La figura del *Data Protection Officer* en la contratación pública en España

Juan Francisco Rodríguez Ayuso[1]

RESUMEN:

Este trabajo de investigación busca ofrecer un análisis sistemático de las transformaciones que trae consigo la incorporación a nivel europeo (RGDP), que es además novedosa dentro del ordenamiento jurídico español (LOPDGDD), de la figura del delegado de protección de datos. De manera concreta, se trata de explorar las circunstancias que rodean la designación, la incorporación y el desenvolvimiento de esta institución en el seno de la contratación pública; poniendo de relieve aquellas notas singulares que caracterizan su nombramiento, su posición dentro de la organización administrativa y las funciones que está llamada a desempeñar.

Palabras clave: protección de datos, contratación pública, RGDP, dato personal, Administraciones públicas.

1 Doctor en Derecho, docente y coordinador académico del máster en Protección de Datos de la Universidad Internacional de La Rioja (UNIR), La Rioja, España. Correo-e: juanfrancisco.rodriguez@unir.net. Enlace ORCID https://orcid.org/0000-0003-4721-1465. Fecha de recepción: 1.º de julio de 2020. Fecha de modificación: 20 de septiembre de 2020. Fecha de aceptación: 22 de septiembre de 2020. Para citar el artículo: Rodríguez Ayuso, Juan Francisco, "La figura del *Data Protection Officer* en la contratación pública en España" *Revista digital de Derecho Administrativo*, Universidad Externado de Colombia, n.º 25, 2021, pp. 309-336. DOI: https://doi.org/10.18601/21452946.n25.10.

The Data Protection Officer in Public Procurement in Spain

ABSTRACT:

This paper aims to offer a systematic analysis of the transformations resulting from the creation of the Data Protection Officer at a European level (GDPR), also a novelty for the Spanish legal system (LOPDGDD). Specifically, this research seeks to explore the circumstances surrounding the appointment, incorporation and development of this institution in the matter of public procurement. To this end, it highlights the singular notes characterizing the appointment, position within the administrative organization, and the functions of the Data Protection Officer.

Keywords: Data Protection, Public Procurement, GDPR, Personal Data, Public Administration.

INTRODUCCIÓN

La Estrategia Europa 2020[2], elaborada por la Comisión Europea y cuyo plazo de vencimiento concluye este mismo año, está orientada a fortalecer la Unión Europea por medio de un sistema económico basado en el crecimiento inteligente, sostenible e inclusivo[3]. Y es que, tal y como ponía de manifiesto este organismo, el territorio comunitario se encuentra incurso en pleno proceso transformador, una vez superado el retraso económico-social instaurado por la crisis iniciada hace más de una década. Para la Comisión, este procedimiento ha de ser considerado como reversible, siempre y cuando se actúe con una visión global e integradora en el marco de la Unión, por lo que resulta imprescindible una estrategia que ayude al territorio europeo a adquirir una mayor fortaleza global tras la precitada situación y poder disfrutar de un elevado nivel de empleo, productividad y cohesión social[4].

La *supra* referenciada Estrategia, que conforma una propuesta del mercado europeo desde una perspectiva económica y social, establece un conjunto de aspectos prioritarios que se retroalimentan de forma recíproca: en primer lugar, la necesidad de que el desarrollo económico sea inteligente, es decir,

2 Comunicación de la Comisión Europea, 2020, Una estrategia para un crecimiento inteligente, sostenible e integrador, Bruselas 03/03/2010. COM (2010) 2020 final.

3 María Magnolia Pardo López, "Mención de criterios sociales y medioambientales en la definición del objeto del contrato", en María Magnolia Pardo López y Alfonso Sánchez García (dirs.), *Inclusión de cláusulas sociales y medioambientales en los pliegos de contratos públicos: guía práctica profesional*, Cizur Menor (Navarra): Aranzadi, 2019, pp. 49-50.

4 COM (2010) 2020 final.

sustentado sobre la base de dos pilares fundamentales: el conocimiento y la innovación. Para ello, resulta necesario profundizar en la idea de la especialización, a fin de conseguir una mayor competitividad a nivel internacional. Además, el crecimiento ha de ser sostenible, entendido como la necesidad de fomentar una economía que potencie y permita un empleo más eficiente de los recursos, siendo esta más verde y, en definitiva, competitiva. Por último, un crecimiento integrador o inclusivo, concebido como garante de un sistema económico capaz de conseguir altos niveles de empleabilidad, suficientes para generar una unión social y territorial óptima[5].

Al mismo tiempo, con el fin de asegurar la consecución de estos objetivos, la Comisión Europea pone de relieve una serie de propósitos esenciales a nivel comunitario, propósitos que se hallan interconectados y que son básicos para la consecución del planteamiento propuesto, además de representar adecuadamente las prioridades que se acaban de apuntar, si bien no de forma limitativa, toda vez que resulta necesario un gran abanico de acciones adicionales desde una perspectiva nacional, comunitaria e internacional que les sirvan de sustento. Al respecto, se proponen un total de siete iniciativas que permitan canalizar los progresos fijados como preferentes[6].

En este orden de ideas, mecanismos como el mercado único, la asistencia económica y los instrumentos de política exterior se movilizan de forma plena para afrontar los inconvenientes expuestos y conseguir los objetivos de la Estrategia 2020. Lo mismo parece hacer la contratación pública, privilegiado instrumento de mercado, hasta el punto de ser esencial y fundamental en el

5 Ibíd.

6 Estas iniciativas son las siguientes: a) "Unión por la innovación", que persigue el objetivo de conseguir una mejora de las condiciones generales y el acceso a la financiación necesaria para investigar e innovar y garantizar que ello pueda generar crecimiento y empleo; b) "Juventud en movimiento", para aumentar los resultados de los sistemas educativos y fomentar el acceso de la gente joven en el mercado laboral; c) "Una agenda digital para Europa", consiguiendo un aceleramiento del desarrollo de la red de redes y que el mercado único llegue a las empresas y a las familias; d) "Una Europa que utilice eficazmente los recursos", a fin de desligar crecimiento económico y empleo de recursos, sustentar la transformación en reducidas emisiones de carbono, fomentar el empleo de fuentes de energía renovables, modernizar el sector del transporte y conseguir una promoción de la eficiencia energética; e) "Una política industrial para la era de la mundialización", mejorando el entorno de trabajo y su competitividad desde una perspectiva internacional; f) "Agenda de nuevas cualificaciones y empleos", modernizando el mercado laboral y potenciando la autonomía de los individuos al desarrollar sus capacidades; y g) "Plataforma europea contra la pobreza", garantizando la cohesión social y territorial de tal suerte que las bondades del crecimiento y del empleo sean ampliamente compartidas y las personas en situación de pobreza y exclusión social consigan vivir de forma digna y participar activamente en la sociedad. Parlamento Europeo, Fichas técnicas sobre la Unión Europea, 2019, p. 1. Disponible en: www.europarl.europa.eu/factsheets/es [consultado el 30 de junio de 2020].

sistema económico de los Estados miembros, conformando entre el 16% y el 20% del PIB[7].

No es extraño el interés mostrado en torno a la licitación en el sector público en el ámbito europeo, especialmente al hilo de dicha Estrategia Europa 2020, aun cuando resulta evidente que la intervención del derecho de la Unión en este ámbito no constituye algo novedoso, pues se ha venido produciendo desde los años setenta del siglo XX[8]. No obstante, fue en la segunda década del siglo XXI cuando, merced al Libro Verde intitulado "Hacia un mercado europeo de contratación pública más eficiente"[9] sobre modernización de la política en materia de contratación pública, se produciría una intensificación del proceso legislativo encaminado a fomentar la conformación de una Unión Europea. Con esto, se buscó que esta última fuera más responsable desde una perspectiva social y medioambiental, apostando por crecer sobre la base de la sostenibilidad y la integración.

De conformidad con este propósito, fueron expedidas las "Directivas de cuarta generación" en materia de contratación[10], transpuestas al ordenamiento jurídico español por la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público[11]. En todas estas directivas, se persigue unir la visión puramente económica de la contratación pública con su vocación de "herramienta jurídica al servicio de los poderes públicos para el cumplimiento efectivo de sus fines o sus políticas públicas"[12] en el ámbito del Estado social y democrático de derecho. El reto consiste en la redacción de los pliegos de la contratación. En concreto, la consecución del fin social y medioambiental propiciado por la Unión Europea ha de traducirse en la inclusión de cláusulas sociales

7 Ibíd.

8 Al respecto, véase JOSÉ MARÍA MIRANDA BOTO, "Contratación pública y cláusulas de empleo y condiciones de trabajo en el Derecho de la Unión Europea", *Lex Social: Revista Jurídica de los Derechos Sociales*, n.º 2, 2016, pp. 69-91.

9 COM (2011) 15 final, de 27 de enero de 2011.

10 Estas directivas son las siguientes: 1) Directiva 2014/23/UE del Parlamento Europeo y del Consejo de 26 de febrero de 2014 relativa a la adjudicación de contratos de concesión (*Diario Oficial de la Unión Europea* –en adelante, DOUE– L 94/1, de 28 de marzo de 2014); 2) Directiva 2014/24/UE del Parlamento Europeo y del Consejo de 26 de febrero de 2014 sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (DOUE L 94/65, de 28 de marzo de 2014), y 3) Directiva 2014/25/UE del Parlamento Europeo y del Consejo de 26 de febrero de 2014 relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE (DOUE L 94/243, de 28 de marzo de 2014).

11 Por la que se transponen al ordenamiento jurídico español las directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (en adelante, LCSP) Boletín Oficial del Estado (en adelante, BOE) n.º 272, de 9 de noviembre de 2017.

12 JOSÉ MARÍA GIMENO FELIÚ, "El nuevo paquete legislativo comunitario de contratación pública: principales novedades. La orientación estratégica de la contratación pública", en AA. VV., *Las nuevas directivas de contratos públicos y su transposición*, Madrid: Marcial Pons, 2016, p. 20.

incorporadas, dependiendo del caso, por el propio legislador o por el poder adjudicador, ya sea en fase de admisión de ofertas, de valoración de las mismas o de ejecución del contrato.

En el presente artículo se abordarán, entre dichas cláusulas sociales, aquellas dirigidas a garantizar el derecho fundamental de los interesados a la protección de sus datos personales, es decir, a la garantía de su privacidad, elemento inherente a la naturaleza social del ser humano. Está prevista de esta forma la incorporación, exigible en el seno de toda organización que quiera optar a la contratación, de la figura conocida como el *Data Protection Officer* (DPO). Se trata de un instrumento esencial para el control y la supervisión del tratamiento de datos personales realizado por parte del responsable del mismo[13]. A lo largo del presente artículo, y comenzando en el siguiente epígrafe, se estudiarán todos los elementos inherentes al DPO en el ámbito de cualquier organización, bajo la nueva regulación nacional y comunitaria en materia de protección de datos. Tras vislumbrar su origen e imbricación con los principios relativos al tratamiento de datos, el estudio se focaliza en tres aspectos esenciales, a la vez que controvertidos: a) su nombramiento, ya sea preceptivo o voluntario, atendiendo a la naturaleza del sujeto responsable y a la sensibilidad de las informaciones; b) su posición dentro de la organización, donde se pone de relieve la necesaria imparcialidad que, como elemento principal, ha de revestir su actuación; y c) las funciones que está llamado a desempeñar dentro de la empresa, algunas de las cuales se han visto reforzadas en tiempos de emergencia sanitaria como la presente, dominada por la crisis de la COVID-19.

Una vez resueltas las aristas específicas de esta cuestión, se examinan las exigencias propias de aquellas cláusulas sociales de pliegos de contratos públicos que requieren del nombramiento y designación, en cumplimiento del derecho fundamental contemplado en el artículo 18 de la Constitución española de 1978[14]. De esta figura, como elemento objetivo de garantía por parte de la Administración pública licitante, se procurará dar respuesta a la valoración que estos organismos públicos hacen de aquellas organizaciones que, optando por una licitación, sigan el principio de responsabilidad proactiva a la hora de contar con un delegado de protección de datos, como se conoce la figura del DPO en el derecho español, de forma voluntaria. Y, amén de lo anterior, se determinará cuáles han de ser los requisitos objetivos que permitan determinar que el delegado de protección de datos designado reúne la formación y cualificación necesarias para poder llevar satisfactoriamente a término las funciones que tiene encomendadas.

13 Sobre esta cuestión, véase Alberto Díaz-Romeral Gómez, "Protección de datos y contratación pública", en Isabel Gallego Córcoles y Eduardo Gamero Casado (coords.), *Tratado de contratos del sector público,* Valencia: Tirant lo Blanch, 2018, pp. 422-466.

14 BOE n.º 311, de 29 de diciembre de 1978.

1. LA PRIVACIDAD EN EL MARCO NORMATIVO DE PROTECCIÓN DE DATOS PERSONALES Y EL DPO COMO EXIGENCIA EN LOS PLIEGOS DE LA CONTRATACIÓN

Para encontrar el origen del DPO debemos ubicarnos en Alemania, siendo el primer país en instituir la figura, integrada en la Ley Federal de la Defensa de Información Personal, nombrada como *Beauftragten für den Datenschutz*[15]. Aun así, hay quienes sostienen que sus antecedentes se ubican al amparo de otra compañía alemana, incluso con anterioridad a la indicada normativa[16].

A nivel europeo, la aparición de esta institución se remonta a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos[17] (en lo sucesivo, DPDP), predecesora del actual RGPD. No obstante, su implantación a nivel interno no se impuso de forma preceptiva, antes bien opcional, motivo por el cual tan solo determinados Estados miembros decidieron proceder a su incorporación dentro de su ordenamiento jurídico interno. Dentro de estos países no se incluía a España, que decidió prescindir de esta figura, tanto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD), como en el Real Decreto 1720/2007, de 21 de diciembre, en el que se establece el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, RDLOPD). Años después, como resultado de una enmienda a la Propuesta de DPDP, exhibida por el Parlamento Europeo, surge el delegado de protección de datos (DPD), anteriormente llamado *encargado de la protección de datos*, conforme la interpretación al castellano, lo cual hizo que se incluyera en el texto final de la Directiva comunitaria, quedando plasmado así en las observaciones propias a la Posición Común: "se han permitido excepciones en el caso de que se haya designado a un encargado que se ocupe de las tareas descritas y garantice así que los tratamientos no pueden menoscabar los derechos y libertades de las personas afectadas".

El segundo guion del artículo 18.2 DPDP establecía que los Estados poseían la facultad de simplificar o no incluir la notificación a la autoridad de control,

15 La ley federal de protección de datos personales (BDSG 1977), denominada *Beauftragten für den Datenschutz*, no es sino la *Bundesdatenschutzgesetz* (1977), que ha sido modificada en varias ocasiones.

16 Sobre esta cuestión, véanse MANUEL GONZÁLEZ CALVO, "La nueva figura del delegado de protección de datos", *Actualidad jurídica Aranzadi,* n.º. 939, 2018, p. 7; JESÚS ALBERTO MESSÍA DE LA CERDA BALLESTEROS, "Consideraciones y perspectivas del delegado de protección de datos", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 47, 2018.

17 *Diario Oficial de las Comunidades Europeas* (en adelante, DOCE) L 281/31, de 23 de noviembre de 1995.

indicada en el artículo 28 DPDP, con antelación a la confección de un proceso o grupo de procedimientos, completa o relativamente automatizados, solamente en aquellos casos en los que la organización contara con un delegado de protección de datos personales que tuviese como cometido, en particular:

a. Reclamar que sean aplicadas, en el espacio interno y de manera autónoma, aquellas resoluciones estatales adoptadas bajo la protección de la DPDP.

b. Mantener una inspección (que podríamos considerar el antecedente del actual registro de las actividades de tratamiento) de los tratamientos realizados, que recogiese los datos englobados en el artículo 21.2 DPDP (con carácter de mínimos, nombre y dirección del responsable del tratamiento o de su representante; el/los propósito/s del tratamiento; los fines del tratamiento; los destinatarios o categorías de destinatarios a los que se podrían comunicar los datos o las transmisiones de datos a terceros países).

De esta forma, se exigía que el tratamiento de la información personal no perjudicara los derechos y libertades de los titulares de dicha información personal (es decir, de los interesados).

Al amparo de esta previsión, varios Estados miembros (Suecia, Países Bajos, Francia o Luxemburgo) procedieron a contemplar la opción introducida por la DPDP en el seno de la Unión Europea. Con el transcurso del tiempo, la experiencia mostrada en estos países ha sido, en términos generales positiva, instaurando al DPO como elemento esencial a la hora de garantizar una verdadera seguridad de la información personal de los interesados en cada uno de los territorios comunitarios en que fue implementada. Gracias a ello, algunos Estados, incluso no comunitarios, procedieron igualmente a adoptar la figura del DPD u otras figuras análogas, y lo hicieron por medio de disposiciones normativas de aplicación obligatoria, como fue el caso de Estados Unidos, México o Suiza[18].

También el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) ha tenido ocasión de pronunciarse en torno a la conveniencia del DPO en sentencias como la de 9 de noviembre de 2010, en el proceso *Volker und Markus Scheke* y *Eifert*[19].

18 Manuel Recio Gayo, "El delegado de protección de datos", en José Luis Piñar Mañas (dir.), *Reglamento General de Protección de Datos*, Madrid: Reus, 2006, p. 369.

19 Sentencia del Tribunal de Justicia (Gran Sala), de 9 de noviembre de 2010, en los asuntos acumulados C-92/09 y C-93/09. En concreto, uno de los aspectos abordados por el TJUE fue el concerniente a si el apartado segundo del artículo 18 DPDP había de ser interpretado de forma que la publicación con arreglo al Reglamento (CE) n.º 259/2008 de la Comisión de 18 de marzo de 2008 por el que se establecen disposiciones de aplicación del Reglamento (CE) n.º 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de fondos procedentes del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader) únicamente podría afectar cuando se hubiera seguido el procedimiento, contemplado en este precepto, que reemplaza, repetimos, a la notificación de la autoridad de control. Respondiendo a esta

Además, debemos tener en cuenta que el delegado de protección de datos ya actuaba, *a priori*, en relación a las entidades e instituciones comunitarias[20]. En efecto, el artículo 24.1 de dicho reglamento fijaba que le correspondía a cada corporación e institución designar como mínimo a una persona para realizar su labor como responsable de la seguridad de la información personal. Asimismo, se establecía en el apartado octavo de ese precepto que era imprescindible valorar las normas adicionales o de ejecución, referente a las labores, atribuciones y jurisdicciones que pertenecen al DPD. Las distribuciones de este texto se han analizado e interpretado, en gran medida, por el supervisor europeo de protección de datos (SEPD), constituyendo las reglas resultantes importantes referentes a tener en consideración.

Conviene añadir, como último dato en el ámbito público, a las autoridades que poseen la jurisdicción para advertir, explorar, localizar o valorar infracciones de índole penal o efectuar sanciones penales, en el cual se engloban la prevención y defensa frente a ataques y/o desafíos para la seguridad pública. También ellas deberán designar un delegado de protección de datos en relación con toda información personal tratada, según la Directiva (UE) 2016/680[21].

Llegamos en la actualidad al Reglamento General de Protección de Datos y, a nivel interno, ampliándolo y suplementándolo, a la LOPDGDD. Más exactamente, a las disposiciones que disciplinan la figura del delegado de protección de datos, contenidas en los artículos 37 a 39 RGPD y 34 a 37 LOPDGDD, las cuales ponen de manifiesto la envergadura e importancia que representa el DPO a nivel nacional y comunitario. Mientras que su incorporación inicial en la DPDP no se exigía de forma imperativa[22], su nombramiento de acuerdo con el RGPD y a la LOPDGDD será obligatorio por parte de todos aquellos responsables y encargados del tratamiento que incurran en cualquiera de los supuestos previstos. Estos últimos, atendiendo a las características de los tratamientos

cuestión, y refiriéndose, de un modo específico a la figura del DPO, el TJUE sostiene que a este encargado de la protección de datos le corresponde aplicar determinadas actividades que tienen por fin garantizar que el tratamiento de los datos personales no conlleve un deterioro de los derechos y libertades de las personas físicas titulares de los datos personales.

20 Apoyado por el Reglamento (CE) n.º 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos; DOCE L 8/1, de 12 de enero de 2001.

21 Directiva del Parlamento Europeo y del Consejo, de 27 de abril de 2016, correspondiente a la seguridad de las personas físicas referente al manejo de información personal por parte de las autoridades competentes para su uso en prevención, exploración, rastreo de datos o proceso jurídico de incumplimientos o ejecuciones penales, y al independiente tráfico de los datos mencionados y por lo que se revoca la Decisión Marco 2008/977/JAI del Consejo DOUE L 119/89, de 4 de mayo de 2016.

22 Ya que no era preceptiva ni su plasmación en la norma de transposición de los Estados miembros ni, por ende, su designación por quien se encargase y responsabilizase del tratamiento.

y/o a la naturaleza de los organismos que los implementen, deberán contar con un tercero que ejerza funciones de inspección y revisión de un óptimo cumplimiento de las previsiones legales establecidas al respecto[23].

Ahora bien, ni en la regulación anterior ni en la vigente, ya sea interna o comunitaria, se procede a definir en qué consiste el DPD. Por este motivo, una descripción adecuada es la expuesta por el documento relativo a la Evaluación de Impacto de la Comisión Europea sobre la Propuesta de Reglamento[24]. En este informe documentado se conceptualiza al delegado de protección de datos como la persona, responsable en el seno de un responsable o de un encargado del tratamiento, de ejecutar la inspección y vigilancia, de manera autónoma, del tratamiento interno de datos personales y de asegurar que se garantiza una seguridad adecuada en el empleo de información personal.

Más allá de lo anterior, hay que considerar, dependiendo del caso, la posibilidad de elegir un único delegado de protección de datos o una pluralidad de DPO. Para ello, es preciso atender a una serie de factores determinantes, como los que se mencionan a continuación:

a. Grupos de empresas[25], en las cuales se podrá elegir a un único delegado de protección de datos, siempre que a él puedan acudir todas las empresas que son parte integrante del grupo (artículo 37.2 RGPD).

b. En aquellos casos de responsables del tratamiento que sean autoridades o instituciones públicas, en las cuales existirá la posibilidad de nombrar a un único delegado de protección de datos para la totalidad si, fundamentado en su configuración y dimensión, la elección de un solo miembro deviene operativa (artículo 38.3 RGPD).

En estos casos anteriores parece evidente la conveniencia de que las organizaciones analicen con carácter previo las características que les son propias

23 De conformidad con los supuestos legales que obligan al nombramiento de un DPO (artículo 37 RGPD y 34 LOPDGDD).

24 Comisión Europea, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Bruselas, 25 de enero de 2012, COM(2012) 10 final, COM(2012) 11 final, SEC(2012) 73 final. En ella se define al DPO en los siguientes términos: *"[a] person responsible within a data controller or a data processor to supervise and monitor in an independent manner the internal application and the respect of data protection rules. The* DPO *can be either an internal employee or an external consultant"*.

25 Los grupos de empresas aparecen definidos en el artículo 4.20 como aquel grupo constituido por una empresa que ejerce el control sobre las demás, que tendrán la condición de empresas controladas.

para, solo entonces, determinar si resulta conveniente designar a uno o varios delegados de protección de datos[26].

Por lo demás, pese a que la definición arriba anotada incluye varias observaciones valiosas en torno a las responsabilidades fundamentales que corresponden a esta figura y abre la posibilidad de que estas funciones puedan ser desempeñadas tanto por un trabajador interno como por un asesor ajeno a la empresa, ella no contiene ninguna mención en torno a si ha de ser un experto con formación en el ámbito jurídico o si es imprescindible que cuente con otras competencias. Al respecto, resulta indispensable acudir al artículo 37.5 RGPD, el cual dispone que el delegado de protección de datos deberá de ser elegido atendiendo a sus facultades profesionales y, de forma específica, a su formación jurídica especializada en el ámbito de la seguridad de la información personal, habiendo de ser capaz de ejecutar las labores recogidas en el artículo 39 del citado reglamento[27]. Se indica que el delegado de protección de datos debe poseer conocimientos especializados en el ámbito jurídico, algo que se puede traducir en la necesidad de que sean expertos jurídicos, teniendo en cuenta su formación. Sin embargo, tal argumento no es óbice para que expertos que no posean dicha formación lleguen igualmente a ser nombrados DPD. Pese a esto, y a fin conseguir la mayor objetividad posible en la valoración de las aptitudes del DPD para poder ejercer como tal, el modelo ejemplar a seguir es que dicha instrucción especializada sea el resultado de una formación reglada, oficial y homologada, a fin de impedir el desarrollo de prácticas que pudiesen acarrear o converger en una merma de la seguridad o en una protección inapropiada del interesado, por no quedar meridianamente claros los requisitos que se deben reunir para desplegar las funciones de DPD[28].

En este sentido, el artículo 35 LOPDGDD dispone, confirmando cuanto se señalaba, que el desempeño de las condiciones dispuestas en el artículo 37.5 RGPD:

> para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

26 Júlia Bacaria Gea, "El DPD en el sector Administración Local", en Pere Simón Castellano y Jordi Bacaria Martrus (coords.), *Las funciones del delegado de protección de datos en los distintos sectores de actividad*, Madrid: Wolters Kluwer, 2020, p. 111.

27 Miguel Ángel Davara Rodríguez, "El delegado de protección de datos", *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n.º 24, 2017, p. 3093.

28 Sobre esta cuestión, véase Esther Botella Pamies, "Posición del delegado de protección de datos", en Mónica Arenas Ramiro y Alfonso Ortega Giménez (dirs.), *Protección de datos: comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Madrid: Sepin, 2019, pp. 194-197.

Asimismo, estas instrucciones tendrán que ser las adecuadas para, llegado el caso, localizar los riesgos inherentes al tratamiento, tal como establece el apartado segundo del artículo 39 del Reglamento General de Protección de Datos[29]. De igual modo, en el contexto propio de la crisis sanitaria derivada de la pandemia de la COVID-19, resulta imprescindible que los conocimientos propios y específicos del RGPD en relación con la seguridad de la información resulten complementados con un profuso conocimiento de la normativa sanitaria, individualmente considerada y, también, en su conjunción con las singularidades que imprime el tratamiento de datos de salud.

Por consiguiente, al encontrarnos con un derecho fundamental y teniendo en cuenta que el DPD posee o puede llegar a poseer un papel destacado en la implementación de tratamientos de datos personales, hay que considerar el hecho de que quien desempeñe esta labor de asesoramiento, control y supervisión sea una persona con una gran experiencia y formación en el ámbito jurídico y, concretamente, en el estudio de la protección de datos personales. Y ello con independencia de que este sea nombrado como pieza de un grupo multidisciplinar de expertos, si es que su designación resulta apropiada para el organismo[30].

Junto a lo anterior, en la ejecución de responsabilidades que competen al DPD, la organización responsable del tratamiento podrá determinar que la ocupación sea total o a tiempo parcial, atendiendo, entre otras valoraciones, a la naturaleza de los tratamientos, al tipo de datos personales tratados (básicos, datos de salud, orientación sexual, afiliación sindical, datos biométricos o genéticos, etc.), a las categorías de interesados (menores de edad o personas especialmente vulnerables) o a los riesgos que el tratamiento comporta para las libertades y los derechos de las personas interesadas (artículo 34.5 LOPDGDD).

1.1. Nombramiento de la figura atendiendo a la naturaleza del sujeto responsable y a la sensibilidad de los datos

Una vez analizadas las cualidades de la persona que pueda ser nombrada como DPD, conviene examinar aquellas otras vicisitudes que propiciarán su nombramiento y designación, la cual deberá realizarse obligatoriamente en determinados casos y, en otros, podrá tener lugar de forma voluntaria por parte del responsable o del encargado del tratamiento. Esto, a fin de garantizar un

29 Gema Alejandra Botana García, "La formación del Delegado de Protección de Datos (DPO)", *Actualidad Civil,* n.º 5, 2018.

30 Y aunando a otros expertos cuya presencia es obligatoria, conforme a la directiva ya suprimida, como los responsables de seguridad (*Chief Security Officer*),; el oficial de cumplimiento (*Compliance Officer*), el oficial de datos (*Chief Data Officer*) o, incluso el experto en relaciones públicas (*Public Relation*). Miguel Recio Gayo, "El delegado de protección de datos", óp. cit., p. 377.

cumplimiento más adecuado del principio de responsabilidad proactiva. En este sentido, conviene aludir que la redacción definitiva del artículo 37 RGPD, que establece aquellos supuestos de designación obligatoria, es el resultado final de una decisión trascendental de política pública que, desde sus orígenes, fue considerada por la Comisión Europea tras un minucioso análisis de impacto a la hora de incorporar la figura. Con independencia de la proposición originaria del Reglamento General de Protección de Datos presentada por la Comisión, que contemplaba un listado distinto de supuestos que terminaba en la obligación de nombrar un DPD, la redacción final del precepto es el resultado de un deseo por evitar cargas innecesarias a las pequeñas y medianas empresas, así como a otras pequeñas organizaciones[31]. En este contexto, y bajo la premisa del contenido de los apartados primero y cuarto del artículo 37 RGPD, y primero del artículo 34 LOPDGDD, se debe indicar que la responsabilidad de nominar un delegado de tratamiento de datos recae en aquellos responsables o encargados del mismo, que incurran en determinadas circunstancias, como continuación se muestra[32]:

a. *Tratamientos de información personal por parte de entidades u organismos públicos, excepto los tribunales que intervengan en ejercicio de las funciones que les son propias*: El actual Reglamento sobre protección de datos habla de *autoridad u organismo público*, aunque no específica qué se ha de entender al respecto. De esta forma, para analizar la amplitud, el contenido y el significado de esta previsión debemos remitirnos al artículo 2 de la Ley 39/2015, de 1.º de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas[33], norma que, al reglamentar su ámbito objetivo de aplicación, precisa qué se ha de estimar por *sector público*. Esta disposición señala que el sector público estará englobado por la Administración General del Estado, la Administración de las comunidades autónomas, las entidades que componen la Administración local y, finalmente, el sector público-institucional. Por ende, conforman este ámbito todos los organismos que se comprendan en cualquiera de los niveles de la Administración ya especificados (excluyendo la excepción referida respecto con los tribunales que actúen en ejercicio de su función judicial), teniendo, absolutamente todas ellas, que designar un delegado de protección de datos[34].

31 United Nations Conference on Trade and Development, Data protection regulation and international data flows: implications for trade and development, 2016, p. 20.

32 Sobre esta cuestión, véase Miguel Ordiozola Alén, "El delegado de protección de datos (DPD): ¿qué entidades están obligadas a designarlo y cuáles son las funciones y perfil de esta figura clave en el nuevo modelo de privacidad?", *Revista CADE: doctrina y jurisprudencia*, n.º 52, 2019, pp. 61-68.

33 BOE, n.º 236, de 2 de octubre de 2015.

34 En la misma línea, Agencia Española de Protección de Datos, "El impacto del Reglamento general de protección de datos sobre la actividad de las Administraciones públicas", 2016, p. 4.

A esta previsión corresponde adicionar la concreción elaborada por el Grupo de Trabajo del Artículo 29 (en lo sucesivo, GTA29)[35], que advierte de la conveniencia (que no obligación) de designar un DPD también en relación con todas las corporaciones privadas que ejerzan el desempeño de tareas públicas o que ejecuten alguna clase de autoridad pública.

En la actualidad, y en un contexto propio del coronavirus, la previsión del artículo 37.1.a RGPD abarca también a los hospitales públicos que traten a pacientes infectados por el virus. Asimismo, se extiende al Ministerio de Sanidad en relación con la aplicación informática de carácter público de la que es responsable del tratamiento y que le permite la autoevaluación de los individuos que, previo consentimiento y con base en los síntomas médicos que comuniquen, quieran conocer la probabilidad de que estén infectados y que se les proporcione información, consejos prácticos y recomendaciones a seguir según la evaluación, además de posibilitar su geolocalización para verificar que se encuentran donde declaran estar.

No obstante, es necesario preguntarnos si: a) todos los centros sanitarios públicos han de nombrar un DPO o si, b) por el contrario, el único DPO para toda la Administración (la sanitaria inclusive) o propio de la Administración sanitaria se responsabilizará de esas labores relacionadas con todos los hospitales de la red sanitaria pública de su zona territorial. Para dar una respuesta a este interrogante, será preciso analizar cada caso en su singularidad, atendiendo a su tamaño y estructura organizativa, aunque sea posible considerar como la solución más adecuada y satisfactoria el nombramiento de un DPD sanitario determinado que actúe en coordinación con sus homónimos del resto de las

35 Grupo de Trabajo sobre Protección de Datos del artículo 29, Directrices sobre los delegados de protección de datos (DPD), 16/ES WP 243 rev.01, adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017, p. 7. En concreto, este grupo, además de reiterar que la noción de autoridad u organismo público debe determinarse en virtud del derecho nacional de los Estados miembros, que "Una labor pública puede llevarse a cabo, y la autoridad pública 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 y energía, las infraestructuras viarias, la radiodifusión pública, la vivienda pública o los órganos disciplinarios de las profesiones reguladas. En estos casos, los interesados pueden estar en una situación muy similar a la que se produce cuando una autoridad u organismo público trata sus datos. En particular, los datos pueden tratarse para fines similares y las personas suelen tener un poder de decisión igualmente escaso o nulo sobre si sus datos se tratan y de qué manera, y pueden, por tanto, requerir la protección adicional que pueda aportar la designación de un DPD. 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 ejercen autoridad pública designen un DPD. La actividad de dicho DPD abarca todas las operaciones de tratamiento realizadas, también las que no estén relacionadas con el desempeño de una función pública o el ejercicio de una autoridad pública (p. ej. la gestión de una base de datos de empleados)".

administraciones autonómicas de sanidad, educación y justicia. Sin embargo, coincidimos con Alonso Suero y Díaz García[36] cuando indican que:

> Lo que no parece aconsejable que ese único delegado actúe respecto de grandes unidades u órganos con entidad y tareas claramente diferenciadas (como ocurre por ejemplo con los servicios de salud autonómicos), como veremos se ha considerado necesario en muchos servicios de salud el nombramiento específico para este ámbito. Parece claro también que, dadas las funciones del delegado de protección de datos, su adscripción dentro de la estructura de la organización deba hacerse a órganos o unidades con competencias y funciones trasversales. El nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones, y lo lógico sería proceder a su creación en la relación de puestos de trabajo, aunque en la práctica no es esto lo que ha ocurrido, dado que en muchos casos los nombramientos se han acumulado a los de los puestos de trabajo que desempeñaba su titular, compaginando, a duras penas, las funciones propias de su puesto y las "añadidas" de DPD.

b. *Tratamientos llevados a cabo por responsables y encargados cuyas actividades principales consistan en operaciones de tratamiento que, atendiendo a su naturaleza, alcance o fines, requieran de una observación habitual y sistemática de interesados a gran escala*: Para entender este supuesto es conveniente diseccionar los elementos de que consta y tener en cuenta, en primer lugar, qué se concibe por *actividad principal*. En relación con esto, el GTA29[37] establece por actividad principal la que se realiza en relación con aquellas operaciones que son imprescindibles para el desarrollo de la actividad, tanto del responsable como del encargado del tratamiento, es decir, de cara a la consecución de sus finalidades.

A las mismas tendrán que adicionarse los tratamientos de datos personales de los interesados que constituyan parte indiscutible de las actividades principales, excepto aquellas otras que sean auxiliares o no sean esenciales. En este sentido, el Grupo de Trabajo pone como ejemplo a los hospitales para ejemplificar esta "ampliación" de la actividad principal, y lo hace en los siguientes términos:

36 Elvira Alonso Suero y Elena Díaz García, "Situación del delegado de protección datos en el SNS", I+S: *Revista de la Sociedad Española de Informática y Salud*, n.º 134, 2019, p. 28. Estos autores sostienen que existen, básicamente, cinco modelos diferentes a la hora de designar a los DPO en el ámbito de las Administraciones públicas: a) un único delegado de protección de datos para toda la Administración de la comunidad autónoma; b) un delegado de protección de datos exclusivo para sanidad; c) el nombramiento de delegado de protección de datos en la figura colegiada de un comité delegado de protección de datos; d) el nombramiento de un delegado de protección de datos con el apoyo de un comité de seguridad; y e) los nombramientos de delegados de protección de datos por cada consejería y organismo autónomo (p. 29).

37 Grupo de Trabajo sobre Protección de Datos del Artículo 29, Directrices sobre los delegados de protección de datos (DPD), óp. cit., pp. 7-8.

> la actividad principal de un hospital es prestar atención sanitaria. Sin embargo, un hospital no podría prestar atención sanitaria de manera segura y eficaz sin tratar datos relativos a la salud, como las historias clínicas de los pacientes. Por tanto, el tratamiento de dichos datos debe considerarse una de las actividades principales de cualquier hospital y los hospitales deben, en consecuencia, designar un delegado de protección de datos.

A la vista de lo anterior, y en un contexto predominado por la COVID-19, podemos concluir que los hospitales, sean públicos o privados, deberán nombrar un DPD, ya que, en ambos casos, el tratamiento de datos de salud resulta indispensable para la realización de su labor principal de atención sanitaria. Para ello, será preciso, no obstante, que se cumplan también los requisitos que nos permitan afirmar que esta actividad es habitual, sistemática y a gran escala.

Lo mismo ocurre en el ámbito de las compañías de seguridad, que podrán, en su condición de encargados del tratamiento y en una situación de pandemia como la actual, tomar la temperatura de los empleados de la empresa responsable del tratamiento o de terceros ajenos a la organización, además de tratar los datos personales de todos ellos para controlar su acceso a las instalaciones[38]. Así lo corrobora de nuevo el GTA29[39] con otro ejemplo que resulta más que adecuado a estos efectos:

> Otro ejemplo sería el de una empresa de seguridad privada que lleva a cabo la vigilancia de una serie de centros comerciales privados y de espacios públicos. La vigilancia es la actividad principal de la empresa, que a su vez está ligada de manera indisociable al tratamiento de datos personales. Por tanto, esta empresa debe también designar un delegado de protección de datos.

Resulta imprescindible dibujar el perfil de un segundo criterio significativo, como es el de *observación habitual y sistemática*. El GTA29[40] ha aportado claridad respecto de esta cuestión, y considera que un tratamiento es habitual cuando incurre en alguno de estos casos (no es necesaria la concurrencia de todos ellos): a) que el tratamiento realizado sea continuado o que sea ejecutado en intervalos específicos dentro de un período establecido; b) que el tratamiento sea reiterado o recurrente en momentos previamente fijados; y c) que el tratamiento sea ejecutado de forma continua o periódica.

A su vez, para que el tratamiento de la información personal sea sistemático tendrá que reunir una serie de condiciones: a) que sea dirigido conforme

38 Raquel Poquet Catalá, "La difícil conjugación del deber de protección de datos de carácter personal y la vigilancia de la salud", en Agustín Sánchez-Toledo Ledesma (dir.), *Actas Congreso Prevencionar 2017*, Madrid: Seguridad y Bienestar Laboral, 2017.

39 Grupo de Trabajo Sobre Protección de Datos del Artículo 29, Directrices sobre los delegados de protección de datos (DPD), óp. cit., p. 8.

40 Ibíd., pp. 9-10.

a un sistema específico; b) que esté constituido de forma preestablecida, ya sea metódica u organizada; c) que forme parte integrante de un plan más amplio y general de obtención la información personal; y d) que responda a una estrategia. Como ejemplos de actividades que pueden implementar tratamientos habituales y sistemáticos se citan los siguientes: manejar una red de telecomunicaciones; ofrecer servicios de telecomunicaciones; redireccionar correos electrónicos; labores de mercadotecnia apoyadas en datos personales; confeccionar perfiles y atribuir una puntuación para las evaluaciones de riesgos (para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude o detectar blanqueo de dinero); efectuar un seguimiento de la localización, por ejemplo, a través de aplicaciones móviles; programas de fidelización; seguimiento de información personal que permita obtener el nivel de bienestar, estado físico y salud a través de dispositivos corporales; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, vehículos inteligentes, domótica, etc.

Siguiendo el contexto actual, la geolocalización de individuos afectados por la COVID-19 para controlar sus desplazamientos o el seguimiento de los datos de salud de las personas que previamente han estado hospitalizadas entrarían a la perfección dentro de este caso.

Conviene precisar el alcance de otro concepto fundamental para delimitar el alcance del artículo 37.1.b RGPD, como es el de *gran escala*. Aquí, se debe acudir a las directrices emitidas por el meritado Grupo de Trabajo[41], que establecen, ante la imposibilidad de proporcionar para todos los casos una cifra exacta que determine cuándo estamos ante un tratamiento de datos a gran escala, una serie de parámetros interpretativos: a) la cantidad de personas afectadas por el tratamiento, como dato concreto o como parte de la población a la que corresponda; b) el alcance geográfico de la actividad, donde se podrá considerar si el tratamiento se realiza a nivel territorial local, provincial, autonómico, estatal, europeo o mundial; c) el volumen de información personal tratada; y d) el tiempo o la estabilidad de la actividad de tratamiento de la información.

Conforme a lo anterior, el uso de información personal de pacientes en el desarrollo normal de la actividad de un hospital es considerado a gran escala, al igual que la forma de usar datos de geolocalización en tiempo real de pacientes afectados por el coronavirus. En cambio, no tendría esta consideración, por el menor volumen de datos y alcance de los tratamientos, el uso de la información de pacientes a través de un solo médico a título individual o las pruebas médicas realizadas por empresas de reducido tamaño para garantizar la protección de sus empleados en el entorno de trabajo.

c. *Operaciones de tratamiento implementadas a gran escala por encargados y responsables del tratamiento cuya actividad principal afecta datos especialmente protegidos o datos*

41 Ibíd., pp. 8-9.

relativos a infracciones o condenas penales: El artículo 37.1.c RGPD afronta el tratamiento de categorías especiales de datos personales, que encuentran acomodo en los artículos 9 RGPD y 9 LOPDGDD, y de información personal referente a condenas e infracciones penales, a que se refieren los artículos 10 RGPD y 10 LOPDGDD. Para que concurra este supuesto, será preciso que el tratamiento se realice a gran escala, atendiendo a los parámetros antes expuestos, algo que se producirá con toda seguridad en gran parte de las actuaciones que realicen los responsables del tratamiento para atajar o controlar la crisis sanitaria más importante de nuestros días.

Por último, conviene subrayar que, aun cuando el artículo 37.1.c RGPD emplea la letra *y*, de la visión en conjunto de la norma no podemos concluir, por carecer de sentido alguno, que sea necesaria la concurrencia cumulativa de datos especialmente protegidos y de datos personales referentes a condenas e infracciones penales, de tal suerte que debemos interpretar el texto como si dijera *o*.

A todos los supuestos anteriores se añaden, dentro del ordenamiento jurídico español, una serie de sectores profesionales que, dadas las características de las actividades que desempeñan y de las implicaciones que estas tienen en los datos personales de los interesados, deberán contar también con un DPO; o si la actividad incurre en alguna de las categorías mencionadas en el artículo 37.1 RGPD[42], lo que implica una labor interpretativa que aquí carece de sentido.

42 En concreto, y de acuerdo con el artículo 34.1 LOPDGDD, estos sectores serán los siguientes: a) los colegios profesionales y sus consejos generales; b) los centros formativos que brinden estudios en alguno de las categorías constituidas en la legislación que regula el derecho a la educación, así como las universidades privadas y/o públicas; c) los organismos que utilicen las redes y proporciones de servicios de comunicación electrónica acorde lo especificado en su legislación específica, cuando utilicen asidua y sistemáticamente información personal a gran escala; d) los sujetos que prestan servicios de la sociedad de la información al elaborar a gran escala perfiles de los clientes del servicio; e) los organismos incluidos en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito; f) las empresas que proporcionan financiación; g) las entidades aseguradoras y reaseguradoras; h) la industria de servicios de inversión, regladas por la legislación del mercado de valores; i) las empresas que distribuyen y/o comercializan energía eléctrica y/o gas natural; j) los organismos encargados de ficheros comunes que permiten evaluar la solvencia patrimonial y crédito o de ficheros comunes para gestionar y prevenir el fraude, incorporando a los responsables de ficheros regularizados por la legislación de prevención del blanqueo de capitales y de financiación del terrorismo; k) las entidades que realicen actividades de investigación comercial y de mercados, junto con las de naturaleza publicitaria y fines comerciales, en relación con tratamientos sustentados en las preferencias de los afectados o en actividades que conlleven la confección de perfiles; l) los centros sanitarios obligados de forma legal a la conservación de las historias clínicas de sus pacientes, a excepción de los profesionales de la salud que, aun hallándose de forma legal obligados a este deber de conservación, desempeñen su actividad a título individual; m) los organismos que persigan la emisión de informes comerciales que aludan a personas físicas; n) las empresas que implementen la actividad de juego a través de medios

De este modo, los centros sanitarios, públicos y privados, que, con ocasión de la COVID-19, tengan la obligación de mantener las historias clínicas de sus pacientes deberán nombrar un DPO salvo que, por no ser a gran escala, este tratamiento sea implementado por profesionales médicos de forma individual[43].

Por lo demás, conviene advertir en un hecho que, por evidente, no podemos pasar por alto. Aun cuando los artículos 37 RGPD y 34 LOPDGDD resultan aplicables tanto a los encargados como a los responsables del tratamiento, el hecho de que estos tengan que nombrar un delegado de protección de datos no determina la necesidad de que aquellos deban (aunque sí pueda resultar conveniente) proceder de igual modo si no incurren en ninguno de los supuestos citados en el RGPD o en la LOPDGDD.

Asimismo, y más allá de los casos de designación obligatoria pormenorizadamente diseccionados, cabe también la posibilidad, en virtud del principio de responsabilidad proactiva (artículo 5.2 RGPD), de proceder a este nombramiento de forma voluntaria. Ahora bien, en estos casos, la exigibilidad de las obligaciones impuestas por los artículos 37 a 39 RGPD y 34 a 37 LOPDGDD será exactamente la misma que si se hubiera integrado al DPO de forma preceptiva[44]. La designación de un DPD puede resultar de gran utilidad y venir justificado en determinados casos: en primer lugar, atendiendo a la dificultad y complejidad jurídica del tratamiento, el requerir de un experto en materia de protección de datos que sea capaz de aconsejar de forma constante a encargados y responsables del tratamiento. En segundo lugar, teniendo en consideración las sanciones, ciertamente más elevadas que en la normativa anterior, que recoge

electrónicos, interactivos, informáticos y telemáticos, con base en las normas reguladoras del juego; o) las compañías de seguridad privada; y p) las federaciones deportivas, siempre que empleen información de menores de edad.

43 De acuerdo con el artículo 14.1 LAP, "La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro". A su vez, los apartados 1 y 2 del artículo 15 LAP establecen el contenido mínimo que debe recoger la historia clínica de los pacientes, lo que permite conocer la amplitud de los datos de salud tratados al efecto; en concreto, dispone este precepto, que "incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente", en concreto: a) la documentación relativa a la hoja clínico-estadística; b) la autorización de ingreso; c) el informe de urgencia; d) la anamnesis y la exploración física; e) la evolución; f) las órdenes médicas; g) la hoja de interconsulta; h) los informes de exploraciones complementarias; i) el consentimiento informado; j) el informe de anestesia; k) el informe de quirófano o de registro del parto; l) el informe de anatomía patológica; m) la evolución y planificación de cuidados de enfermería; n) la aplicación terapéutica de enfermería; ñ) el gráfico de constantes; y o) el informe clínico de alta.

44 Manuel Vallín López, "Apuntes sobre el delegado de protección de datos y la administración general de Euskadi", *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, n.º 14, 2018, p. 95.

la regulación actual (artículos 83 RGPD y 70 a 78 LOPDGDD). En tercer lugar, constatando la progresiva concienciación de las personas en defensa de su derecho fundamental a la protección de sus datos personales, que conllevará, previsiblemente, un aumento en el número de procedimientos de ejercicio de los derechos que les son reconocidos.

Comoquiera que sea, de producirse este nombramiento, ya sea de forma voluntaria u obligatoria, de un delegado de protección de datos, los encargados y responsables del tratamiento notificarán a la Agencia Española de Protección de Datos (en adelante, AEPD) o, si procede, a las autoridades autonómicas de protección de datos (en adelante, AAPD), con diez días de plazo, tales designaciones, así como, también, los ceses y nombramientos que se produzcan. A tal efecto, estas agencias conservarán, en el área de sus correspondientes competencias, una lista permanentemente revisada de DPD, a la que se podrá acceder mediante medios electrónicos (artículo 34, 3 y 4, LOPDGDD).

1.2 Posición dentro de la organización: imparcialidad como elemento esencial

La posición que ha de ocupar el DPD dentro de toda organización que proceda, voluntaria u obligatoriamente, a su nombramiento, se incluye en los artículos 38 RGPD y 36 LOPDGDD. La ejecución de esta normativa conlleva cumplir con las siguientes exigencias[45]:

– Se establece que el DPO debe intervenir de manera apropiada en cualquier decisión referente al uso de información personal de los afectados. Para ello, se ha de posibilitar que el DPD posea un acceso apropiado, en tiempo y forma, a cualquier decisión relativa a la protección de datos dentro de la entidad a la que pertenece.

– Además, el responsable o encargado del tratamiento que incorpore al DPO deberá poner a su disposición los recursos que el delegado de protección de datos necesite para poder ejercer su función de forma adecuada y efectiva, habiendo de tener acceso a la información personal y a las operaciones de tratamiento que se implementen en el seno de la entidad, que no podrá oponerse a ello so pretexto de la presencia de algún deber de secreto y/o confidencialidad, ya que este deber afecta también al propio DPD (artículo 38.5 RGPD).

– Se señala también que el DPO deberá actuar con independencia, no recibiendo instrucción alguna en el desempeño de sus funciones y rindiendo cuentas únicamente a nivel jerárquico superior. Esto implica que el delegado de protección de datos no podrá recibir órdenes del encargado o del responsable

45 Sobre esta cuestión, véase Esther Botella Pamies, "Posición del delegado de protección de datos", óp. cit., pp. 194-197; Miguel Ángel Davara Rodríguez, "Posición y funciones del delegado de protección de datos", *Actualidad Administrativa*, n.º 1, 2018.

del tratamiento que lo designe ni, en consecuencia, podrá ser suspendido o sancionado por el mero hecho de haber actuado independientemente, siempre que, huelga decirlo, no incurra en estafa o negligencia respecto de este ejercicio.

– Es también una exigencia, ligada al punto anterior, el deber para la organización responsable de proteger la autonomía del DPD en el área organizativa, por lo que tendrá que evitar toda actuación que pueda implicar en este un conflicto de intereses.

– En todo caso, el DPD deberá cumplir fielmente con el deber de confidencialidad y con el deber de secreto profesional.

Del total de exigencias citadas, destaca fundamentalmente aquella que establece que la organización obligatoriamente deberá apoyar en su totalidad al delegado de protección de datos, ya que, en caso contrario, si el organismo no se compromete y no otorga los recursos que propicien el buen cumplimiento de sus labores, el DPD, aun designado formalmente, no dispondrá de funcionalidad práctica.

1.3. Cometidos en términos de *numerus apertus*, reforzados en tiempos de emergencia sanitaria

Respecto a las labores del DPD, el artículo 39.1 RGPD asigna aquellas que, como mínimo, debe asumir[46]:

– La primera consistirá en notificar e instruir al encargado o al responsable del tratamiento y a aquellas personas empleadas que se ocupen del tratamiento de las responsabilidades que les competen en el ámbito de la protección de datos personales (como, en nuestro caso, la regulación en materia sanitaria que necesariamente se habrá de poner en estrecha relación con el RGPD y la LOPDGDD).

– La segunda, fundamental también en su labor de control, residirá en comprobar de forma regular que toda la normativa anterior, comunitaria o nacional, sea cumplida en el interior de la organización, con vistas a asegurar la privacidad de los afectados. Se incluye aquí una óptima distribución de la responsabilidad entre las personas implicadas y una apropiada formación, sensibilización y aprendizaje del personal que participa en la realización de

46 Sobre esta cuestión, véanse Borja Adsuara Varela, "El delegado de protección de datos: funciones y funcionalidad en el ámbito local", en María Concepción Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el Reglamento Europeo*, Madrid: Wolters Kluwer, 2018, pp. 293-330; Esperanza Macarena Sierra Benítez, "El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, n.º 1, 2018, pp. 236-260; Pere Simón Castellano, *El desempeño de las funciones de delegado de protección de datos: gestión de procesos críticos y casos prácticos*, Madrid: Wolters Kluwer, 2018.

actividades de tratamiento, amén de una favorable gestión de las auditorías que tengan lugar en el seno del responsable o del encargado del tratamiento, dependiendo del caso.

– La tercera, de naturaleza más orientadora, se traducirá en el deber de asesorar adecuadamente, en el momento en el que sea requerido por la organización o entidad que lo haya elegido, en la ejecución de las evaluaciones de impacto que proceda realizar de acuerdo con lo señalado en los artículos 35 y 36 RGPD.

– La cuarta, propiamente de intermediación, implicará ejercer como interlocutor de los responsables o de los encargados del tratamiento en cualquier comunicación establecida con la AEPD y las AAPD. En este caso, el DPD tiene la potestad de inspeccionar los procedimientos respecto a la seguridad de la información personal y recomendar y asesorar en el ámbito de sus competencias.

– La quinta, inmanente a la anterior, establece la necesidad de cooperar e intervenir como punto de referencia de los encargados o de los responsables del tratamiento frente a las reivindicaciones que interpongan los afectados antes de instar la intervención de la autoridad de control nacional o autonómica[47]. Por tanto, en el momento en que la organización, pública o privada, nombre un DPO, el afectado podrá, previamente a la incoación de reclamaciones contra aquella, acudir a esta figura, la cual deberá notificar al interesado la respuesta acordada en nombre de la entidad en un período no superior a dos meses, que comenzará a contar desde el momento en el que la reclamación haya sido recibida. Igualmente, cuando el interesado interponga una reclamación frente a la AEPD o, en su caso, ante las AAPD, estas podrán enviar la misma al DPD para que emita una respuesta en un plazo de treinta días. Luego de ese término, si no hubiese emitido comunicación alguna, la autoridad de control competente seguirá con el proceso según lo previsto en las normas aplicables. El proceso a seguir ante la AEPD es el dispuesto en el Título VIII LOPDGDD y en los preceptos de desarrollo; por su parte, las comunidades autónomas tendrán que disciplinar también el método que corresponda frente a sus AAPD. Las actuaciones implementadas por el DPD frente a la autoridad de control se encuadran dentro de lo que el GTA29[48] define como el *papel de facilitador* del delegado de protección de datos. Efectivamente, al cumplir estas labores, el DPD atribuye a la autoridad de control el poder de acceder, en muchos casos de forma indispensable, a toda la documentación e información que esta necesita para el cumplimiento de sus obligaciones, en especial aquellas vinculadas a su potestad en materia de investigación o autorización. Todo bajo la responsabilidad continua del DPD de

47 Juan Francisco Rodríguez Ayuso, *Control externo de los obligados por el tratamiento de datos personales*, Barcelona: Bosch, 2020, pp. 21-75.

48 Grupo de Trabajo Sobre Protección de Datos del Artículo 29, Directrices sobre los delegados de protección de datos (DPD), óp. cit., p. 20.

cumplir con el precitado deber de secreto y confidencialidad, lo que parece plenamente coherente con esta cooperación a que nos referimos.

– La sexta, no menos importante, exigirá del DPO el registro y la inmediata comunicación al órgano que administre y dirija la organización a la que pertenece el DPO o donde este brinde sus servicios profesionales que existe una vulneración importante en materia de privacidad.

– Por último, aunque no está recogida por no ser imprescindible dentro del elenco de funciones del artículo 39 RGPD, cabe distinguir la importante labor que el DPD puede desempeñar elaborando y manteniendo actualizado el registro de las actividades de tratamiento, contemplado en los artículos 30 RGPD y 31 LOPDGDD. En este contexto, el DPO habrá de coordinar, junto con el responsable o el encargado del tratamiento, el registro de las actividades de tratamiento dentro de la organización, realizando un seguimiento constante y periódico del mismo de cara a cumplir con las exigencias impuestas por la regulación sobre protección de datos.

Más allá de lo anterior, en el derecho español el DPD habrá de efectuar estas funciones con la máxima diligencia posible, advirtiendo los riesgos de toda índole inherentes a las operaciones de tratamiento (artículo 32 RGPD) y valorando, en cada supuesto, la naturaleza, el alcance y los fines del tratamiento de los datos personales. Hemos de considerar lo anterior, no como una obligación, sino como una forma de ejecutar las labores que le competen. Por consiguiente, el DPD deberá de dar preferencia a aquellos tratamientos que supongan un riesgo más elevado, tan pronto como hayan sido analizados y relacionados con su naturaleza, alcance y finalidades, sin obviar aquellas otras actividades expuestas a un menor riesgo, pero que habrá de abordar y que deberán tener respuesta.

Esta óptica basada en el riesgo deviene esencial en relación con el cumplimiento de los preceptos ínsitos en la normativa reguladora de la privacidad de los interesados, ya que, independientemente de las labores de asesoramiento y supervisión acometidas por el DPD, es esencial que la organización, igualmente con el apoyo del delegado de protección de datos, tenga la posibilidad de adelantarse al riesgo que presenten las distintas operaciones de tratamiento[49]. Por ende, deben considerarse las características propias de la organización, pues, situándolo en la excepcionalidad derivada de la crisis sanitaria actual, nunca será lo mismo un centro de atención hospitalaria que realice el tratamiento de notables cantidades de información de salud de personas infectadas que

49 Esto guarda relación con lo establecido por la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al* RGPD, 2016, que dispone que determinadas medidas establecidas por la nueva regulación únicamente resultarán aplicables en aquellos supuestos en que se desprenda la existencia de un riesgo elevado en relación con el tratamiento para los derechos y libertades de los interesados; en cambio, otras habrán de modularse atendiendo al nivel y al tipo de riesgo que conlleve el tratamiento.

otros que tan solo atiendan una pequeña cantidad de datos menos invasivos para la privacidad.

Una vez analizados los contornos esenciales y controvertidos que rodean la incorporación del DPO de forma preceptiva en el seno de la Unión Europea, resulta imprescindible completar el estudio de esta materia determinando los requisitos y exigencias que, en torno a su nombramiento, se contienen en los pliegos de contratación pública. Sobre esta cuestión pivota el siguiente epígrafe.

2. LA EXISTENCIA Y CUALIFICACIÓN DEL DPD EN LOS PLIEGOS DE LA CONTRATACIÓN

Podemos vislumbrar dos circunstancias esenciales en las que los pliegos de contratación pública podrán llegar a exigir determinadas condiciones por parte de quienes intervienen como licitadores, estando todas ellas vinculadas con la figura del DPO. De un lado, están aquellos casos mencionados en el epígrafe anterior, en los que no proceda su nombramiento de forma obligatoria (artículo 37.1 RGPD y artículo 34.1 LOPDGDD) y, de otro lado, está la consideración de su cualificación, ya sea preceptiva o voluntaria su designación.

En el caso de que se considere que el sector en el que el DPO desarrolla el objeto del contrato presenta importantes efectos y repercusiones en el ámbito de la seguridad de información personal, por cuanto que implica el tratamiento de información privada a una escala mayor o porque afecta a categorías especiales de datos personales, pueden concurrir dos posibilidades. Una primera alternativa consiste en la incorporación al pliego de cláusulas administrativas como un criterio de solvencia al amparo y sobre la base de los epígrafes 1.b y 3 del artículo 90 LCSP. En virtud de estas disposiciones, se determina de manera objetiva la ostentación por el licitador de una determinada organización que haga presumir el respeto en la ejecución del contrato, cual es el derecho fundamental a la protección de datos personales, emanado del artículo 18 de la Constitución española. Una segunda alternativa radica en la ponderación positiva de esta circunstancia en sede de pautas de concesión, el fundamento de las circunstancias de carácter social enunciadas con carácter de *numerus apertus* en el artículo 145.2.1º LCSP, que dispone que la adjudicación de los contratos se realizará empleando múltiples criterios de adjudicación, sobre la base de la mejor calidad relación-precio. Al amparo de esta afirmación, sostiene que esta relación se evaluará con arreglo a criterios económicos y cualitativos, donde destaca la calidad, incluido el valor técnico, las características estéticas y funcionales, la accesibilidad, el diseño universal o diseño para todas las personas usuarias, las características sociales, medioambientales e innovadoras, y la comercialización y sus condiciones.

En ambos casos, sería procedente la inclusión, en los contratos cuya ejecución se vaya a prolongar en el tiempo (entendemos que la mayor parte en la que el análisis de impacto conduzca a la conclusión anterior), de un requisito

esencial de actuación en el cual se acredite el mantenimiento durante todo este intervalo en la persona del DPD e, incluso, la posibilidad de mantener actualizadas y compartidas las comunicaciones que terceros le puedan hacer llegar.

En cuanto al segundo de los supuestos, se considera factible la posesión por el DPD de la sociedad o de una determinada cualificación o nivel de estudios que concrete la parquedad con la que se expresan los artículos 37.5 y 35 LOPDGDD. Lo anterior, en cualquier sector[50] en el que la relevancia cuantitativa y/o cualitativa de los datos personales tratados por el eventual adjudicatario en el desarrollo del objeto del contrato se pueda exigir vía criterio de solvencia técnica o de ponderación positiva en los criterios de adjudicación. Y esto puede producirse, bien estableciendo un nivel de horas de formación especializada mínimas u obteniendo un determinado título o grado de estudios, en el caso de los criterios de solvencia; bien prorrateando la concesión de una determinada puntuación asignada a este aspecto en función de su grado de cumplimiento, en sede se criterios de adjudicación.

Atendiendo a las exigencias de los conocimientos y formación específica a acreditar e, incluso, como medio de justificación de este apartado, resulta de gran utilidad la consulta del Esquema de certificación de DPD de la AEPD[51]. En este caso, se refuerza, en todo momento, la necesidad de salvaguardar la neutralidad certificadora, de modo que no se indique en el pliego tanto el cumplimiento de un determinado requisito formal, como la búsqueda de un determinado elemento sustantivo que pueda ser acreditado (si bien puede referir, no solo el contenido del título, sino la forma de su evaluación, por ejemplo, a través de terceros especialistas independientes al centro de matriculación) por medio de determinados certificados, como el planteado por la AEPD, o que pudiera otorgar cualquier otra entidad académica o formativa.

– En línea con estas posibles cláusulas, la introducción de una condición especial de ejecución vuelve a ser conveniente a la hora de acreditar, a la finalización de la ejecución del contrato, el mantenimiento de esta circunstancia durante toda ella.

Por último, teniendo en consideración, en la línea del apartado segundo del artículo 202[52] LCSP, las condiciones especiales de ejecución como instrumento

50 Sobre la base de los artículos 90 y 145 LCSP. Ya sea preceptivo o no el nombramiento del DPD.

51 Disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/delegado-de-proteccion-de-datos/certificacion

52 De acuerdo con este apartado: "Estas condiciones de ejecución podrán referirse, en especial, a consideraciones económicas, relacionadas con la innovación, de tipo medioambiental o de tipo social.

En particular, se podrán establecer, entre otras, consideraciones de tipo medioambiental que persigan: la reducción de las emisiones de gases de efecto invernadero, contribuyéndose así a dar cumplimiento al objetivo que establece el artículo 88 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible; el mantenimiento o mejora de los valores medioambientales

independiente para el fomento de esta mayor calidad de la prestación objeto del contrato en su vertiente de cuidado de la protección de datos personales, se podría instituir en el primero de los bloques de casos planteados la obligación de nombrar al DPD en el supuesto de resultar adjudicatario del contrato (con una menor distorsión de la competencia que en el caso de su inclusión como criterio de solvencia), o bien, en el segundo de dichos bloques, la necesidad de llevar a cabo y acreditar una determinada formación continua por parte de esta figura.

CONCLUSIONES

A lo largo del presente estudio ha sido posible advertir los esfuerzos que, en el seno de la Unión Europea y dentro del profundo proceso transformador a que se haya expuesta, se han implementado para fortalecer y fomentar la cohesión del territorio comunitario por medio de la renovación y/o configuración de elementos de naturaleza económica, social y jurídica. En este último ámbito, uno de los retos fundamentales reside en la redacción de los pliegos de la contratación, más concretamente en la introducción de cláusulas sociales focalizadas en garantizar el derecho fundamental de los afectados a la protección de sus datos personales como elemento central en la garantía de su privacidad.

que puedan verse afectados por la ejecución del contrato; una gestión más sostenible del agua; el fomento del uso de las energías renovables; la promoción del reciclado de productos y el uso de envases reutilizables; o el impulso de la entrega de productos a granel y la producción ecológica.

Las consideraciones de tipo social o relativas al empleo, podrán introducirse, entre otras, con alguna de las siguientes finalidades: hacer efectivos los derechos reconocidos en la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad; contratar un número de personas con discapacidad superior al que exige la legislación nacional; promover el empleo de personas con especiales dificultades de inserción en el mercado laboral, en particular de las personas con discapacidad o en situación o riesgo de exclusión social a través de Empresas de Inserción; eliminar las desigualdades entre el hombre y la mujer en dicho mercado, favoreciendo la aplicación de medidas que fomenten la igualdad entre mujeres y hombres en el trabajo; favorecer la mayor participación de la mujer en el mercado laboral y la conciliación del trabajo y la vida familiar; combatir el paro, en particular el juvenil, el que afecta a las mujeres y el de larga duración; favorecer la formación en el lugar de trabajo; garantizar la seguridad y la protección de la salud en el lugar de trabajo y el cumplimiento de los convenios colectivos sectoriales y territoriales aplicables; medidas para prevenir la siniestralidad laboral; otras finalidades que se establezcan con referencia a la estrategia coordinada para el empleo, definida en el artículo 145 del Tratado de Funcionamiento de la Unión Europea; o garantizar el respeto a los derechos laborales básicos a lo largo de la cadena de producción mediante la exigencia del cumplimiento de las Convenciones fundamentales de la Organización Internacional del Trabajo, incluidas aquellas consideraciones que busquen favorecer a los pequeños productores de países en desarrollo, con los que se mantienen relaciones comerciales que les son favorables tales como el pago de un precio mínimo y una prima a los productores o una mayor transparencia y trazabilidad de toda la cadena comercial".

De entre estas cláusulas, adquieren preeminencia aquellas que exigen la incorporación, en el ámbito público, de la figura del DPO (o DPD, como se conoce en el derecho español), instrumento básico para la consecución del objetivo de las Administraciones públicas de controlar y supervisar el tratamiento de datos personales realizado por parte del responsable del tratamiento en la consecución de los fines marcados y previamente definidos. Al respecto, se han examinado los elementos definitorios más relevantes en cuanto a su nombramiento, su posición dentro de la organización en la que interviene y sus funciones.

Se constataron luego las circunstancias que, recogidas en los pliegos de contratación pública, pueden estar vinculadas con el DPD: a) la valoración de su designación proactiva; y b) la atención a su cualificación como elemento definitorio de su presumible adecuada actuación. En relación con la primera, cuando la labor del DPO presente, dentro del contrato, una incidencia relevante en el ámbito de la seguridad de información personal por implicar el tratamiento de información privada a una escala mayor o por afectar a datos especialmente protegidos, se podrá incorporar al pliego de cláusulas administrativas como un criterio de solvencia o se podrá ponderar positivamente esta circunstancia en el momento de la concesión. En cuanto a la segunda, es posible concluir que se podrá requerir al DPO que vaya a ser designado una determinada cualificación o formación, a fin de acreditar que podrá desempeñar con solvencia la función a la que está llamado, especialmente atendiendo a la relevancia cuantitativa y/o cualitativa de los datos personales objeto de tratamiento; al respecto, se impone la neutralidad de la entidad que haya de certificar esta cualificación y la necesidad de determinar el elemento a certificar.

BIBLIOGRAFÍA

Adsuara Varela, Borja. "El delegado de protección de datos: funciones y funcionalidad en el ámbito local". En María Concepción Campos Acuña (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el Reglamento Europeo* (pp. 293-330). Madrid: Wolters Kluwer, 2018.

Agencia Española de Protección de Datos. "El impacto del Reglamento general de protección de datos sobre la actividad de las Administraciones públicas", 2016.

Alonso Suero, Elvira y Elena Díaz García. "Situación del delegado de protección datos en el SNS". *I+S: Revista de la Sociedad Española de Informática y Salud*, n.º 134, 2019, pp. 27-31.

Bacaria Gea, Júlia. "El DPD en el sector Administración Local". En Pere Simón Castellano y Jordi Bacaria Martrus (coords.), *Las funciones del delegado de protección de datos en los distintos sectores de actividad* (pp. 111-125). Madrid: Wolters Kluwer, 2020.

Botana García, Gema Alejandra. "La formación del delegado de protección de datos (DPO)". *Actualidad Civil*, n.º 5, 2018.

Botella Pamies, Esther. "Posición del delegado de protección de datos". En Mónica Arenas Ramiro y Alfonso Ortega Giménez (dirs.) *Protección de datos: comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)* (pp. 194-197). Madrid: Sepin, 2019.

Davara Rodríguez, Miguel Ángel. "El delegado de protección de datos". *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal*, n.º 24, 2017, pp. 3091-3097.

Davara Rodríguez, Miguel Ángel. "Posición y funciones del delegado de protección de datos". *Actualidad Administrativa*, no. 1. 2018.

Díaz-Romeral Gómez, Alberto. "Protección de datos y contratación pública". En Isabel Gallego Córcoles y Eduardo Gamero Casado (coords.), *Tratado de contratos del sector público* (pp. 422-466). Valencia: Tirant lo Blanch, 2018.

Gimeno Feliú, José María. "El nuevo paquete legislativo comunitario de contratación pública: principales novedades. La orientación estratégica de la contratación pública". En AA. VV. *Las nuevas directivas de contratos públicos y su transposición* (pp. 15-127). Madrid: Marcial Pons, 2016.

González Calvo, Manuel. "La nueva figura del delegado de protección de datos". *Actualidad jurídica Aranzadi*, no. 939, 2018.

Messía de la Cerda Ballesteros, Jesús Alberto. "Consideraciones y perspectivas del Delegado de Protección de Datos". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 47, 2018.

Miranda Boto, José María. "Contratación pública y cláusulas de empleo y condiciones de trabajo en el Derecho de la Unión Europea". *Lex Social: Revista Jurídica de los Derechos Sociales*, n.º 2, 2016, pp. 69-91.

Ordiozola Alén, Miguel. "El delegado de protección de datos (DPD): ¿qué entidades están obligadas a designarlo y cuáles son las funciones y perfil de esta figura clave en el nuevo modelo de privacidad?". *Revista CADE: doctrina y jurisprudencia*, n.º 52, 2019, pp. 61-68.

Pardo López, María Magnolia. "Mención de criterios sociales y medioambientales en la definición del objeto del contrato". En María Magnolia Pardo López y Alfonso Sánchez García (dirs.), *Inclusión de cláusulas sociales y medioambientales en los pliegos de contratos públicos: guía práctica profesional* (pp. 49-62). Cizur Menor: Aranzadi, 2019.

Poquet Catalá, Raquel. "La difícil conjugación del deber de protección de datos de carácter personal y la vigilancia de la salud". En Agustín Sánchez-Toledo

Ledesma, (dir.) *Actas Congreso Prevencionar 2017*, Madrid: Seguridad y Bienestar Laboral, 2017.

Recio Gayo, Miguel. "El delegado de protección de datos". En José Luis Piñar Mañas (dir.), *Reglamento General de Protección de Datos* (pp. 367-388). Madrid: Reus, 2006.

Rodríguez Ayuso, Juan Francisco. *Control externo de los obligados por el tratamiento de datos personales*. Barcelona: Bosch, 2020.

Sierra Benítez, Esperanza Macarena. El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, n.º 1, 2018, pp. 236-260.

Simón Castellano, Pere. *El desempeño de las funciones de delegado de protección de datos: gestión de procesos críticos y casos prácticos*. Madrid: Wolters Kluwer, 2018.

Vallín López, Manuel. "Apuntes sobre el delegado de protección de datos y la administración general de Euskadi". *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, n.º 14, 2018, pp. 92-105.