G A _ P

Gómez-Acebo & Pombo

La independencia del delegado de protección de datos y el conflicto de intereses como límites a su nombramiento

Francisco Pérez Bes

Of counsel

Director del Área de Derecho y Economía Digital de Gómez-Acebo & Pombo

Cada vez son más las empresas que están obligadas a nombrar un delegado de protección de datos cuando ya han incorporado a un responsable de la información por estar certificadas conforme al Esquema Nacional de Seguridad. Esta situación puede plantear ciertos problemas de incompatibilidad entre ambos.

El Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos —comúnmente conocido como Reglamento General de Protección de Datos—), introdujo, por primera vez, la figura del delegado de protección de datos (DPD), figura de nombramiento obligatorio en aquellas empresas en las que concurran determinados requisitos establecidos en la ley.

En España, el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, aprobado mediante el Real Decreto 3/2010, de 8 de enero, regulaba —en su artículo 10— la figura del responsable de la información diferenciándolo de la del responsable del servicio y de la del responsable de la seguridad.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

Y, aunque su adopción es obligatoria para la Administración Pública, son cada vez más numerosas las empresas privadas que optan por adecuar sus sistemas de seguridad para poder certificarse conforme al referido esquema, lo que les permite acreditar que el nivel de seguridad de los sistemas de la compañía ha cumplido las exigencias marcadas por los procedimientos establecidos en dicha norma[1].

Esto supone que, en aquellas empresas privadas que hayan obtenido la certificación de conformidad con el Esquema Nacional de Seguridad, podrían concurrir las figuras del responsable de seguridad y del delegado de protección de datos, lo que plantea una duda jurídica acerca de su posible asunción por una misma persona.

En este sentido, hay que señalar que, de conformidad con el Esquema Nacional de Seguridad, la figura del responsable de seguridad que señala su artículo 10 está sometida a las instrucciones del responsable de la información, pues es éste el que tiene atribuida la competencia de determinar los requisitos de la información tratada.

En cuanto al delegado de protección de datos, el mencionado reglamento señala que sus actuaciones deben regirse por los principios de independencia e imparcialidad. Así, en cuanto a su actuación independiente, el artículo 38.3 de la misma norma obliga al responsable y al encargado del tratamiento a garantizar que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones, mientras que el artículo 38.6 recoge el principio de imparcialidad de dicho delegado cuando afirma que el responsable o encargado del tratamiento garantizará que sus funciones y cometidos no den lugar a conflicto de intereses.

En este mismo sentido se expresa la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando exige asegurar la independencia de las personas físicas que actúen como delegados de protección de datos dentro de una organización. Así se recoge expresamente en el artículo 36 cuando en su apartado 2 señala que «se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses».

En relación con el asunto del conflicto de intereses, podemos traer a colación una controversia surgida en Alemania en el año 2016 cuando la autoridad de protección de datos alemana (FDPA) interpretó que el delegado de protección de datos no debía desempeñar otras funciones que pudieran entrar en conflicto con las obligaciones de control que la normativa alemana de protección de datos reservaba para aquél.

En este caso, una empresa alemana domiciliada en Baviera había nombrado delegado de protección de datos a su director de Tecnología al considerar que cumplía la exigencia legal de contar con suficiente conocimiento de la regulación de protección de datos, además de las de ser independiente *(independent)* e imparcial *(reliable)*.

[1] https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/empresas-certificadas

Ante esta situación, la autoridad bávara de protección de datos requirió a la empresa para que sustituyera a dicho delegado, pues consideraba que no cumplía la obligación de imparcialidad. El argumento empleado por la mencionada autoridad era que el cargo de director de Tecnología de la empresa era incompatible con el cargo de delegado de protección de datos, ya que, a la hora de revisar sus actuaciones y garantizar que las que llevaba a cabo como director cumplían la normativa de protección de datos, se convertía en juez y parte. Y este control de las actuaciones del director de Tecnología por él mismo —interviniendo como delegado— no es compatible con la expectativa de objetividad e independencia que se tiene de un delegado de protección de datos conforme al Reglamento 2016/679 y a la normativa alemana.

La empresa hizo caso omiso del requerimiento del regulador bávaro, por lo que éste le impuso una sanción.

Una de las cuestiones que mostró esta resolución de la autoridad bávara tenía que ver con el alcance y los límites del conflicto de intereses y con la independencia del delegado de protección de datos en las empresas, ya que el supuesto que se planteó en dicho caso podría llegar a darse también en alguna otra figura dentro de la organización si aquélla, dentro de sus competencias y actuaciones, tuviera responsabilidad en un tratamiento de datos cuando éste fuera relevante, bien por volumen, bien debido a la sensibilidad de los datos manejados.

Esta cuestión quedó resuelta al año siguiente cuando las directrices sobre los delegados de protección de datos adoptadas por el Grupo de Trabajo del artículo 29, el 5 de abril del 2017, afirmaban que «aunque los DPD puedan tener otras funciones [...], el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales».

Añadían dichas directrices que, en cuanto a los posibles cargos con funciones en conflicto con la del delegado de protección de datos, se encuentran los puestos de alta dirección, pero también otros cargos inferiores si éstos pueden decidir acerca de los fines y medios del tratamiento.

Especialmente destacables son las prácticas recomendables que ahí se definen y que ayudan a una organización con delegado de protección de datos a evitar cualquier tipo de incompatibilidad con otro cargo, como podría ser, en el caso que aquí nos ocupa, el del responsable de seguridad que prevé el Esquema Nacional de Seguridad.

En relación con la situación que aquí se expone, también la Agencia Española de Protección de Datos tuvo la oportunidad de pronunciarse en un informe de su gabinete jurídico, precisamente a raíz de una consulta que planteaba la posible compatibilidad entre el delegado de protección de datos y el responsable de seguridad. La conclusión a la que nuestro regulador llegó en esta cuestión es clara: con carácter general, debe existir la necesaria separación

entre el delegado de protección de datos y el responsable de seguridad del Esquema Nacional de Seguridad, sin que —salvo en situaciones excepcionales— sus funciones puedan recaer en la misma persona u órgano colegiado, precisamente para poder garantizar que se cumplen las obligaciones de independencia y ausencia de los conflictos de intereses recogidos en el Reglamento General de Protección de Datos.