios), de recursos materiales y de un espacio físico en el que pueda desempeñar de forma correcta (y con la necesaria autonomía funcional y discreción) las funciones asignadas. Ello implica, según se ha dicho, que el DPD tenga una identificación nominal precisa (también aconsejable en el caso de empresas de servicios profesionales con individualización de sus datos de contacto), correo electrónico y teléfono de contacto, así como ubicación física de la dependencia orgánica en la que preste sus servicios, con los datos postales. Todo ello es importante, en efecto, por la condición de "punto de contacto" que tiene el DPD. La existencia de una dependencia orgánica con medios propios de la Administración (o lugar "de trabajo" o de ·"punto de contacto") del DPD externo, puede plantear problemas efectivos de si no se está produciendo en este caso una cesión ilegal de trabajadores. Parece, por tanto, razonable que el "punto de contacto" en estos casos también sea externo, lo que puede plantear problemas de "accesibilidad", salvo que sus relaciones sean siempre telemáticas.

Asimismo, el artículo 38.2, "in fine", establece la obligación de que el responsable o encargado del tratamiento faciliten al DPD "el mantenimiento de sus conocimientos especializados". Por tanto, será la Administración Pública la que deberá velar porque el DPD (o los DPD que se creen) sean receptores de programas de formación continua que le permitan ejercer sus funciones en un entorno de permanente cambio y transformación, como es el ámbito de las tecnologías y del tratamiento de datos. Esta obligación difícilmente se puede predicar frente a los profesionales o empresas que presten externamente sus servicios a la Administración Pública, pues esa formación debería ser un compromiso que las propias empresas asumieran por sí mismas. No estaría de más reflejar todas estas cuestiones en los propios pliegos de contratación, sobre todo para evitar problemas ulteriores.

[21] *Directrices sobre los delegados de protección de datos*, cit. p. 15.

Cabría plantearse, igualmente, cuáles son las soluciones o canales que puede tener el DPD ante un obstruccionismo del responsable o encargado del tratamiento de datos: ¿podría acudir a la autoridad de control?; ¿qué mecanismos de reacción se prevén? En principio, hay una anomia legal en este punto. Y no parece fácil definir nada al respecto.

En relación con los "recursos" de que debe proveer el responsable o encargado del tratamiento al DPD, el Grupo de Trabajo incluyó en su último documento una serie de observaciones, a las que sumamos un conjunto de reflexiones personales sobre algunos de tales puntos. A saber:

- El DPD debe recibir apoyo activo por parte de la dirección, en este caso por los niveles de máxima responsabilidad de las Administraciones Públicas.
- Se le debe garantizar al DPD (obviamente cuando esa figura tenga carácter interno) el "tiempo suficiente" para que cumpla con sus funciones, algo "particularmente importante cuando se designa un DPD interno a tiempo parcial" (es, tal como se añade, "una práctica recomendable establecer un porcentaje de tiempo para la labor propia del DPD cuando no se lleve a cabo por tiempo completo") o cuando el servicio es prestado externamente por un DPD que lleve la protección de datos de forma complementaria a otras actividades (piénsese en un profesional de la Abogacía). Por tanto, en este último caso (y se podría decir que en todos) sería asimismo importante determinar el tiempo de dedicación de tales servicios profesionales para cada Administración Pública. A tal efecto, se sugiere asimismo la confección de un plan de trabajo donde se determine el tiempo necesario para realizar cada labor y el nivel de prioridad adecuado.
- En el caso del DPD interno, se le debe dotar de "apoyo adecuado en cuanto a recursos financieros, infraestructuras (locales, instalaciones, equipos) y personal, según se requiera". Por tanto, el DPD puede tener adscrito personal (siempre que sea necesario para el desarrollo de sus funciones; una adscripción que podría ser plena, en el caso de que se creara una estructura orgánica específica, o parcial, cuando desempeñe funciones de apoyo instrumental solo durante parte de la jornada), pero debe disponer de una ubicación física específica que, dada su posición institucional, debería comportar un local definido (despacho propio), así como las infraestructuras y recursos necesarios para el ejercicio de sus funciones.
- Se recomienda igualmente que se curse una comunicación oficial de la designación del DPD dirigida a todo el personal, con la finalidad de que sea conocida su existencia y función dentro de cada organización. En el caso de las Administraciones Públicas podría vehicularse tal información a través de los canales internos, ya sean telemáticos o de otra naturaleza, así como difundirlo en el Portal de Transparencia o, en su caso, en la página Web institucional.
- Igualmente, se debe fomentar la formación continua de este personal que asuma las funciones de DPD, con la finalidad de que se mantenga al día de la evolución de todas aquellas cuestiones que afecten a la protección de datos (aunque no solo; también al procedimiento, seguridad de la información, Derecho y tecnologías de la información, etc.). El Grupo de Trabajo utiliza la expresión "animar", pero si se trata de personal interno la formación del DPD no debe solo configurarse como un derecho, sino especialmente como un deber (artículos 14 g) y 54.8 TREBEP), al menos en los casos en que esa figura esté cubierta por un empleado público.
- Hay que partir del hecho de que cuanto más complejas o sensibles sean las operaciones de tratamiento, más recursos se deberán destinar para el DPD. Bajo esas premisas, cabe perfectamente –como se viene indicando- que el DPD se configure como una estructura orgánica de la Administración (un departamento, servicio o unidad organizativa específica), con una persona responsable (DPD) y personal a su servicio (técnicos y personal instrumental). Tal como indica el Grupo de Trabajo, todo dependerá del "tamaño y estructura de la organización", pues también cabría la designación de un DPD únicamente, incluso a tiempo parcial (si bien, aun en estos casos, parece obvio que requerirá de apoyo instrumental). Si quien desempeña el servicio es una empresa externa, se recomienda asimismo que, sin perjuicio de que disponga de personal técnico o administrativo que trabaje en ese proyecto, se determine una persona de contacto, puesto que el equipo trabajará bajo su responsabilidad al servicio del adjudicatario del servicio y esa determinación de la persona servirá, asimismo, para canalizar todas las cuestiones y rendir cuentas, en su caso, por el trabajo realizado o para actuar con "punto de contacto" con los interesados y con la autoridad de control (AEPC, ACPD o AVPD y, cuando así se determine, el CTPD de Andalucía).

Una de las notas distintivas y probablemente de mayor importancia para definir su posición estructural en la organización y el papel institucional que la figura del DPD tiene, es *el estatuto de independencia* que se predica del ejercicio de tales funciones por el RGPD. Se trata, en efecto, de una suerte de nota determinante o existencial de su estatuto jurídico, pues el Reglamento persigue con claridad que se *salvaguarde la posición de independencia del DPD frente al responsable o encargado del tratamiento*.

En efecto, el artículo 38.3 RGPD concreta esa garantía de independencia en los siguientes términos: "El responsable y el encargado del tratamiento *garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones*". Se debe preservar, así, su autonomía funcional, por lo que debe quedar extramuros de la línea jerárquica de la organización, transformándose en una suerte de "autoridad independiente individual (o unipersonal)", o si se prefiere un nivel orgánico o estructura que goza de un estatuto singular de "independencia" por exigencia del propio RGPD. Pero la singularidad (e incluso paradoja) de ese puesto o unidad orgánica de carácter "independiente" es que se inserta (lo cual es tremendamente peculiar) en el seno de una estructura administrativa de naturaleza jerárquica (a la que "asesora", "aconseja" o "alerta"; pero no debe formar parte de la estructura decisional, pues está exento de responsabilidad). Dicho de otro modo, la inserción del DPD en las Administraciones Públicas tiene unas connotaciones de particularismo notables, que contrastan con la configuración tradicional de los puestos de trabajo o de las unidades administrativas en una línea jerárquica en la que actúan siguiendo directrices y criterios de los superiores. En este caso, la autonomía funcional del órgano o de la figura es evidente, pues no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones.

A juicio del Grupo de Trabajo del Artículo 29, ese artículo 38.3 RGPD incorpora una serie de garantías básicas "que contribuyen a asegurar que los DPD puedan realizar sus tareas con el suficiente grado de autonomía dentro de su organización". Como indica el Considerando 97 del RGPD, se pretende preservar que el DPD pueda "desempeñar sus funciones y cometidos de manera *independiente*". La nota de autonomía funcional debiera derivar, por tanto, en un estatuto de ejercicio *independiente* (fuera de la línea jerárquica, habría que precisar) de sus cometidos funcionales. Por ello tiene pleno sentido que no se deba instruir a un DPD en relación a "cómo abordar un asunto, por ejemplo qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de control" sobre un determinado tema. Tampoco cabe admitir ninguna instrucción dirigida a adoptar "una determinada postura con respecto a un asunto relacionado con la ley de protección de datos, por ejemplo, (sobre) una interpretación concreta de la ley". Estas reglas de conducta que deben respetar los responsables y encargados de tratamiento se deben entender plenamente aplicables a los supuestos en que se haya producido una contratación del servicio, aunque no cabe ocultar que su aplicación efectiva puede mostrar algunas debilidades obvias en este caso. Aunque sería oportuno también resaltar todas estas cuestiones en el oportuno pliego de contratación.

Si nos detenemos en el caso de internalización del DPD, no cabe duda que ese perfil de autonomía funcional e, incluso, de independencia en el ejercicio de su papel institucional, casa mal con unas organizaciones públicas y un comportamiento habitual de sus funcionarios que está más bien dirigido a respetar las órdenes y criterios de los superiores jerárquicos, por lo que cabe presumir que el encaje de esta figura del DPD, con el perfil indicado, en las organizaciones públicas no será sencillo. Requiere, tal como vengo insistiendo, un cambio de mentalidad y de comportamiento, así como una nueva cultura organizativa. Algo que exige tiempo, pues no será una transición sencilla.

Por un lado, habrá que explicar muy bien a los responsables políticos y directivos, así como a los responsables funcionariales, las limitaciones que presenta el RGPD por lo que afecta a sus facultades o poderes de dirección y mando en relación con este tipo de puestos de trabajo o unidades orgánicas. Por otro, habrá que mentalizar igualmente a los funcionarios o empleados públicos que asuman tales cometidos para que realmente defiendan o preserven esa posición de autonomía funcional y de independencia frente a determinadas intromisiones o interferencias de la línea jerárquica en las actuaciones del DPD, que dado lo sensible del objeto no cabe extrañar de que se puedan dar, sobre todo teniendo en cuenta las responsabilidades que se pueden derivar por parte del responsable o encargado en caso de incurrir en algunas de las infracciones que se prevén en el RGPD y, especialmente, en la

legislación del Estado miembro (PLOPD). En todos estos casos, el papel de las autoridades de control se torna importante, para llevar a cabo procesos formativos comunes, preparar circulares de funcionamiento y promover esa necesaria transformación de la cultura organizativa y funcionarial que implica (auto) dotar a tales figuras de los delegados de protección de datos de un estatuto efectivo de independencia funcional que evite cualquier tipo de interferencias y realce su posición de garante de los interesados en todos los procesos de tratamiento de datos, más aún en lo que tengan carácter intensivo o masivo.

El artículo 38.2 "in fine" también exige que el DPD rinda cuentas "directamente al más alto nivel jerárquico del responsable o encargado". Este peculiar rasgo de su estatuto implica (o debería implicar) una especial posición en la estructura orgánica, pero cuando menos sitúa la rendición de cuentas de tales delegados en las Administraciones Públicas en el mayor nivel orgánico ejecutivo de estas, sea Alcaldes en el caso municipal o Junta de Gobierno Local. Los problemas pueden surgir, en efecto, en relación a cómo articular la rendición de cuentas en aquellos casos en que el servicio sea prestado externamente, aspecto sobre el cual algo deberán decir asimismo los pliegos de la contratación pública que en su día se promueva.

Pero ese estatuto de "autonomía funcional interna" se ve aún más reforzado cuando el propio RGPD prevé expresamente que el DPD "no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones" (artículo 38.3 RGPD). Por tanto, el RGPD blinda al titular del cargo frente a ceses discrecionales (al igual que en el modelo de autoridades independientes) y ante la aplicación del régimen sancionador por el ejercicio de sus funciones.

Así se regula este blindaje: "No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones". Tanto esta nota de blindaje frente a la destitución discrecional como la relativa a la rendición de cuentas al máximo nivel son muy importantes, en efecto, para definir –como se hará inmediatamente- la posición estructural en la organización del DPD. El PLOPD lleva a cabo alguna precisión sobre este tema en su artículo 36.2, y concreto expone: "Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos *no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio*". En qué casos se puede sancionar y por quién, son dos preguntas que también cabe resolver y que la normativa en trámite de elaboración tampoco resuelve.

Esa garantía de autonomía funcional a través del blindaje frente a destituciones discrecionales también se aplicaría al ámbito de la contratación pública, sobre todo en lo que afecta a la determinación de las causas de resolución del contrato, aunque en este caso la determinación temporal de la prestación debería ser el parámetro inicial que tendría que respetar el responsable o encargado del tratamiento, siempre que se cumplan debidamente las obligaciones derivadas del contrato.

La peculiar posición del DPD, tal como vengo reiterando, se advierte asimismo por su configuración como punto de contacto con los interesados, al fin y a la postre los titulares de los datos y del derecho fundamental a su protección. El artículo 38.4 RPD establece al efecto lo siguiente: "Los interesados podrán ponerse en contacto con el DPD por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento". Este papel de "mediador", "intermediario" y, a su vez, de "consultor" o "asesor" de los interesados es clave en el diseño de la figura, pero también lo es que se convierte en el canal (o, al menos, en uno de los canales) a través del cual los interesados pueden activar el ejercicio de sus derechos. Es, por tanto, el DP un "punto de contacto" nuclear en esa *relación triangular entre interesados-administración pública-autoridad de control.* Su posición es claramente intermedia y conviene preservar razonablemente ese estatuto.

En efecto, su dimensión "exógena" se advierte no solo en su papel de "interlocución" con la autoridad de control, sino además porque, tal como se ha visto, los interesados pueden ponerse en contacto con el DPD en relación con el tratamiento de sus datos personales y el ejercicio de sus derechos. Cabe así preguntarse si no se configura como una suerte de Ombudsman interno en materia de protección de

datos. Esta función se ve acrecentada por lo establecido en el artículo 37 del PLOPD, que transforma ese órgano en una instancia preliminar de reclamaciones en materia de protección de datos antes de que se acuda a la autoridad de control, con el fin, no escondido, de servir de filtro a esta. Una actuación potestativa, pero menos: pues la autoridad de control tiene la facultad de enviarle cualquier tipo de reclamación que se haga *per saltum* (artículo 37.2 PLOPD), para su previa valoración. Dicho de otro modo, si el interesado no ha solicitado el criterio del DPD mediante una reclamación previa (¿no hay funciones de autoridad en este caso?) y opta por dirigirse directamente a la autoridad de control, esta (según la redacción actual del PLOPD) "podría" reenviarle dicha reclamación para que sea valorada o informada por el DPD para que este responda en el plazo de un mes. Esta es una función "nueva", tal como diré de inmediato, que se añade a las previstas nominalmente en el RGPD. Y puede tener su importancia para definir correctamente la naturaleza de la citada figura del DPD.

Y, en fin, el DPD está obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones (38.5 RGPD). Algo especialmente importante tanto cuando las funciones sean desempeñadas internamente como cuando se lleven a cabo de forma externa. En este último caso parece lógico que tales exigencias se incorporen a los propios pliegos, aunque no es menos cierto que esa confidencialidad y secreto tendrá siempre menos garantías cuando el servicio se preste externamente.

Este estatuto jurídico de la figura del DPD, así como sus funciones que seguidamente se analizan, le aleja sustancialmente de otras figuras existentes en la actualidad en el campo de la protección de datos, . Realmente, la configuración del DPD desborda de forma notoria –como se viene insistiendo- el marco anterior, pues en realidad del análisis de las funciones del DPD se podrá concluir con claridad que "esta nueva figura supone reforzar la cultura de *compliance* en materia de protección de datos", tal como ha reconocido por la doctrina[22].

Funciones del delegado de protección de datos según el RGPD y el PLOPD

El RGPD le asigna al DPD unas funciones mínimas (artículo 39) que se proyectan sobre una serie de ámbitos. Es importante constatar que tales funciones tienen, efectivamente, el carácter de *mínimas*, por lo que nada impide que se añadan otras (tal como hace, por ejemplo, el PLOPD), siempre que no alteren la naturaleza y rasgos esenciales ya examinados de la figura.

Una nota singular que enmarca el ejercicio de tales funciones es la recogida en el artículo 39.2 RGPD, donde se prevé la siguiente regla: "El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance y los fines del tratamiento". Sin duda se trata de una previsión importante, pues representa una regla de actuación a la hora de delimitar la intervención del DPD, que directamente se enmarca en todos aquellos tratamientos que impliquen o a los que estén asociados riesgos para la intimidad de las personas. Por tanto, una primera pauta en la actuación del DPD es precisamente esta: identificar en qué operaciones de tratamiento hay riesgos para la protección de datos. A tal fin, solo se dan cuatro criterios genéricos: el DPD ha de tener siempre en cuenta la *naturaleza, alcance, contexto y fines* del tratamiento.

En todo caso el RGPD enuncia una serie de funciones que, como mínimo, deberá ejercer el DPD. A saber:

a) *Informar y asesorar al responsable o al encargado del tratamiento y a los empleados* que se ocupen del tratamiento de las obligaciones, que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión Europea o de los Estados miembros. De ahí que, tal como se decía anteriormente, el DPD deba tener un exhaustivo y detallado conocimiento del RGPD y de

[22] Por todos, A. Ortega Giménez y J.J. Gonzalo Domenech, "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", cit.

la normativa aplicable en materia de protección de datos, en este caso para desarrollar esas funciones informativas y asesoras de carácter interno (es decir, dirigida "ad intra") que este precepto le encomienda.

b) *Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, o de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales,* incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes. No se trata, por tanto, de una función ejecutiva, sino estrictamente de "supervisión del cumplimiento", tanto en lo que concierne a la política que sobre esta materia lleve a cabo el responsable o encargado del tratamiento, como en las acciones que impulse (u omita) en materia de concienciación y formación del personal, así como de las auditorías. De esa función de supervisión del cumplimiento se debiera derivar en buena lógica la posibilidad de emitir algún tipo de recomendaciones o advertencias que, en caso de no seguirse, lo normal sería que se trasladaran a la autoridad de control. Pero nada nos dice el RGPD sobre este punto ni tampoco el PLOPD.

c) *Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.* Probablemente se trate de una de las funciones esenciales del DPD, puesto que la clave de bóveda de este nuevo paradigma por el que apuesta el RGPD es, precisamente, la evaluación de riesgos del tratamiento. Y el papel del Delegado de Protección de Datos es, en efecto, de "asesoramiento" (artículo 35.2 RGPD), pero también una vez más de "supervisión", según se deduce de este artículo 39.1.c) RGPD.

d) *Cooperar con la autoridad de control.*

e) Y *actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.* Estas dos funciones se pueden tratar conjuntamente, por sus evidentes conexiones. También se trata de unas funciones nucleares dentro de ese papel triangular de la figura del DPD, pues en este caso el DPD se convierte en "punto de contacto" con la autoridad de control (AEPD, ACPD o AVPD). Tal como se ha visto, esta función del DPD le pone en contacto con las funciones de la autoridad de control, por ejemplo en todo lo que tiene que ver con evaluación de riesgos, dado que cualquier consulta previa que lleve a cabo el responsable del tratamiento deberá incluir asimismo los datos de contacto del DPD (artículo 36.3, d) RGPD), que cabe presumir que ya están en poder de la propia autoridad de control (puesto que el artículo 34.4 de la LOPD obliga a que las autoridades de control mantengan "una lista actualizada de delgados de protección de datos que será accesible por medios electrónicos"). Asimismo, tal como se dirá de inmediato, esa función de cooperación del DPD se incrementa en el caso de lo previsto en el artículo 37 del PLOPD. Pero, además, de tales funciones y sobre todo de la regulación establecida en el artículo 36.1 PLOPD (que establece la previsión de que "el DPD actuará como *interlocutor* del responsable o encargado del tratamiento ante" la autoridad de control competente en razón de la materia), se deriva asimismo la facultad que tiene el DPD de ser el "interlocutor privilegiado" de la propia autoridad de control en la institución o entidad respectiva, pues esas funciones de cooperación y consulta configuran una red de relaciones institucionales que, en cierta medida y dado el singular estatuto que tiene la figura, en algunos casos (o en el ejercicio de determinadas funciones) le aproximan más a la autoridad de control con la que lleva a cabo un papel de "puente" que a la propia Administración Pública en la cual se inserta.

El PLOPD no tiene, sin embargo, un artículo específico relativo a cuáles son las funciones del DPD, por lo que cabe deducir las mismas de lo establecido en el artículo 39 RGPD. Pero no es menos cierto que en algunos de estos artículos del PLOPD, se derivan una serie de obligaciones adicionales o funciones complementarias que cabe resaltar debidamente.

Por un lado, el DPD en el ejercicio de sus funciones, algo que cabe entender también implícito del listado de estas recogido en el artículo 39 RGPD, "tendrá acceso a los datos personales y procesos de tratamiento", sin que quepa oponer por parte del "responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto" (artículo 36.3 PLOPD). Esta facultad expresamente recogida en el PLOPD refuerza las funciones de "supervisión" antes enunciadas.

Por otra parte, esa función de supervisión se refuerza notablemente a través de lo establecido en el artículo 36.4 PLOPD, cuando específicamente se afirma lo siguiente: "Cuando el delegado de protección

de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo comunicará inmediatamente a los órganos de administración y de dirección del responsable o encargado del tratamiento". En esta atribución del DPD se advierte una nota que refuerza más aún el estatuto jurídico de la figura y enlaza con la "rendición de cuentas" al máximo nivel, así como con la posibilidad de que la supervisión del DPD derive en un control directo de los tratamientos que lleven a cabo el responsable o encargado. Probablemente, en este caso hubiera sido más apropiado establecer una suerte de requerimiento previo para que se llevara a cabo la corrección oportuna y, en caso de no hacerse, trasladar la comunicación pertinente al órgano de dirección del responsable o encargado.

Pero, las novedades más relevantes por lo que al ámbito funcional del DPD se contienen en el artículo 37 del PLOPD. Y, aunque ya se ha hecho mención a algunas cuestiones allí tratadas, puede ser oportuno reproducirlo en su integridad:

Artículo 37.- Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.
"1.- Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.
En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.
2.- Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, sin haber hecho uso de la posibilidad a la que se refiere el apartado anterior, aquéllas podrán remitir la reclamación al delegado de protección de datos a fin de que éste responda en el plazo de un mes".
Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo".

En cualquier caso, se trata de una regulación recogida en un proyecto de ley, por lo que puede sufrir alteraciones sustanciales. No obstante, conviene detenerse en una serie de puntos que afectan a las funciones del DPD, pero asimismo que tienen impactos sobre el estatuto de la figura, el perfil de competencias y la hipotética posibilidad de externalizar su ejercicio. Veamos rápidamente estos puntos:

En relación con las funciones, es obvio que a través de esa atribución de intervenir en las reclamaciones que, con carácter previo y potestativo, puedan presentar los afectados por un tratamiento de datos, se le confiere al DPD una nueva función no expresamente prevista en el artículo 39 RGPD. Se trata de una función que enlaza directamente con la de "cooperar con la autoridad competente" (artículo 39.1.d) RGPD), dotándola así de mayor contenido. Pero cabe plantearse de inmediato si esa función, en lo que respecta a las Administraciones Públicas, no implica realmente una función de autoridad, pues no en vano se trata de una reclamación previa en vía administrativa anterior a la formalización de la reclamación ante la autoridad de control y, obviamente, debería finalizar con una resolución del propio DPD, aunque en ningún momento (dado que la regulación se aplica también al sector privado) se utilicen tales términos. En este caso, da la impresión de que si se interpusiera por parte de un afectado o afectados una reclamación previa ante el DPD, esta daría lugar a un procedimiento administrativo que debería ultimarse por medio de una propuesta de resolución o de una resolución, en su caso. Y ello implicaría ejercicio de funciones de autoridad, con lo cual ni la figura podría tener régimen laboral ni tampoco podría ser objeto de una contratación de servicios, salvo que se disociara entre quien realiza las funciones instrumentales de apoyo al responsable y encargado del tratamiento (un DPD de soporte) y la existencia de un DPD "formal" (un funcionario público) que llevara a cabo, en su caso, el ejercicio de las funciones de autoridad. Pues la otra solución es que tal figura del DPD externo no resuelva en el sentido formal del término, sino que simplemente emita opinión a través de un informe o un dictamen y pueda sugerir al responsable o encargado del tratamiento (o, en su defecto, al nivel jerárquico con el que rinda

cuentas) la rectificación o subsanación de alguna irregularidad detectada en el tratamiento de datos de carácter personal.

Si se opta por la primera solución (reclamación administrativa que finaliza en una resolución) la figura del DPD en el ámbito público debería ser funcionario, haciendo prácticamente inviable la contratación externa. Sí, por el contrario, la solución es la segunda (que se asemejaría al tratamiento de la reclamación en el sector privado) nada impediría que esa figura pudiera tener régimen laboral o, en su caso, ser objeto de un procedimiento de contratación pública. El problema no es baladí y puede tener unas implicaciones muy importantes en la traslación de esa figura a la Administración Pública, pues el estatuto de régimen jurídico del DPD puede sufrir en uno u otro caso alteraciones radicales.

También esa regulación recogida en el PLOPD impacta con fuerza sobre el perfil de competencias requerido para desempeñar llamadas funciones de DPD. En efecto, al atribuirle al DPD la facultad de que atienda las reclamaciones que planteen los afectados con carácter previo a acudir a la autoridad de control, no cabe ocultar que el legislador orgánico español pretende dotar a esta figura de un carácter fuertemente jurídico, tanto si se internaliza como si se acude a una contratación de servicios, pues "resuelva", "informe" o "dictamine", parece obvio que deberá hacerlo en Derecho y, por tanto, requerirá una sólida formación jurídica, así como algún tipo de formalización documental. Así, mientras que el RGPD permitía que las funciones de DPD las pudiera desarrollar cualquier perfil profesional, siempre que acreditara las competencias exigidas y antes analizadas, aunque requería conocimientos del Derecho, el PLOPD se inclina indirectamente por dibujar un perfil profesional de DPD de carácter netamente jurídico.

En cualquier caso, sea cual fuere la interpretación que se le dé a esa regulación del PLOPD, lo cierto es que cambia cualitativamente el estatuto y naturaleza del DPD, cerrando (no sabría decir si acertadamente o no) la regulación abierta que establecía el RGPD. No cabe plantear, sin embargo, objeción alguna en términos de adecuación de la futura LOPD al RGPD. La opción de la futura LOPD cabe perfectamente dentro de las funciones de "cooperación" del DPD con la autoridad de control. Tal vez se pudieran plantear algunas dudas en torno a la oportunidad de esa medida normativa, que parece tener un sesgo claro, y que no es otro que reforzar la dimensión preventiva del DPD en su aplicación jurídica, pero "descargando" o "facilitando" la actuación de la autoridad de control en las reclamaciones que pudieran plantearse.

¿Qué nivel orgánico debe tener en la estructura el Delegado de Protección de Datos?

No cabe duda que el estatuto jurídico y las funciones establecidas en el RGPG y en el PLOPD son aspectos que condicionan o enmarcan una de las decisiones más relevantes a la hora de insertar la figura del DPD en la estructura organizativa. La primera decisión crítica ya ha sido expuesta anteriormente: el dilema entre internalizar o externalizar la figura. Una vez resuelto este problema, el siguiente es dónde y con qué carácter lo insertamos en la estructura de la Administración Pública; esto es, con qué nivel orgánico y en qué posición quedaría el delegado de protección de datos en relación con el resto de órganos y unidades administrativas, especialmente en lo que tiene que ver con el responsable y encargado de tratamiento de los datos personales (aunque de este último punto ya se han visto algunas cuestiones).

Pero hay otra decisión previa a la expuesta. Y tiene que ver sobre si se crea una sola figura o se multiplica esta en función de áreas, departamentos o entidades. El RGPD parece dejar abiertas las dos posibilidades, pero solo en apariencia. En su artículo 37.3 se expone lo siguiente: "Cuando el responsable o encargado del tratamiento sea una autoridad u organismo, *se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño*". No cabe duda que una entidad local de pequeño o mediano tamaño podría optar por la creación de una figura singular, pero un nivel de gobierno de cierta complejidad (por su estructura de áreas, departamental o de entidades vinculadas, dependientes o adscritas) parece razonable (según el espíritu del RGPD) que se incline por la implantación de delegados de protección de datos en cada ámbito previamente definido (algunas áreas o departamentos especialmente sensibles a

los tratamientos de datos deberán disponer probablemente de varios delegados). El DPD es un nivel orgánico *ad hoc*, pero también puede configurarse como un puesto de trabajo singular.

Cabe asimismo plantearse la duda de si el DPD puede configurarse como un escalón directivo o lo que se conoce en la terminología de la Administración Pública como "alto cargo"; es decir, como titular de un órgano directivo de la Administración. Mi tesis es que, al ser estos cargos públicos de libre nombramiento o remoción y no existir procedimiento efectivo alguno de acreditación de competencias profesionales, la creación de una figura de DPD como alto cargo no cumpliría con las exigencias del artículo 38.2 RGPD y vulneraría además el estatuto jurídico de independencia o autonomía funcional que se prevé en ese mismo artículo 38.3 RGPD y en el Considerando 97 de ese mismo texto normativo. Además, tampoco se cumpliría con la exigencia de que su posición estructural no diera lugar a posibles conflictos de intereses, evidentes o potenciales. Únicamente, la previsión de una figura de cargo directivo con perfil profesional y sistema de acreditación de competencias, así como previendo la imposibilidad de materializar el cese discrecional, podría atenuar esas resistencias expuestas. Pero ello exigiría normar o, al menos, establecer algún tipo de acuerdo de gobierno o plenario que regulara ese procedimiento específico de provisión de tan singular nivel orgánico.

Una vez descartada, con los matices expuestos, la figura del alto cargo como cauce para la designación del DPD, cabe plantear cómo insertar en la estructura el nivel orgánico o puesto de trabajo de DPD.

Y la primera respuesta al problema vendría de la mano de vincular la unidad orgánica o puesto de trabajo, al menos en el mundo local, a la estructura de Alcaldía o Presidencia, salvo que existieran varios delegados de protección de datos en diferentes departamentos o áreas. Si hay varios DPD, lo razonable es que se articulara un sistema de coordinación entre todas esas figuras, que debería ser implantado desde Alcaldía o Presidencia por medio de una figura de DPD coordinador. Esa ubicación en la estructura le permitiría llevar a cabo de forma efectiva las funciones de supervisión del responsable o encargado del tratamiento y de cooperación con la autoridad de control.

La segunda respuesta tendría como objetivo encuadrar dentro de las unidades organizativas de la Administración la inserción de tal figura. Descartado el recurso a la figura del "alto cargo" como paraguas del DPD y atendiendo principalmente al ejercicio directo o indirecto de potestades públicas que conlleva el ejercicio de algunas de tales funciones, lo más razonable que es ese puesto de trabajo estuviera cubierto por personal funcionario de carrera del Grupo de Clasificación A1 y con un rango orgánico que se situara entre una Subdirección o, en su caso, una Jefatura de Servicio.

La figura del DPD se caracteriza, tal como se ha visto, por su peculiar estatuto, cuya nota dominante es la independencia funcional. Por tanto, consecuencia de todo lo expuesto anteriormente, es que esa unidad orgánica o ese puesto de trabajo no puede estar incorporado en la línea jerárquica de ninguna estructura: debe crearse una estructura organizativa *ad hoc*, singularizada por su no dependencia orgánica ni funcional, pero adscrita desde el punto de vista presupuestario a un departamento o área de actuación. La AEPD considera que la DPD debe adscribirse a órganos o unidades de naturaleza "horizontal", pero eso no es lo determinante (cuestión formal), sino que el aspecto crucial es que el diseño organizativo por el que se adopte salvaguarde plenamente la independencia en su funcionamiento (cuestión material).

En cualquier caso, el DPD no es una pieza aislada del modelo organizativo, sino que se debe incardinar en el modelo de seguridad informática y de tratamiento de datos de cada entidad pública y formar parte de los órganos que se creen con esa finalidad (con las singularidades que presenta; esto es, como "asesor", pero no como miembro de pleno derecho). Su inserción en el sistema de seguridad se ha hecho, por ejemplo, la Orden JUS/1293/2107, de 14 de diciembre, sobre política de seguridad de la información en el ámbito de la Administración electrónica (BOE 28 diciembre 2017), o se está trabajando en esa línea en el Ayuntamiento de Sant Feliú de Llobregat, articulando el ENS con la protección de datos en todo lo que afecta a análisis de riesgos, incorporando esa figura a la Comisión de Seguridad de la citada entidad. Cabe no obstante tener en cuenta que el RGPD supone una transformación radical del

modo de tratar los datos, que ahora no puedo abordar. Pero, por ejemplo, esa concepción de responsabilidad activa obliga a llevar internamente un Registro de actividades de tratamiento que debe estar siempre a disposición de la autoridad de control y suprime, por tanto, la obligación de comunicar a la AEPD todos los ficheros, dejando en manos de la Administración Pública las medidas necesarias para preservar los datos y el uso que se haga de los mismos. Por tanto, y de todo ello se deriva la posición central del DPD en este modelo, es la propia Administración Pública la que tiene que determinar las medidas concretas de seguridad en cada caso y, por tanto, cabe afirmar que con el nuevo RGPD se exime de aplicar la clasificación de niveles de seguridad (alto/medio/bajo) que se requiere en la normativa reglamentaria (en concreto Real Decreto 1720/2007), que también habrá de adaptarse.

Tal como se ha dicho, lo habitual es que en un determinado ámbito de actuación (departamentos, áreas ejecutivas o entidades del sector público, salvo que estas se agrupen) haya un DPD para cada una de ellas, pero la complejidad de determinados departamentos puede aconsejar que haya varios delegados según esferas de actuación (pensemos en ministerios o departamentos tales como Interior, Educación, Sanidad, etc.). Bien es cierto que esa es una alternativa, pues nada impediría la existencia de un solo DPD que volcara su radio de acción sobre toda la organización. El artículo 37.3 RGPD prevé esa posibilidad de nombramiento de un único delegado, pero en estos casos, salvo que la organización sea de pequeño tamaño, necesitará estar dotado de personal e, incluso, como también se ha indicado, de "subdelegados" o personal técnico que dependiera orgánica o funcionalmente del DPD. También cabe, según se ha visto, que se designe un DPD a tiempo parcial, con las garantías antes indicadas.

Dado el perfil de exigencias funcionales que se le atribuyen al DPD, así como las relativas a conocimiento y experiencia que debe acreditar para su nombramiento, este tipo de puestos de trabajo se deberán proveer entre funcionarios públicos del subgrupo de clasificación A1 (dado que ejercerán funciones de autoridad o potestades públicas) que acrediten tales competencias en procesos de provisión de puestos de trabajo abiertos. El RGPD deja claro que deben ser "puestos de plantilla" y "empleados", algo en lo que también insiste la Nota de la AEPD que habla expresamente de "empleados públicos", lo que parece cerrar por completo la puerta –según se ha defendido en este mismo trabajo- a que se cree un nivel orgánico de "alto cargo", dado que se trata de puestos de trabajo de estructura y no aleatorios o cambiantes en función de políticas coyunturales.

El DPD tiene, según se viene insistiendo en estas páginas, una *dimensión trifásica de sus funciones*, que se concreta en los siguientes elementos: (a) como punto de contacto con la autoridad de control, con la que debe cooperar y servir de enlace; (b) como soporte y asesoramiento a la Administración pública en estos temas (especialmente al responsable y encargado del tratamiento, pero también a los empleados públicos que participen en esos procesos), con funciones asimismo de supervisor; y (c) como instancia de resolución con carácter previo reclamaciones de los interesados sobre protección de datos (artículo 37.2 PLOPD) y con una dimensión de "garante" o "protector" de los datos personales de los interesados, a los que puede también asesorar e informar. Su posición topográfica desde un punto funcional se sitúa en el centro de ese triangulo y conectado directamente con los tres vértices.

Como también se ha examinado, este puesto de trabajo tiene que configurarse como una suerte de "autoridad unipersonal independiente" que actúa en el seno de las estructuras administrativas, pero con una configuración dual (interna/externa) y de interlocución, lo que obliga a diseñar un modelo organizativo distinto y distante al tradicional. No encaja en las pautas ordinarias de la creación de puestos de trabajo en la función pública. Aquí las Administraciones públicas tienen un importante reto y sería bueno que lo afrontaran mediante la instauración de un modelo organizativo del DPD que sea singular, lo que tal vez requiera una regulación normativa de corte reglamentario (un reglamento organizativo) o, cuando menos, un acuerdo del órgano plenario o ejecutivo (resolución de alcaldía) en la que se determine cuál es el encuadre organizativo de la figura, se delimiten sus funciones y se deje claro el estatuto jurídico del DPD, así como se establezca un sistema de provisión específico atendiendo a la naturaleza singular de esta nueva pieza orgánica.

Es cierto que el RGPD admite que el DPD "pueda desempeñar otras funciones y cometidos", por lo que cabría configurar una suerte de puestos de trabajo o estructuras funcionales mixtas, pero tal como se ha defendido anteriormente no es muy recomendable. No solo por los hipotéticos conflictos de intereses que se puedan producir, sino también por la esquizofrenia en el desarrollo de las tareas que ello puede conllevar. Tal vez esta figura del DPD con dedicación parcial pueda ser una opción a barajar en las estructuras de gobiernos locales de pequeño o mediano tamaño o, en su defecto, en áreas de actuación pública con riesgos limitados en esta materia, así como tal vez en una primera fase de implantación de la figura. En estos casos y como ya se ha dicho, según las *Directrices* citadas, debe reservarse un porcentaje de tiempo para las tareas de DPD.

La denominación del órgano "*ad hoc*" (y del puesto de trabajo) debería ser Delegado/a de Protección de Datos. Debe dotársele de un nivel orgánico y estatuto retributivo, al menos, similar al de una Subdirección General o Jefatura de Servicio, donde aquella no exista. Incorporarlo como "alto cargo" falsearía la finalidad y espíritu del RGPD, pues el nombramiento sería discrecional (no así el cese) y no se podrían acreditar las exigencias profesionales y de experiencia que el perfil del puesto requiere.

Final: Algunos aspectos de política de recursos humanos ¿Cómo cubrir estos singulares puestos de trabajo? Los nuevos retos.

Sin duda, los aspectos relacionados con el encuadre de esta figura en la política de recursos humanos están estrechamente pendientes de cuál sea finalmente el diseño organizativo por el que se incline cada Administración Pública para la inserción definitiva de la figura del DPD. Por tanto, en las líneas que siguen se omitirá cualquier referencia a la contratación externa del DPD, algo que ya se ha tratado circunstancialmente en páginas anteriores (aunque, cabe insistir, que este tema requiere un análisis monográfico). El foco de atención lo pondré, por tanto, en una internalización de la figura en la organización que conlleva en consecuencia la creación de un nuevo puesto de trabajo o la inserción de tales funciones en otro previamente existente, así como la provisión de ese puesto.

Descarto aquí, en principio, la creación de un puesto de trabajo específico (una plaza) y su cobertura externa mediante un procedimiento selectivo de oposición o concurso-oposición, aunque cabría potencialmente la posibilidad de llevar a cabo tal sistema. Pero la necesidad de incorporar la plaza en la Oferta de Empleo Público, previa creación de la misma y su inserción en la relación de puestos de trabajo y en la plantilla, así como la realización de la oportuna convocatoria de la prueba selectiva y la ejecución de la misma, conllevaría que este proceso se prolongara durante varios meses (e inclusive algún tiempo más) dejando a la Administración Pública sin dotar ese puesto de trabajo necesario a partir del 25 de mayo de 2018. Por razones temporales no parece operativa esta vía de cobertura, aunque si las Administraciones Públicas detectan que no disponen de personal suficientemente cualificado para esas funciones también podrían valorar una cobertura temporal o transitoria y poner en marcha en su día la máquina de realización de tales pruebas selectivas. Para realizar ese proceso con relativa rapidez hubiese sido operativo que la LOPD permitiera que el acceso a esas plazas se pudiera producir excepcionalmente por concurso, pero nada al respecto señala.

Tampoco parece nada operativo proceder a crear la plaza y dotarla a través de una figura de personal funcionario interino. Podría ser una solución, siempre que esa creación de la plaza no suponga incremento de gasto público en el capítulo de personal y se haya amortizado previamente alguna otra (esta operación es perfectamente factible, tal como reconoció la STC 88/2016). Pero el recurso a la figura del funcionario interino debilitaría en exceso el estatuto jurídico del DPD, puesto que quedaría siempre pendiente de la consolidación o estabilización del empleo temporal y se podría ver afectado su nota existencial de autonomía funcional e inclusive de independencia frente al responsable o encargado del tratamiento. No es una vía cerrada absolutamente, pero no es tal vez la más apropiada.

Lo que sí parece cierto es que, teniendo en cuenta que se trata de una figura nueva con las enormes singularidades que ofrece, lo más normal es que se produzca la creación de un puesto de trabajo de nuevo cuño, que se habría de definir funcionalmente de acuerdo con lo establecido en el RGPD y en la

futura LOPD, así como en la normativa que la desarrolle, y encuadrarlo en tal condición en la estructura orgánica de la organización, pero sin dependencia jerárquica de ninguna otra estructura.

La creación de un nuevo puesto de trabajo supone la inserción del mismo en la Relación de Puestos de Trabajo o Instrumento de gestión de similares características, salvo que el puesto se califique como de personal directivo profesional (de acuerdo con lo que luego se dirá). Y ello también representa que la modificación de la Relación de Puestos de Trabajo se ha de aprobar por los órganos de gobierno que prevé la LBRL (Pleno o Junta de Gobierno), previa negociación con los agentes sociales, y este proceso implica tiempo. En tal sentido hay que ser conscientes de que apenas quedan dos meses para la plena efectividad del RGPD. Por tanto, las decisiones que se han de tomar deberían ser expeditivas o rápidas.

Además de todo ello, se debería consignar en plantilla la existencia de tal plaza (algo que con toda seguridad no se habrá previsto en la inmensa mayoría de los casos en que se hayan aprobado los Presupuestos para 2018 y las correspondientes plantillas presupuestarias).

Y, una vez que se hayan cumplido estos trámites preceptivos y necesarios se habrá de establecer el modo de provisión del puesto de trabajo o, en su defecto, las convocatorias selectivas que procedan. La puesta en marcha del procedimiento de provisión de puestos de trabajo requiere, en primer lugar, la elaboración de las bases y la ejecución del procedimiento hasta la cobertura del puesto de trabajo. También esto requiere tiempo y, tal como se ha visto, es algo que las organizaciones públicas no tienen si quieren llegar a la fecha indicada (25 de mayo de 2018) con los deberes hechos, algo que se antoja casi imposible.

Siempre quedan fórmulas alternativas para intentar salir del paso. Una sin duda es la creación del puesto de trabajo y su cobertura transitoria mediante comisión de servicios. En este caso, la debilidad del DPD también sería obvia, pero cabría recurrir a ese medio hasta la provisión del puesto por un procedimiento ordinario. No obstante, en la comisión de servicios se debería salvaguardar plenamente que la persona designada acredite el perfil profesional requerido para el desempeño del puesto y, por tanto, lo lógico sería que se abriera un proceso público y competitivo, siquiera fuera rápido, para esa provisión por ese mecanismo excepcional.

Otra es acudir a atribuir las funciones de DPD a un puesto de trabajo ya existente en la estructura, con carácter parcial o mediante la redefinición funcional del puesto, lo que comportaría una modificación de la RPT. Si se opta por la atribución de las funciones a un puesto de trabajo ya existente, se ha de partir del dato objetivo que las funciones de DPD son enormemente singulares y que –tal como se ha visto- no tienen parangón con ninguna otra de las que actualmente se desempeñan en las organizaciones públicas (ni siquiera con la vieja figura del responsable del fichero o de seguridad). Por tanto, cualquier adición de las nuevas funciones conllevaría una redefinición del puesto de trabajo y una necesaria modificación del mismo, así como una configuración “ex novo” de su estatuto jurídico.

Si no se configura como alto cargo por las razones expuestas, cabe plantearse cuáles serían las soluciones institucionales que se pueden barajar en torno a la provisión del puesto de trabajo del Delegado de Protección de Datos. Y aquí surgen los problemas, pues se plantean dos tipos de tensiones que se proyectan sobre dos principios también en tensión: a) Por un lado, la profesionalidad *versus* discrecionalidad; y, por otro, b) la temporalidad *versus* permanencia (o estabilidad). Veamos sucintamente ambas tensiones y sus consecuencias.

La primera tensión (profesionalidad/discrecionalidad) debería resolverse a favor del primer principio, puesto que una “designación discrecional” no cumpliría las exigencias mínimas establecidas por el RGPD. El procedimiento de libre designación, en su formulación tradicional, no encajaría en el espíritu ni finalidad del Reglamento, a pesar de que en este (y en el propio PLOPD se utilice la expresión “designación”: hay que tener en cuenta que se aplica también al sector privado). La única forma de paliar esta limitación estribaría en establecer previamente a la entrada en acción del procedimiento de libre designación (o de libre nombramiento) algún sistema de acreditación de competencias (incluida, en su

caso, la certificación) que garantice los conocimientos, experiencia y capacidades necesarios para desarrollar esas funciones. Lo normal es que el sistema de provisión de estos puestos de trabajo recoja esas exigencias de profesionalidad y elimine o acote al máximo la discrecionalidad en la designación, sino que esta obedezca al cumplimiento de tales parámetros. La AEPD sugiere, en buena lógica y ante la carencia de perfiles especializados, "desarrollar de forma inmediata una labor de formación de posibles candidatos a ocupar por primera vez los puestos de DPD en todos los niveles de las AAPP". Asimismo, también propone "establecer con carácter permanente actividades de formación en protección de datos para empleados públicos que deseen especializarse en la materia y optar eventualmente a ocupar los puestos de DPD". Son dos medidas sensatas, pero que se deben completar con una visión más amplia: las administraciones públicas deben invertir muchísimos recursos y tiempo en construir nuevos perfiles de puestos de trabajo relacionados con la digitalización y las TIC, así como formar intensivamente a sus empleados públicos en esta línea. La robotización y la inteligencia artificial harán desaparecer muchos puestos de trabajo del sector público (o dejarlos sin funciones), pero asimismo se demandarán otros muchos puestos de perfiles completamente distintos o nuevos y, por lo común, muy tecnificados (vinculados a la gestión de información y datos). La provisión del DPD puede ser un buen banco de pruebas para iniciar un proceso en la dirección indicada. No estaría mal comenzar por ello y explorar construcción de nuevos perfiles, así como herramientas formativas.

Parece más razonable que si se crea un puesto de trabajo singular de DPD, su provisión se lleve a cabo por medio del procedimiento de *concurso específico* mediante el cual se podrán realizar, aparte de la valoración de los méritos, determinadas pruebas tales como la elaboración de memorias o celebración de entrevistas, por medio de las cuales se pueda acreditar mejor que la persona designada adecua su perfil de competencias a las peculiaridades derivadas del puesto de trabajo objeto de la convocatoria[23]. Una vez más, el tiempo juega en contra, también en este caso.

La segunda tensión se suscita en torno a si la cobertura de tales puestos de trabajo debe ser temporal o permanente. Parece claro que, dadas las funciones que así se establecen en el RGPD, son puestos de naturaleza estructural, por tanto la primera impresión sería que cabría defender su estabilidad y permanencia. Más aún teniendo en cuenta que la política de protección de datos antes los riesgos evidentes de los tratamiento masivos o generalizados de datos y el cruce de algoritmos, se deberá incrementar con el paso del tiempo, teniendo estos puestos de trabajo un perfil cada vez más central en torno a esa evaluación y prevención de riesgos en los tratamientos de datos, así como requiriendo un proceso (y capacidades, por tanto) de adaptación permanente.

Pero una cosa es que el puesto tenga ese carácter y otra bien distinta es que la persona (funcionario) que sea nombrado o designado para tales funciones deba serlo con carácter definitivo. Al ser puestos de nueva creación y sin recorrido previo en las administraciones públicas, esa puede ser una opción no exenta de riesgos. Un error inicial en la provisión mediante concurso o concurso específico pudiera dejar desarmada a la Administración Pública de una pieza esencial para el correcto andamiaje de la puesta en marcha del RGPD en sus respectivas organizaciones. Tampoco estaría mal construir un sistema que permitiera una cierta rotación. Pero estas son decisiones organizativas y algunas no exentas de cierta complejidad, dada la rigidez del régimen jurídico de la función pública que se encuentra absolutamente inadaptado para asumir tales retos organizativos.

Si se va a un modelo de puestos de trabajo permanentes o estructurales rígidos, la solución sería –tal como se ha dicho- acudir a la provisión de tales puestos por el procedimiento de concurso específico, mucho mejor que el mero y simple concurso de méritos. Si se opta por puestos de trabajo estructurales (algo complejo de articular en el actual contexto normativo), pero con una temporalidad marcada, la opción más cabal es aplicar a la cobertura de puestos de trabajo una serie de exigencias que se derivan del estatuto jurídico de la figura del DPD según se puede deducir del RGPD: convocatoria pública, libre concurrencia, acreditación de los conocimientos, experiencia y capacidad para el desarrollo del puesto

[23] Ver, por ejemplo, artículo 45 del Real Decreto 364/1995, de 10 de marzo, por el que se aprueba el Reglamento General de Ingreso del personal al servicio de la Administración General del Estado y de provisión de puestos de trabajo y promoción profesional.

de trabajo, prever una temporalidad en su desempeño con posibilidades de volver a concursar en las sucesivas convocatorias, pero asimismo no incluir este tipo de puesto de trabajo en las relaciones de puestos de trabajo o, si se hiciera, dejarlos extramuros, dada su especial singularidad, de la negociación sindical.

Para dar respuesta a esa opción organizativa una vía a explorar podría ser la de aplicar un estatuto jurídico similar a la figura de la Dirección Pública Profesional, pero en este caso la rendición de cuentas (evaluación) se debería vehicular, tal como expone el Reglamento, al más alto nivel jerárquico del responsable o encargado del tratamiento. Sin embargo, el carácter casi inédito de esa figura de la Dirección Pública Profesional, que solo se ha (mal) desarrollado normativamente en algunas leyes de Comunidades Autónomas que establecen un sistema de provisión público y de libre concurrencia donde se tiene en cuenta la idoneidad, el mérito y la capacidad, pero que acto seguido establece una modalidad de libre cese, hace muy difícil explorar esa vía para adecuarla a las necesidades de insertar el DPD en la estructura, en particular porque no hay regulación de desarrollo o porque esta es inadecuada para cumplir las exigencias del RGPD, pues no puede haber cese discrecional en ninguno de los casos.

La única opción para transitar esta vía de la inserción del DPD como "directivo público profesional" sería, allí donde el EBEP no esté desarrollado en estas materias[24], promover la regulación de esta cuestión mediante Reglamento la figura y dotarla de ese carácter, aplicándole las exigencias básicas del artículo 13 TREBEP, pero modulando sus contenidos a través de una acreditación previa de competencias profesionales y cerrando el paso a la discrecionalidad del cese.

Dada la singularidad de la figura del DPD y su peculiar encaje en la estructura orgánica de la Administración Pública, no cabría descartar que la solución normativa (un Reglamento de carácter estrictamente organizativo) fuera la vía más correcta para resolver todos y cada uno de los problemas analizados a lo largo de estas páginas. De nuevo nos topamos con la dificultad del tiempo que conlleva aprobar un Reglamento de estas características, al menos en el ámbito del gobierno local, puesto que requiere la aprobación inicial, el período de información pública y la aprobación definitiva, sin perjuicio de que en este caso no sea preceptiva la consulta pública previa. Pero, tal vez, puede ser la opción más limpia si se opta por una fórmula de DPD con una impronta de temporalidad (que se debería acotar en el tiempo a un mínimo de 4 o 5 años) y se acude a la figura del Directivo Público Profesional y no a un funcionario cuya provisión sea por concurso específico.

En todo caso, parece prudente que ante los obvios vacíos de regulación que ofrece el Reglamento (UE) 2016/679, así como frente a las anomias (auténticas "calvas") que en esta materia tiene el PLOPD, al tratarse de una potestad de autoorganización, tendrá que ser la administración pública correspondiente o el nivel de gobierno competente la instancia adecuada para elaborar alguna disposición normativa de naturaleza reglamentaria (o, en su defecto, un acuerdo de gobierno o plenario) que desbroce muchas de las incógnitas que todavía quedan a dos meses vista de la plena aplicación de la normativa europea. Reformar los sistemas de provisión de puestos de trabajo requiere una Ley, pero adaptar esos sistemas a las enormes singularidades que ofrece esta figura del Delegado de Protección de Datos (preludio tal

[24] Por ejemplo, en el País Vasco los municipios de más de 40.000 habitantes podrían perfectamente acudir a esta vía, de acuerdo con lo establecido en el capítulo IV del Título III de la Ley 2/2016, de 7 de abril, de instituciones locales de Euskadi, en relación con lo que prevé la disposición adicional decimosegunda de ese mismo texto normativo. En otras CCAA que hayan desarrollado a través de Ley la figura de la DPP hay que examinar si esa regulación normativa es aplicable a las entidades locales y, en todo caso, eliminar de tal régimen jurídico el cese discrecional, por estar directamente vedado por el artículo 38.3 RGPD. En Cataluña no hay ningún desarrollo del EBEP en estas materias, salvo en algún municipio (por ejemplo, Sant Feliú de Llobregat, aunque prevé el cese discrecional de los directivos públicos profesionales), por lo que se debería aprobar un Reglamento específico que regulara la figura del DPP y su sistema de provisión, sobre todo si se le quiere dar el carácter de DPD. En Cataluña hay que examinar, no obstante, la regulación específica que algunas Diputaciones tienen de la figura del directivo público profesional (Barcelona) o de los órganos directivos (Lleida), pero en ninguno de ambos casos podría servir plenamente tal regulación porque habría que adaptarla a las previsiones del estatuto singular de inamovilidad (relativa) que tiene quien ostente tales funciones, que solo podrá ser removido o sancionado –de acuerdo con el artículo 36.3 PLOPD, cuando incurra "en dolo o negligencia grave en su ejercicio".

vez de otras muchas figuras o puestos de trabajo de especial factura que, en el campo de la digitalización y Big Data, se puedan dar en los años venideros, también en el sector público) requiere sin duda dosis de ingenio, propuestas creativas e innovadoras, adaptabilidad, flexibilidad en el diseño y una línea de trabajo sostenida que haga avanzar a la administración pública por el camino de la profesionalización, la tecnificación y la apertura a la sociedad, en consonancia con el Gobierno Abierto y la Gobernanza Pública, ámbitos en los que también debe encajarse este nuevo e inmediato reto.

Los problemas –y no descubro nada nuevo- son los de siempre: la rigidez enorme (y absoluto desfase) de nuestro sistema normativo de función pública y su clara y evidente obsolescencia para dar respuesta a estas nuevas necesidades que ya comienzan a emerger de forma clara en el sector público. Habrá que ponerse creativos, aunque algunos estén tentados a trampear una vez más una normativa, actitud que debe ser recriminada. Pero, guste más o guste menos, ese nuevo marco normativo de protección de datos de carácter personal ha venido para quedarse o, cuando menos, para ser profundizado y adaptado en los próximos años. Veremos qué respuestas dan también los tribunales de justicia (TJUE, TC o jurisdicción contencioso-administrativa) a las numerosas cuestiones abiertas y no menos dudas que existen sobre su inmediata aplicación.

En cualquier caso, la regulación en materia de protección de datos personales es la única vía sensata para intentar evitar (no digo conseguir) que la intimidad personal y el derecho a la autodeterminación informativa y el resto de derechos fundamentales de la persona física no se vean lapidados completamente por una revolución tecnológica que hace de los datos personales un objeto cada vez más vulnerable. También en la Administración Pública. Al menos comencemos por ahí, aunque la laxitud sancionadora del PLOPD cuando de instituciones públicas se trata que reitera, como si nada hubiera pasado, el esquema de la aún vigente LOPD de 1999, no augure nada bueno en este terreno, donde se avanzará poco a poco y probablemente con mucha menos convicción de la que sería necesario asumir (pues hay "zanahoria", pero el "palo" está escondido). Aunque los responsable públicos deben tomar nota, puesto que el artículo 73, v) del PLOPD, prevé como falta grave el incumplimiento de la obligación de designar el DPD, si bien como no se aprobará tal Ley antes de unos meses, buena parte de las Administraciones Públicas procrastinará una vez más el cumplimiento de tal exigencia. Sea como fuere, el papel del Delegado de Protección de Datos y de las autoridades de control, especialmente de estas últimas, se torna imprescindible en este proceso que ahora se inaugura. Como siempre, nos hemos despertado muy tarde. Y, según parece, tampoco demasiado bien.