

N/REF: 0034/2023

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en el Preámbulo de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

El proyecto tiene por objeto crear una nueva política de protección de datos personales en el ámbito de la Generalitat Valenciana, que incluye además la estructura organizativa y funcional, de un lado, referida al aparato administrativo del responsable del tratamiento, y de otro lado, al delegado de protección de datos.

Como antecedente debe indicarse que la creación de la Delegación y las subdelegaciones de protección de datos de la Generalitat se llevó a cabo a través del Decreto 195/2018, de 31 de octubre, por el que se aprobó el reglamento orgánico y funcional de la Conselleria de Transparencia, Responsabilidad Social, Participación y Cooperación, actualmente derogado por el Decreto 179/2020, de 30 de octubre, del Consell, de aprobación Reglamento orgánico y funcional de la Conselleria de Participación, Transparencia, Cooperación y Calidad Democrática.

El Proyecto de Decreto justifica la adecuación de un nuevo marco normativo por los cambios que el RGPD y la LOPDGDD introducen, así como la constante evolución tecnológica, que hacen necesaria la adopción de una nueva política para la protección de datos personales, que sea común en sus aspectos básicos para toda la administración del Consell y su sector público instrumental y que esté coordinada con las exigencias que en seguridad de la información establece el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

En consecuencia, mediante el Proyecto de Decreto sometido a informe se pretende aprobar política general, estructura organizativa y asignación de funciones en materia de protección de datos en la administración del Consell y su sector público instrumental, sin perjuicio de su desarrollo y concreción en cada Consejería y entidad de su sector público.

En lo que a la materia de protección de datos personales se refiere, la norma a la que debe ajustarse el proyecto sometido a consulta al RGPD y a la LOPDGDD.

Además, teniendo en cuenta que estamos ante la regulación por parte de la administración de una comunidad autónoma de aspectos relacionados con un derecho fundamental, de acuerdo con el artículo 18.4 de la CE, será preciso analizar la adecuación de la misma al reparto competencial que deriva del bloque de constitucionalidad.

I

Como punto de partida debe ponerse de manifiesto que una de las consecuencias de la naturaleza jurídica de los Reglamentos Europeos (en tanto derecho europeo) es que son de aplicación directa y por tanto no necesitan de norma nacional de transposición. (El efecto directo del derecho europeo de consagra en la Sentencia del Tribunal de Justicia de 5 de febrero de 1963 y en concreto respecto de los Reglamentos hace lo propio la Sentencia del Tribunal de Justicia de 14 de diciembre de 1971).

Ahora bien, debe tenerse en cuenta el Preámbulo de la LOPDGDD, que a este respecto indica que:

(...) Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión. En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar

situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación... (...).

En efecto, esta doctrina ya la recogía el Dictamen del Consejo de Estado nº 757/2017 sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, indicaba que:

Por otra parte, la entrada en vigor de un Reglamento obliga a llevar a cabo una segunda tarea de depuración del ordenamiento nacional, del que deben igualmente eliminarse cuantas disposiciones hayan devenido redundantes como consecuencia del efecto directo de aquél, en la medida en que puedan poner en cuestión esa aplicación directa del Reglamento.

En fin, la adaptación de la legislación nacional puede también exigir, en algunos casos puntuales, la adopción de nuevas disposiciones llamadas a completar o aclarar la regulación europea. La aplicabilidad directa del Reglamento no excluye, en efecto, esa labor puntual de complemento de la normativa de los Estados miembros. Así lo reconoce expresamente la jurisprudencia comunitaria, al destacar que, "si bien, en razón de la propia índole de los Reglamentos y de su función en el sistema de las fuentes del Derecho comunitario, sus disposiciones tienen, por lo general, un efecto inmediato en los ordenamientos jurídicos nacionales, sin que sea preciso que las autoridades nacionales adopten medidas de aplicación, algunas de sus disposiciones pueden requerir, para su ejecución, la adopción de medidas de aplicación por los Estados miembros" (STJCE de 11 de enero de 2001, Monte Arcosu, C-403/98, apartado 26); y, más concretamente, la aplicabilidad directa de un Reglamento no se opone a que el mismo "faculte a una Institución comunitaria o a un Estado miembro para dictar medidas de aplicación" (STJCE de 27 de septiembre de 1979, Eridiana, 230/78, apartado 34).

Así lo hace el Reglamento general de protección de datos. Pese a su intensa vocación armonizadora, el Reglamento contiene al menos 56 remisiones de diverso alcance al Derecho de los Estados miembros, permitiendo a estos adaptar la regulación europea, en distintos casos, al contexto nacional, o fijar exenciones, derogaciones o condiciones específicas para determinadas categorías de tratamiento de datos; incluso, en algunos supuestos puntuales, el Reglamento confiere carácter preceptivo a esa labor normativa de desarrollo por los Estados miembros (el artículo 51, en primer lugar, prevé que cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades de control supervisar la aplicación del Reglamento; y el artículo 84 prevé que establezcan "las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento").

La jurisprudencia también ha aceptado, aunque en términos restrictivos, la validez de habilitaciones implícitas a favor de los Estados miembros en las normas de un Reglamento comunitario, a la luz del contexto jurídico en que éste se inserta y cuando la aplicación eficaz de aquél exija esa intervención del legislador nacional (SSTJCE de 17 de diciembre de 1970, Scheer, 30/70, apartados 7 y 8; y de 30 de octubre de 1975, Rey Soda, 23/75). Es más, esa misma jurisprudencia ha sostenido que los Estados miembros tienen el derecho -e incluso la obligación- de hacer cuanto sea necesario para asegurar el efecto útil del conjunto de las disposiciones del Reglamento (STJCE Scheer, ya citada, apartado 10).

Ahora bien, estas medidas nacionales de aplicación de un Reglamento, por habilitación expresa o implícita, están, en todo caso, sujetas a estrictas limitaciones. En particular, la jurisprudencia viene reiteradamente estableciendo que las normas de desarrollo de un Reglamento que dicten los Estados miembros:

1º) No pueden ocultar a los justiciables la naturaleza comunitaria del Reglamento en cuestión y los efectos que del mismo derivan (Sentencias Variola, antes citada, apartado 11; Zerbone, antes citada, apartado 26; de 14 de octubre de 2004, Comisión/Países Bajos, C113/02, apartado 16; de 21 de diciembre de 2011, Danske Svineproducenter, C-316/10, apartado 41; Al Asa/Consejo, antes citada, apartado 87; y de 25 de octubre de 2012, Anssi Ketelä, apartado 36).

2º) Deben regular el ejercicio del margen de apreciación que ese Reglamento les confiera manteniéndose en todo caso dentro de los límites de sus disposiciones (Sentencias, antes citadas Zerbone,

apartado 27; y Danske Svineproducenter, apartado 41) y sin poner en peligro la finalidad del Reglamento o modificar el alcance o el efecto útil del mismo (STJCE de 18 de febrero de 1970, Bollman, C-40/69, apartado 4).

3º) Deben ser conformes tanto con los objetivos de ese Reglamento, como con los principios generales del Derecho de la Unión y, en particular, con el principio de proporcionalidad (Sentencia Danske Svineproducenter, C-316/10, ya citada).

Por lo tanto, la primera conclusión que se puede extraer de lo indicado hasta ahora es que es posible que los Estados Miembros regulen aspectos que se deriven del RGPD teniendo en cuenta los límites que se acaban de indicar.

Ahora bien, teniendo en cuenta la naturaleza jurídica del organismo del que emana el proyecto de Decreto sometido a informe, debe ponerse la atención en el reparto competencial que es propio del estado de las autonomías y, en consecuencia, la capacidad normativa de los parlamentos autonómicos y su relación con las atribuciones, constitucionales y legales que se hacen en favor de la regulación estatal de determinadas materias, como es un derecho fundamental.

Respecto de la naturaleza de “fundamental” del derecho a la protección de datos, de acuerdo al artículo 18.4 de la CE, y en relación a las competencias normativas de las Comunidades Autónomas, continua el Preámbulo de la LODPGDD:

A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. (...)

Teniendo en cuenta lo anterior, sobre la capacidad normativa de las administraciones de las Comunidades Autónomas y el Estado en materia de protección de datos y su afección al reparto competencial que deriva del bloque de constitucionalidad, esta Agencia se ha pronunciado en otras ocasiones como en el Informe 71/2021 que haciéndose eco de la Sentencia del Tribunal Constitucional 292/2000, se recoge lo siguiente:

Por otra parte, la competencia ejercida por el Estado para la regulación actual, que confiere a la Agencia Española de Protección de Datos (AEPD) la supervisión respecto de los tratamientos de datos personales sobre ficheros o tratamientos llevados a cabo por personas privadas en todo el territorio nacional se considera no sólo difícilmente traspasable, por no sostenerlo la regulación legal vigente, sino que dicha competencia deriva directamente del art. 149.1.1ª de la Constitución, y constituye por lo tanto una competencia exclusiva el Estado no susceptible de transferencia o delegación, en cuanto que no es traspasable la competencia exclusiva del Estado sobre la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

(...)

En segundo lugar, el TC, al razonar sobre el objeto y fines de la LORTAD considera que dicha norma fue dictada para garantizar el respeto o el pleno ejercicio del derecho fundamental previsto en el art. 18.4 CE, esto es, la protección de los datos personales, y ello porque (FJ 11) existe la necesidad de que los derechos fundamentales sean protegidos incluso en el ámbito del reparto competencial (art. 149.1.1 CE).

El mismo objetivo y fines cabe predicar de la actual LOPDGDD, la cual no sólo garantiza el derecho fundamental del art. 18.4 CE, sino que garantiza la igualdad de todos los españoles en el ejercicio de su derecho fundamental a la protección de datos personales.

En el mismo sentido, el citado Dictamen nº 757/2017 del Consejo de Estado, recoge la doctrina constitucional debiendo destacarse lo siguiente:

(...) según la jurisprudencia constitucional en la materia, "lo que está constitucionalmente reservado a Ley orgánica es la regulación de determinados aspectos esenciales para la definición del derecho -en este caso, a la protección de datos de carácter personal ex artículo 18.4 CE-, la previsión de su ámbito y la fijación de sus límites en relación con otras libertades constitucionalmente protegidas". (STC 135/2006).

De acuerdo con lo expuesto y en relación con el objeto del Proyecto de Decreto sometido a informe, debe indicarse que únicamente podrá regular aspectos derivados del desarrollo normativo y de la ejecución y aplicación del RGPD y la LOPDGD en su ámbito de actividad, sin que en ningún caso sea conforme al rango de ley exigido (artículo 81.1 de la Constitución) y al reparto competencial

que entren a regular aspectos esenciales del contenido del derecho fundamental.

II

Teniendo en cuenta lo anterior, procede acudir al régimen legal de atribuciones de la consultante en relación con el objeto del proyecto de Decreto, en tanto administración pública de ámbito territorial circunscrito a la Comunidad Valenciana y su conexión con la potestad de autoorganización que ostentan las administraciones públicas.

La Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana determina en sus artículos 49 y 50 lo siguiente:

Artículo 49.

1. La Generalitat tiene competencia exclusiva sobre las siguientes materias:

1.^a Organización de sus instituciones de autogobierno, en el marco de este Estatuto.

Artículo 50.

En el marco de la legislación básica del Estado, y, en su caso, en los términos que la misma establezca, corresponde a la Generalitat el desarrollo legislativo y la ejecución de las siguientes materias:

1. Régimen jurídico y sistema de responsabilidad de la administración de la Generalitat y de los entes públicos dependientes de ésta, así como el régimen estatutario de sus funcionarios.

Por su parte, el artículo 5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece en sus apartados 2 y 3 lo siguiente:

2. Corresponde a cada Administración Pública delimitar, en su respectivo ámbito competencial, las unidades administrativas que configuran los órganos administrativos propios de las especialidades derivadas de su organización.

3. La creación de cualquier órgano administrativo exigirá, al menos, el cumplimiento de los siguientes requisitos:

a) Determinación de su forma de integración en la Administración Pública de que se trate y su dependencia jerárquica.

b) Delimitación de sus funciones y competencias.

c) Dotación de los créditos necesarios para su puesta en marcha y funcionamiento.

Ahora bien, el ejercicio de la potestad de autoorganización también tiene límites respecto de los que el Tribunal Constitucional ha tenido ocasión de pronunciarse, como en la Sentencia número 142/2018 de 20 de diciembre, dónde pone de manifiesto lo siguiente:

La “potestad de autoorganización” de la Comunidad Autónoma (STC 204/1992, de 26 de noviembre (RTC 1992, 204) , FJ 5) supone la potestad para crear, modificar y suprimir los órganos, unidades administrativas o entidades que configuran la respectiva Administración autonómica o dependen de ella (STC 55/1999, de 6 de abril (RTC 1999, 55) , FJ 3, y las que allí se citan) que nuestra doctrina ha identificado con la competencia autonómica en materia de régimen de organización de su autogobierno, esto es, de decidir cómo organizar el desempeño de sus propias competencias. Resulta de lo anterior que la Comunidad Autónoma puede “conformar libremente la estructura orgánica de su aparato administrativo” (STC 165/1986, de 18 de diciembre (RTC 1986, 165), FJ 6), creando los departamentos o unidades que estime convenientes en orden al adecuado ejercicio de las competencias que le han sido atribuidas, siempre y cuando con ello no interfiera en las que son propias del Estado. Así pues, tan indiscutible es esta competencia autonómica para la propia organización, como el que la misma solo podrá ejercerse sobre ámbitos que, materialmente, correspondan a la propia Comunidad Autónoma, “pues no son concebibles, en Derecho, órganos, servicios o agencias autonómicos cuyas funciones no sean reconducibles a unas u otras competencias estatutarias” (STC 52/2017, FJ 5).

La Generalidad ostenta competencias para la organización de su propia Administración (arts. 71.6 y 150 EAC), así como que el diseño, creación y mantenimiento de “servicios de administración electrónica” es un aspecto central de la “potestad de autoorganización” inherente a la autonomía (STC 111/2016, de 9 de junio (RTC 2016, 111), FJ 11). Sin embargo, la cuestión planteada no es ésta, sino la de las funciones que la Ley 15/2017 (LCAT 2017, 482) reconoce o atribuye a la Agencia que crea. La queja que ha planteado el Abogado del Estado se centra en que el objeto y funciones en que se inserta la actividad de la Agencia no se ciñe al ámbito de la protección de la seguridad de las redes de comunicación electrónicas de la Administración de la Generalidad, sino que, por el contrario, el abanico de actuaciones que desarrolla la

Agencia, de naturaleza muy diversa, permite deducir elementos que, según el caso, pueden incidir sobre las competencias en materia de seguridad pública (149.1.29 CE) y de telecomunicaciones y régimen general de comunicaciones (art. 149.1.21 CE).

Como puede observarse, existen límites no solo en cuanto al aspecto material del contenido del derecho fundamental a la protección de datos, sino que también las funciones que se establezcan para los órganos y unidades creados como consecuencia de la potestad de autoorganización deben observar el reparto competencial que se deriva del artículo 149 de la Constitución y del propio Estatuto de Autonomía.

III

Dicho lo anterior, lo que pretende el proyecto de Decreto sometido a informe es el establecimiento de una política de protección de datos, así como la regulación de estructuras organizativas y procedimientos de actuación para dotar de mayor eficacia al deber de cumplimiento del RGPD.

Tal como indica el Considerando 74 del RGPD:

Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

En efecto, las medidas en las que se concreta el proyecto de Decreto son al fin y al cabo manifestaciones del principio de responsabilidad activa y del mandato previsto en los artículos 24 del RGPD y 28 de la LOPDGDD, que disponen lo siguiente:

Artículo 24 RGPD:

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

Artículo 28 de la LOPDGDD:

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable.

En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

Y en su apartado 2, determina que:

Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

- a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.
- b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.
- c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.
- d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales,

su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Ahora bien, tal como esta Agencia indicó en la “Guía del Riesgo y evaluación de impacto en tratamiento de datos personales”¹ lo que exige el RGPD con relación a las políticas de protección de datos es el aspecto efectivo, práctico y ejecutivo de un conjunto de directrices, yendo más allá de la referencia al aspecto formal de la existencia de un documento titulado “política de protección de datos” donde se realiza la mera reproducción formal del articulado del RGPD y se reduce a una mera declaración de la voluntad de compromiso del responsable con el cumplimiento normativo. En este sentido y no sólo con relación a las políticas, sino también en la gestión de riesgo, hay que evitar confundir el fondo con la forma, ya que es el fondo lo que reclama el RGPD.

(...) podría ser aconsejable disponer de un documento marco siempre que se emplee como guía para la adopción las directrices señaladas en procedimientos específicos como, por ejemplo, los procedimientos de recursos humanos, teletrabajo, contratación de productos y servicios, desarrollo de aplicaciones, etc. Pero siempre que tenga el objeto de garantizar la eficacia en la protección de datos y que no se limite a una pura declaración formal en un documento desvinculado de la realidad de los procedimientos de la entidad. (...)

En este sentido, puede adelantarse ya que esa necesidad de que la “política de protección de datos” no sea una reproducción del RGPD o únicamente una declaración formal de asunción de compromisos de cumplimiento normativo, es lo que confronta principalmente con el texto sometido a informe.

¹ <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>
c. Jorge Juan 6
28001 Madrid

En segundo término, y al margen de la estructura organizativa de la que se pretende dotar al responsable del tratamiento, debe tenerse en cuenta que es una obligación del RGPD que la administración pública consultante, en tanto autoridad u organismo público, cuente con un delegado de protección de datos.

En efecto, así lo establece el artículo 37.1 a) del RGPD:

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

- a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial

En el mismo sentido las Directrices “Sobre los Delegados de Protección de Datos” de 05/04/2017 del Grupo de Trabajo del Artículo 29 actualmente sustituido por CEPD indican lo siguiente:

El RGPD no define qué constituye una «autoridad u organismo público». El Grupo de Trabajo del artículo 29 considera que dicha noción debe determinarse en virtud del Derecho nacional. Por consiguiente, las autoridades y organismos públicos incluyen las autoridades nacionales, regionales y locales, pero además el concepto, con arreglo a la legislación nacional aplicable, normalmente incluye también una serie de organismos regidos por el derecho público. En tales casos, la designación de un DPD es obligatoria.

IV

Sobre el contenido del Proyecto de Decreto se realizan las siguientes consideraciones:

En cuanto al Preámbulo del texto proyectado, debe indicarse que comienza indicando la finalidad del desarrollo de una política de protección de datos personales concretándola en los siguientes términos:

“garantizar los derechos de la ciudadanía sobre la privacidad y seguridad de sus datos”

Se propone la sustitución por el contenido exacto del artículo 24.1 del RGPD a los efectos de una mayor precisión, y eliminar la posible ambigüedad del uso de términos como “privacidad” y “seguridad”, y no confundirlos con la política de seguridad de la organización que tiene otros objetivos complementarios. Por lo tanto, el párrafo propuesto sería el siguiente:

“garantizar y poder demostrar que los tratamientos son conforme con el RGPD y su normativa de desarrollo, aplicar la medidas técnicas y

organizativas apropiadas a dicho fin, así como revisarlas y actualizarlas cuando sea necesario”

En segundo lugar, en el preámbulo se indica lo siguiente:

“Asimismo, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, establece lo propio en su ámbito de aplicación. “

Frente a lo que cabe señalar que, si no resulta de aplicación al tratamiento que realice el responsable del tratamiento, es innecesaria su indicación.

Dicho lo anterior, en cuanto a la estructura y sistemática del texto proyectado, debe señalarse que la ubicación de los Títulos en los que se divide el proyecto debería ser objeto de modificación pues tal como se presenta, dificulta la comprensión de su contenido y en definitiva la aplicación de la norma, ya que de acuerdo con el principio deductivo debe partirse de conceptos generales para luego establecer las especificades de éstos.

Esta cuestión resulta de especial relevancia en lo que se refiere a la materia de protección de datos y el objeto de la regulación del proyecto de Decreto, que pretende regular las obligaciones que establece el RGPD.

Por lo tanto, debería empezarse por identificar a los sujetos obligados, es decir, primero se debe determinar con claridad quien es el responsable del tratamiento y en su caso, el encargado y a partir de ahí indicar las obligaciones y desarrollar las funciones que se les pretenda atribuir, sin perjuicio de que luego exista un Título o Capítulo dedicado a la Estructura Organizativa en materia de protección de datos como se indica en el Título III.

Es decir, hay que delimitar quién se considera responsable del tratamiento y luego, incluso en otros Capítulos la estructura de los órganos que van a tener competencias y obligaciones para ejecutar las políticas que se establezcan, como por ejemplo, la propia Delegación de Protección de Datos de la Generalitat (artículo 22), las Unidades de Protección de Datos que se establecen con carácter general en el artículo 17, o la organización complementaria que prevista para centros sanitarios, docentes y de servicios sociales prevista en el artículo 18, así como los Grupos de Trabajo de Protección de Datos previstos en el artículo 23 y siguientes.

La necesidad de la modificación o redefinición indicada se muestra en el artículo 4 denominado “Políticas internas en materia de protección de datos”, donde se indica en sus apartados 1 y 2 lo siguiente:

1. Las consellerías y las entidades del sector público instrumental deberán establecer políticas internas de protección de datos personales con las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento del Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, de 5 de diciembre y la política general de protección de datos prevista en el presente decreto. Asimismo, deberán establecer políticas internas de protección de datos aquellos órganos y unidades administrativas que determine este decreto.

2. Las personas titulares de las consellerías y los órganos unipersonales de gobierno de las entidades del sector público deberán aprobar las políticas internas de protección de datos.

Los destinatarios de las obligaciones del RGPD, son los responsables del tratamiento, y en su caso, los encargados, por lo que debería clarificarse quien ostenta esta cualidad.

De acuerdo con el artículo 24 del RGPD, es el responsable del tratamiento el que debe aplicar las medidas, entre las que se incluyen políticas de protección de datos.

En consecuencia, indicar en el precepto analizado, que deberán establecer políticas internas “las consellerías y las entidades del sector público”, y también “aquellos órganos y unidades que determine este decreto” -que se deduce por la regulación que se hace en otros preceptos por razón de la materia, como sanidad, educación o servicios sociales- y, por otro lado, que deberán aprobar las políticas de protección de datos “las personas titulares de las consellerías y los órganos unipersonales de gobierno de las entidades del sector público”, induce a confusión en cuanto a la figura que ostenta cada sujeto indicado y en cuanto a las atribuciones que se asignan derivados de los verbos utilizados, establecer y aprobar.

Por lo tanto, se propone que se identifique al responsable del tratamiento y se simplifique el verbo utilizado para establecer la obligación de contar con una política interna de protección de datos y se elimine el apartado 2.

Se propone la siguiente modificación:

Las consellerías y las entidades del sector público instrumental, en tanto responsables del tratamiento, aprobarán las políticas internas de protección de datos personales con las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento del Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, de 5 de diciembre y la política general de protección de datos prevista en el presente decreto.

Asimismo, deberán establecer políticas internas de protección de datos aquellos órganos y unidades administrativas que, sin ser responsables del tratamiento y en atención a la especial protección de los datos que sometan a tratamiento, determine este decreto.

En cuanto a lo indicado en el apartado 3, debemos hacer una remisión a lo ya indicado en el apartado III del presente informe sobre el contenido de las políticas de protección de datos y gestión del riesgo a los efectos de que no sean una mera transcripción de la norma, sino que vayan más allá convirtiéndose en auténticas herramientas útiles, que no se basen únicamente en indicar “el qué”, sino que también aborden “el cómo”.

Respecto del apartado 4, éste indica lo siguiente:

4. Con objeto de garantizar la mayor disponibilidad, en la página web principal de cada Conselleria o entidad se habilitará un apartado denominado “Protección de datos”, donde constará, al menos, información sobre su política interna de protección de datos, especialmente en lo que afecte a los derechos de la ciudadanía, y el Registro de Actividades de Tratamiento correspondiente.

En primer lugar, debe señalarse que se utiliza erróneamente el termino Registro de Actividades de Tratamiento, ya que de acuerdo con el artículo 31 de la LOPDGDD, cuando estamos ante los sujetos a los que se refiere el artículo 77.1, la obligación de publicidad se refiere a Inventario de Actividades de Tratamiento. Lo que no exonera a la administración en tanto responsable del tratamiento, de la elaboración de un RAT y tenerlo a disposición de la autoridad de control, en los términos establecidos tanto en el RGPD como en la LOPDGDD.

Por lo tanto, atendiendo a que el precepto se refiere a la publicidad, debería sustituirse la indicación de Registro de Actividades de Tratamiento, por la de Inventario de Actividades de Tratamiento.

En segundo lugar, debe recordarse que el Inventario hará referencia a lo que afecte a los ciudadanos teniendo en cuenta que la publicación del mismo es una obligación de transparencia tal como consta en el artículo 6. bis de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

No obstante, lo anterior, debe recordarse que la transparencia no puede ser un riesgo ni para los interesados ni para la propia administración, por lo que debe evitarse la publicación de cualquier información que pueda suponer un riesgo como podría suceder, por ejemplo, al publicar el análisis de riesgos.

V

En cuanto al artículo 5 denominado “Principios Reguladores”, debe indicarse que el objeto del texto proyectado es establecer las “políticas de protección de datos” por lo que no tiene sentido una reproducción del artículo 5 del RGPD.

Dicho lo anterior, el citado precepto comienza indicando lo siguiente:

1. Conforme al Reglamento (UE) 2016/679, las políticas internas se elaborarán aplicando el principio de responsabilidad proactiva, lo que supone adoptar las medidas técnicas y organizativas en función del riesgo asociado a los tratamientos de datos de carácter personal.

Pues bien, debe comenzarse indicando que de la redacción de la norma se deduce un error de concepto, en el sentido de que las políticas deben considerarse como un documento de alto nivel que refleja el compromiso del responsable con una forma de actuar en la organización, en este caso, con relación a la protección de datos. No es un mecanismo para adoptar las medidas técnicas y organizativas en función del riesgo asociado a un determinado tratamiento. Ya que tienen que reflejar qué va a existir y cómo se va a articular una gestión de la responsabilidad proactiva, por ejemplo, del riesgo, de las herramientas de seguimiento (auditoría), etc.

Es un error aplicar prescriptivamente desde una política cualquier medida sin tener en cuenta el caso a caso de cada tratamiento.

Por eso, del análisis del precepto parece que asume el modelo prescriptivo de la derogada Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y se aparta del modelo prospectivo basado en el riesgo de cada tratamiento, propio del RGPD y en especial del significado del principio de responsabilidad proactiva.

El segundo apartado se limita indicar que “todo tratamiento de datos de carácter personal cumplirá con alguna de las bases de legitimación previstas en el artículo 6 del Reglamento (UE) 2016/679”, lo que no tiene sentido por cuanto resulta obvio, pues de otro modo se estaría incumpliendo dicho RGPD, es decir, no aporta ningún valor añadido a la regulación. Asimismo, como se ha dicho con anterioridad, una política de protección de datos no puede limitarse a copiar el RGPD o la LOPDGDD.

En cuanto al tercer apartado que tiene esta redacción:

La base de legitimación que proceda se determinará de conformidad con lo previsto en la normativa y las directrices que establezca la autoridad de control de protección de datos. Estas bases de legitimación deberán constar en el registro de actividades del tratamiento y en la información

que se facilite a las personas interesadas como consecuencia del deber de informar.

Debe indicarse que las bases jurídicas no las establece la Autoridad de control de protección de datos, sino que son las previstas en el artículo 6 del RGPD y es su identificación la que corresponde al responsable del tratamiento, es decir, que debe tratar los datos siempre que se dé, al menos una de ellas.

Asimismo, sobre la información que debe proporcionarse acerca de la base jurídica en cuestión, el artículo 31.2 de la LOPDGDD, establece la obligación de que en el Registro de Actividades del Tratamiento se informe de la misma cuando estamos ante uno de los sujetos enumerados en el artículo 77.1, en este caso, resulta de aplicación porque estamos ante una administración de una comunidad autónoma (apartado 1. c del citado artículo) y el artículo 13.1 c) del RGPD, hace lo propio en cuanto al contenido de la información que hay que proporcionar cuando los datos que van a ser objeto de tratamiento son obtenidos del interesado. A lo que hay que añadir que, incluso, existe un régimen sancionador que tipifica la inobservancia de estas obligaciones.

Es decir, estaríamos ante una repetición innecesaria y que podría conducir a considerar que dicha obligación nace en el Decreto y no en la norma general de aplicación como es el RGPD y la LOPDGDD. En este sentido se pronuncia el Dictamen nº 757/2017 del Consejo de Estado antes referido:

(...) aunque la jurisprudencia europea no prohíbe de forma tajante toda medida interna de recepción o reproducción de los reglamentos comunitarios, sí reprueba que los preceptos de éstos sean reproducidos por los Estados miembros, buscando dar la idea de que se trata de normas nacionales. El Tribunal de Justicia, por tanto, no condena tal práctica en sí misma considerada, pero sí procura evitar determinados efectos que de ella podrían derivarse, perjudicando la correcta aplicación del Derecho de la Unión, como sucedería cuando lo invocado y aplicado no es el reglamento comunitario, sino la norma interna de recepción, corriéndose así el peligro de que se confunda el momento de entrada en vigor (tomando como fecha la de publicación de la norma interna en el correspondiente Boletín Oficial, y no la del reglamento en el Diario Oficial de la Unión Europea), o a la ubicación de la regulación en cuestión en el sistema general de fuentes (sometiendo la norma interna de recepción al propio sistema de fuentes, desconectándola del marco comunitario). Lo que importa, en definitiva, no es tanto el hecho de la recepción o reproducción del reglamento, cuanto las consecuencias que esta actuación podría tener en perjuicio de la uniformidad perseguida por tal instrumento normativo comunitario: si bien con carácter general cabe

afirmar la prohibición de cualquier modalidad de recepción o reproducción, habrá que estar a cada caso concreto para ver si efectivamente se producen tales consecuencias nocivas para la uniformidad del ordenamiento comunitario. Por ejemplo, en la Sentencia de 28 marzo 1985, Comisión/Italia, 272/83, el Tribunal admitió la reproducción de ciertas disposiciones de reglamentos comunitarios por leyes regionales italianas, argumentando que esa "situación particular" había tenido lugar en interés de una mayor coherencia y mejor comprensión de tales leyes regionales, mientras que, en la sentencia de 7 de febrero 1973, Comisión/Italia, 39/72, ante la adopción por el Gobierno italiano de un Decreto cuyo artículo 1 establecía que determinados reglamentos comunitarios "son considerados como recibidos por el presente Decreto", limitándose a reproducir las disposiciones de dichos reglamentos, el Tribunal de Justicia consideró que "mediante la utilización de este procedimiento, el Gobierno italiano ha creado un equívoco en lo que se refiere tanto a la naturaleza jurídica de las disposiciones aplicables como al momento de su entrada en vigor".

VI

En el Capítulo IV se abordan los "Derechos de la Ciudadanía", y comienza en el artículo 6 denominado "Transparencia e información a la persona titular de los datos", respecto del que deben realizarse las siguientes consideraciones:

De nuevo se observa que gran parte de sus apartados se dedican a cumplimiento normativo, lo que como se ha indicado en reiteradas ocasiones el contenido de la política de protección de datos, -que es el objeto de esta regulación sometida a informe -no puede limitarse a este contenido, sencillamente porque ya está en el propio RGPD.

Dicho lo anterior, en el apartado 2 se indica que:

La información se facilitará, preferentemente, por el mismo medio por el que el ciudadano o la ciudadanía aporte sus datos de carácter personal, ya sea a través de formularios en soporte papel o electrónicos o mediante locuciones telefónicas, garantizando la plena accesibilidad de los medios e información facilitados.

La obligación que se deriva sobre el modo o manera de facilitar la información puede resultar obstativa para el normal desarrollo de la relación ciudadano-administración y su eficacia.

Imagínese que el interesado aporta los datos personales verbalmente en la “ventanilla” de un servicio de la administración, tal como está redactado el apartado, el personal del servicio en cuestión debería informarle, “verbalmente” en los términos del artículo 13 del RGPD o utilizar la fórmula del artículo 11 de la LOPDGDD. En un caso y en otro, resulta farragoso y puede suponer una pérdida de eficacia en el servicio público que va a ser objeto de prestación.

El artículo 12.1 del RGPD nos indica que:

(...) La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. (...)

En las Directrices WP260 “Sobre la Transparencia en virtud del RGPD” de 11/04/2018 del Grupo de Trabajo del Artículo 29 (actualmente sustituido por el Comité Europeo de Protección de Datos, CEPD en lo sucesivo), establece que:

Es fundamental que el método o métodos elegidos para facilitar la información sean adecuados para las circunstancias concretas, esto es, la manera en que el responsable del tratamiento y el interesado interactúan o la manera en que se recoge la información del interesado.

Por lo tanto, se propone reconsiderar la literalidad del apartado 2, y utilizar una fórmula que no dificulte la prestación del servicio en sí mismo considerado y que se adapte al contexto en el que se recaban los datos, de modo que la información se ofrezca verbalmente, solo en el caso de que así lo solicite el interesado, no menoscabe la calidad y eficacia del servicio y no siempre que sea este medio por el que se recaban los datos. Sobre todo, teniendo en cuenta el apartado 5 del artículo 6 que más adelante se analizará.

En los apartados 3 y 4 se indica lo siguiente:

3.Cuando los datos sean obtenidos directamente de las personas afectadas, el responsable del tratamiento pondrá a su disposición, en el momento de su recogida, la información establecida en el artículo 13 del Reglamento (UE) 2016/679.

Esta obligación se cumplirá, de manera preferente, facilitando la información básica a la que hace referencia el artículo 11 de la ley Orgánica 3/2018, de 5 de diciembre, proporcionando la información completa mediante una dirección electrónica o un código de conexión.

4.Cuando los datos no se hubieran obtenido de la persona titular, se cumplirá con el deber de informar en la primera comunicación que se le haga a la persona interesada que, en todo caso, deberá respetar los

plazos regulados en el artículo 14.3 a) del Reglamento (UE) 2016/679. En estos supuestos la información básica incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que proceden los datos.

Se observa que se establece una diferenciación en cuanto al deber de informar cuando los datos son obtenidos del interesado y cuando no, tal como hacen los artículos 13 y 14 del RGPD, y se propone como preferente el uso de un sistema por capas o niveles, de acuerdo con el artículo 11 de la LOPDGDD.

Ahora bien, la diferenciación de un supuesto u otro se considera asimétrica en lo referente al contenido y deficiente en cuanto a la existencia de supuestos que excepcionan el deber de información. Asimismo, respecto de la información básica en el supuesto de tratamiento de datos no recogidos del interesado, tal como está ubicada y redactada la información no resulta del todo clarificadora en el sentido de que también se dará preferencia a esta opción por “capas” en ambos estos supuestos.

En consecuencia, se propone la siguiente modificación de los apartados 3 y 4:

3.Cuando los datos sean obtenidos directamente de las personas afectadas, se dará cumplimiento a la obligación de informar de conformidad con lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679, y en especial, en lo referido al contenido y a los supuestos en los que no es necesaria dicha información.

La obligación de informar se cumplirá, de manera preferente, facilitando la información básica a la que hace referencia el artículo 11 de la ley Orgánica 3/2018, de 5 de diciembre, proporcionando la información completa mediante una dirección electrónica o un código de conexión.

4.Cuando los datos no se hubieran obtenido de la persona titular, se dará cumplimiento a la obligación de informar, de conformidad con lo dispuesto en el artículo 14 del Reglamento (UE) 2016/679, y en especial, en lo referido en los plazos y a los supuestos en los que no es necesaria dicha información.

En estos supuestos, en la información básica referida en el apartado anterior, se incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que proceden los datos.

En el apartado 5 se indica lo siguiente:

5.Asimismo, en función de la naturaleza del tratamiento, el responsable podrá cumplir con el deber de informar mediante la colocación de un dispositivo informativo en lugar visible identificando, al menos, la

existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos en materia de protección de datos junto con una dirección electrónica o un código de conexión que enlace a la información completa sobre estos tratamientos.

Este apartado será aplicable, en todo caso, a los tratamientos relacionados con la videovigilancia y con los accesos a edificios, instalaciones y medios de transporte.

De acuerdo con el último párrafo, parece que este apartado está pensado, sobre todo para tratamientos de imágenes captados por sistemas de videovigilancia.

No obstante, como complemento informativo podría utilizarse también en otros supuestos que pueden presentar dificultades añadidas por el propio contexto en el que se dan, tal como se ha indicado en el análisis que se hace sobre el apartado 2. En efecto, podría incluir en la redacción, “la finalidad del tratamiento” y así dar cobertura a lo indicado en el artículo 11 de la LOPDGDD y servir a otros tipos de tratamiento.

Por lo tanto, se propone la siguiente modificación:

5. Asimismo, en función de la naturaleza del tratamiento, el responsable podrá cumplir con el deber de informar mediante la colocación de un dispositivo informativo en lugar visible identificando, al menos, la existencia y finalidad del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos en materia de protección de datos junto con una dirección electrónica o un código de conexión que enlace a la información completa sobre estos tratamientos.

Este apartado será aplicable, en todo caso, a los tratamientos relacionados con la videovigilancia y con los accesos a edificios, instalaciones y medios de transporte.

VII

Siguiendo con Capítulo IV referido “Derechos de la Ciudadanía”, el artículo 7 se refiere expresamente al “ejercicio de derechos”.

En su apartado 2 consta lo siguiente:

2. De conformidad con lo previsto en la normativa reguladora del procedimiento administrativo común, las solicitudes de ejercicio de derechos requerirán la acreditación de la identidad de la persona interesada, así como estar debidamente firmadas y deberán ser

presentadas electrónicamente a través del procedimiento establecido o por cualquiera de los otros medios previstos en dicha normativa.

Como puede observarse el apartado aborda el modo o manera a través del cual los afectados pueden ejercer sus derechos.

El primer análisis que hay realizar se refiere a lo indicado en el artículo 12 apartados 3 y 6 del RGPD que determina que:

Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

(...)

Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

Sobre los modos en que los ciudadanos deben relacionarse con las administraciones públicas, y en concreto respecto de la obligatoriedad de identificación, firma y el uso de un canal electrónico o presencial, debe acudirse a la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP en lo sucesivo), en tanto que la Comunidad Valenciana como administración de las CCAA está sometida a su aplicación (artículo 2.1 b):

Artículo 9. Sistemas de identificación de los interesados en el procedimiento.

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

Artículo 11 Uso de medios de identificación y firma en el procedimiento administrativo.

1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.

2. Las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:

a) Formular solicitudes.

Artículo 12. Asistencia en el uso de medios electrónicos a los interesados.

1. Las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios, así como los sistemas y aplicaciones que en cada caso se determinen

Artículo 13 Derechos de las personas en sus relaciones con las Administraciones Públicas.

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.

Artículo 14. Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.

1. Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.

Teniendo en cuenta los preceptos que se acaban de indicar se informa favorablemente el apartado analizado, salvo la última parte que al utilizar la expresión “deberán ser presentadas” y a continuación “o por otros medios”, resulta confusa y contradictoria. Se impone una obligación y luego se excepciona sin justificación alguna directa ni indirecta.

Es decir, de las normas parcialmente transcritas se infiere que se pueden utilizar tanto medios electrónicos como otros medios para el relacionarse con la administración pública en general y para el ejercicio de los derechos en particular, y debe ser respetado dicho medio por parte de aquella.

Asimismo, ha sido un criterio de la Agencia a la hora de tramitar procedimientos de reclamaciones por desatención de derechos que, si un responsable del tratamiento determina un canal, por ejemplo, electrónico, y se solicita un derecho a través de otro medio, lo relevante es que se acredite que, efectivamente, el responsable ha tenido conocimiento del mismo para que

pueda atender dicho derecho, por eso resultaría adecuado, que fuere el medio que fuere, pueda el ciudadano acreditar el efectivo ejercicio del derecho.

Por lo que se sugiere la siguiente modificación a fin de que se plasme sin asomo de duda que ambos medios, en un plano de igualdad y por tanto sin preferencia, pueden ser utilizados:

2.De conformidad con lo previsto en la normativa reguladora del procedimiento administrativo común, las solicitudes de ejercicio de derechos requerirán la acreditación de la identidad de la persona interesada, así como estar debidamente firmadas y podrán ser presentadas electrónicamente a través del procedimiento establecido o por cualquiera de los otros medios previstos en dicha normativa.

Con independencia del medio elegido, el responsable del tratamiento deberá garantizar que interesado obtenga justificación de la presentación de su solicitud.

Siguiendo con el artículo 7 del Proyecto de Decreto, en su apartado 3 se indica que:

3.La persona interesada deberá ser informada en un lenguaje claro, sencillo y accesible de las actuaciones en relación con su solicitud, los medios, así como del plazo máximo para resolver ésta.

Se informa favorablemente esta cláusula pues resulta acorde con el mandato del artículo 12.1 RGPD referida a que el responsable tomara las medidas oportunas para facilitar al interesado cualquier comunicación con arreglo a los artículos 15 a 22, de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

En cuanto al apartado 4, se establece la obligatoriedad de tener un protocolo para la atención de los derechos, con un contenido mínimo y que estará disponible para la autoridad de control que lo solicite.

Se valora positivamente este apartado en la medida en que, impone medidas para que el responsable del tratamiento con el objeto de dar cumplimiento de la mejor manera posible al ejercicio de derechos.

Es, al fin y al cabo, otra expresión más de la potestad de autoorganización que refuerza los compromisos para demostrar que se cumple con el RGPD, sin que entre a regular de cara al ciudadano el ejercicio de sus derechos. Es decir, no impone cargas adicionales, no modifica plazos que le afecten, etc...., no regula aspectos esenciales del contenido de este derecho.

VIII

Siguiendo con Capítulo IV referido “Derechos de la Ciudadanía”, el artículo 8 se refiere expresamente a las “Reclamaciones ante el delegado o delegada de protección de datos de la Generalitat” cuyo contenido de su apartado 1 es el siguiente:

1. Las personas afectadas podrán presentar una reclamación, bien ante la autoridad de control, bien ante la Delegación de Protección de Datos de la Generalitat, en los supuestos en los que no haya sido atendida su solicitud de ejercicio de derechos o se haya producido una posible infracción de lo dispuesto en la normativa de protección de datos por parte de la administración del Consell o su sector público instrumental.

Como puede observarse se recoge la posibilidad de presentar la oportuna reclamación, ya sea por desatender los derechos previstos en los artículos 15 a 22 RGPD, ya sea por posibles vulneraciones de la normativa, ante la autoridad de control o ante el delegado de protección de datos, es decir, posibilidades que ya las ofrece el ordenamiento jurídico aplicable.

Debe indicarse que el artículo 38.4 del RGPD establece lo siguiente:

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

Y en el artículo 77.1 del RGPD se indica que:

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

Teniendo en cuenta lo recogido en los preceptos que se acaban de citar, la denominación del artículo que hace referencia únicamente a la reclamaciones ante el delegado, así como la circunstancia de que el derecho a presentar una reclamación, ya sea ante la autoridad de control, ya sea ante el Delegado de Protección de datos, forma parte de las facultades que conforman el derecho fundamental a la protección de datos y es uno de los elementos del “poder de control y disposición” sobre los datos que recoge la STC 292/2000, es decir, se tiene ese derecho con independencia de que así lo indique el proyecto de Decreto, se propone la eliminación del apartado 1.

El apartado 2 está redactado en los siguientes términos:

2. Cuando una reclamación se presente ante la Delegación de Protección de Datos, de acuerdo con el artículo 37.1 de la Ley Orgánica 3/2018, de 5 de diciembre, esta deberá notificar a la persona reclamante la decisión adoptada en el plazo de dos meses. La Delegación de Protección de Datos realizará una valoración previa de la reclamación recibida y la remitirá, sin dilación indebida, al responsable del tratamiento para que en el plazo de un mes emita informe o adopte decisión formal al respecto.

Se establece una regulación en relación con la tramitación que se debe llevar a cabo cuando se presente una reclamación de acuerdo con el artículo 37.1 LOPDGDD.

Pues bien, dicho precepto establece en su párrafo segundo que:

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

En consecuencia, se informa favorablemente este apartado 2 en la medida en que es respetuoso con lo indicado en la LOPDGDD al establecer un plazo ad intra, que no altera el plazo máximo de dos meses que impone la ley.

Por su parte, el apartado 3, indica lo siguiente:

3. Cuando una reclamación se presente ante la autoridad de control, de acuerdo con el artículo 37.2 de la Ley Orgánica 3/2018, de 5 de diciembre, esta podrá remitirla a la Delegación de Protección de Datos para que analice y remita a dicha autoridad de control la información requerida en el plazo de un mes. Durante este plazo, la Delegación de Protección de Datos dará traslado de la reclamación al responsable del tratamiento para que emita informe o decisión formal al respecto en el plazo de 10 días hábiles desde su recepción.

Pues bien, dicho precepto establece lo siguiente:

Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Al igual que en el anterior párrafo, se considera que la regulación propuesta es acorde con la LOPDGDD, al establecer un plazo ad intra, que no altera el plazo de un mes que impone la ley.

IX

En el Capítulo V del proyecto de Decreto, se regulan las “Medidas de responsabilidad activa en el tratamiento de datos”, respecto del que debe indicarse lo siguiente:

El artículo 9 en sus apartados 1 a 3, trata del análisis de riesgos y evaluación de impacto, recordando la obligación de realizar el análisis de riesgos e indicando el modo de realizarlo y la posibilidad de su actualización cuando se produjese una modificación en el tratamiento de datos que pudiera suponer un incremento del riesgo. En este sentido debería incluirse en el precepto que la actualización no solo procederá cuando hay una modificación del tratamiento, sino también, cuando haya un cambio de contexto, por ejemplo, cuando haya algún tipo de amenaza por la aparición de un nuevo virus o ataque informático, o cuando exista un nuevo contexto, político, social y económico que suponga un aumento del riesgo, etc.,

Asimismo se echa en falta alguna remisión y adaptación (que no transcripción) al artículo 32.2 del RGPD y al artículo 28.2 de la LOPDGDD, que proporcionan elementos a tener en cuenta en el análisis de riesgos.

En el apartado 4 del artículo 9 se aborda la Evaluación de Impacto en los siguientes términos:

4.Cuando los tratamientos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, el responsable realizará una evaluación de impacto, de acuerdo con lo establecido en la normativa de protección de datos y según los criterios que establezca la autoridad de control de protección de datos y la Delegación de Protección de Datos de la Generalitat.

De su lectura se deduce que recoge prácticamente la literalidad del artículo 35.1 del RGPD, pero omite un aspecto que debe considerarse esencial, el momento en que hay que hacer la EIPD, el precepto dice “antes del tratamiento” y si bien en la cláusula analizada hace una remisión a “lo establecido en la normativa de protección de datos”, resultaría más adecuado y en consonancia con dicho precepto, que este aspecto se incluyera en la literalidad de la cláusula.

En el artículo 10 se regula el Registro de Actividades del Tratamiento (RAT en lo sucesivo), haciendo una remisión al RGPD y a la LOPDGDD en cuanto a su contenido y estableciendo una obligación de actualización de su información, así como la obligación de comunicar cualquier modificación a la delegación de Protección de Datos en el plazo máximo de 10 días después de que se publique la misma en el registro publicado.

Como se ha indicado antes, debe tenerse en cuenta que, en las administraciones públicas, las obligaciones referidas al RAT, son de publicación de un Inventario de Actividades de Tratamiento (artículo 31 LOPDGDD), lo que las exonera de la obligación establecida en el artículo 30 del RGPD.

Por lo que teniendo en cuenta lo anterior, el precepto debería plasmar estas dos obligaciones, por un lado, disponer de un RAT y por otro publicar un IAT.

Por eso en el apartado 3, debería sustituirse la indicación del RAT por la del IAT. Asimismo, el precepto atribuye la obligación de su creación y llevanza a “Cada Conselleria y entidad del sector público”, cuando como se ha indicado antes, sería más acorde indicar o resaltar su cualidad de responsables del tratamiento.

Asimismo, el artículo 30.2 del RGPD y el artículo 31.1 LOPDGDD también incluyen al encargado del tratamiento como destinatario de esta obligación, y podría darse que aquellos organismos que forman parte de la administración de la Comunidad Valenciana actúen en determinadas ocasiones como encargados del tratamiento.

A lo que hay que añadir que el citado artículo 31 de la LOPDGDD establece que:

Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Respecto de la indicación contenida en el apartado 2 sobre la comunicación de la modificación del RAT a la Delegación de Protección de Datos, se deduce que primero se ha producido la misma y luego se debe comunicar, cuando puede no tener sentido teniendo en cuenta las funciones que tiene el DPD al responsable en cuanto a la supervisión del cumplimiento de las obligaciones en el RGPD de acuerdo con el artículo 39.1 b).

Las Directrices “Sobre los Delegados de Protección de Datos” de 05/04/2017 del Grupo de Trabajo del Artículo 29 actualmente sustituido por CEPD, indican que:

En virtud del artículo 30, apartados 1 y 2, es el responsable o el encargado del tratamiento, y no el DPD, quien está obligado a llevar «un registro de las actividades de tratamiento efectuadas bajo su responsabilidad» o a mantener «un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable». En la práctica, es frecuente que los DPD elaboren inventarios y

mantengan un registro de las operaciones de tratamiento basándose en la información que les proporcionan los distintos departamentos responsables del tratamiento de datos en su organización. Esta práctica se ha establecido en virtud de muchas legislaciones nacionales vigentes y de las normas sobre protección de datos aplicables a las instituciones y organismos de la UE. El artículo 39, apartado 1, establece una lista de tareas mínimas de que debe encargarse el DPD. Por tanto, nada impide que el responsable o el encargado del tratamiento asignen al DPD la tarea de mantener un registro de las operaciones de tratamiento bajo la responsabilidad del responsable o del encargado del tratamiento. Dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de las normas y de información y asesoramiento al responsable o al encargado del tratamiento.

En consecuencia, resulta lógico que el DPD intervenga en la modificación del RAT (y en su caso del inventario de actividades del tratamiento), y a pesar de que el momento de dicha intervención no está determinado por la normativa, pero se indica que la comunicación debe realizarse *“en un plazo máximo de 10 días después de que el cambio se haya reflejado en el Registro publicado”* parece que con la publicación ya se “ha oficializado el cambio” y que el asesoramiento y supervisión del DPD ya no tenga sentido.

Es decir, la “validación” o supervisión del RAT y sus modificaciones por parte del DPD deberían realizarse antes de la publicación y no con posterioridad.

En consecuencia, se propone la siguiente modificación:

- 1.Los sujetos enumerados en el artículo 2 del presente Decreto que actúen como responsable del tratamiento, y en su caso, como encargado del tratamiento, publicarán un Inventario de sus Actividades de Tratamiento de acuerdo con lo dispuesto en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre, sin perjuicio de la obligación de disponer del Registro de Actividades del Tratamiento.
- 2.El Registro de las Actividades de Tratamiento, y la publicación del Inventario de Actividades del tratamiento, deberán estar permanentemente actualizados y las modificaciones se comunicarán a la Delegación de Protección de Datos de la Generalitat con anterioridad a que el cambio se haya reflejado tanto en el citado registro como en la publicación del inventario.

Por otra parte, la redacción del apartado 4 se refiere a:

El Registro de las Actividades de Tratamiento se entenderá aprobado con su publicación en la página web del responsable.

Con independencia de las consideraciones realizadas sobre el Inventario de Actividades de Tratamiento, y el RAT, tal como está redactado el artículo se plantean varias cuestiones como, por ejemplo, ¿Quién lo aprueba? y ¿en base a qué? Es decir, la redacción resulta innecesaria ya que la publicación del IAT y en su caso del RAT, es una obligación del responsable del tratamiento, y en su caso, del encargado del tratamiento, es decir, existe dicha obligación y se cumple con la publicación, resultando un añadido sin justificación lógica que se deba aprobar o que dicha aprobación deba revestir de una determinada liturgia.

En consecuencia, se propone la eliminación del apartado 4.

El artículo 11 aborda las “Violaciones de la seguridad de los datos de carácter personal”, respecto del que deben realizarse las siguientes consideraciones:

Se observa que se establece la necesidad de tener un protocolo de actuación con un contenido mínimo y el establecimiento de unos plazos internos que resultan respetuosos con lo indicado en el artículo 33.1 del RGPD.

En el apartado 3 se regula la notificación de la violación de seguridad a los afectados en los siguientes términos:

3. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará a las personas afectadas, en los términos establecidos en el Reglamento (UE) 2016/679, pudiéndose recabar el asesoramiento de la Delegación de Protección de Datos de la Generalitat en la valoración de dicho riesgo.

Se observa de nuevo que se hace una remisión a la normativa pero que sin embargo no se indica nada de la notificación a la autoridad de control. Es decir, resulta confuso el precepto por incompleto.

En el apartado 4 consta lo siguiente:

4. Las violaciones de seguridad en el ámbito de los sistemas informáticos que pudieran afectar a datos de carácter personal serán puestas en conocimiento de la Delegación de Protección de Datos de la Generalitat por parte del órgano directivo con competencias en materia de tecnologías de la información y comunicación.

Resulta incompleto en el sentido de que si se pretende cubrir aquellos supuestos en los que se produce una violación de seguridad en los sistema

informáticos, se echa en falta cuando la violación de seguridad se produzca en una parte no automatizada del tratamiento de datos.

Por otra parte, respecto de lo indicado sobre la intervención de la Delegación de Protección de Datos, debe tenerse en cuenta las funciones que le son propias y que si bien en el artículo 39.1 RGPD no se determina expresamente su intervención en las violaciones de seguridad, resultaría acorde con las funciones de supervisión que intervenga en las mismas.

Por lo tanto, se propone la eliminación de la última frase del apartado *“pudiéndose recabar el asesoramiento de la Delegación de Protección de Datos de la Generalitat en la valoración de dicho riesgo”*, pues no aporta valor añadido resultando innecesaria dicha mención.

En el artículo 12 referido al “Encargado del tratamiento” se recuerdan las obligaciones derivadas del artículo 28 del RGPD, indicando lo siguiente:

1. Cuando vaya a realizarse un contrato, encargo a medio propio, encomienda de gestión o convenio, que conlleve que la otra parte, para desarrollar sus funciones, tenga que tratar datos de carácter personal por cuenta de la administración de la Generalitat o entidades de su sector público instrumental, deberán adoptarse medidas que garanticen que el encargado del tratamiento ofrece garantías suficientes de cumplimiento de la normativa de protección de datos y se formalizará de acuerdo con lo previsto en el artículo 28 del Reglamento (UE) 2016/679.

En este aspecto es preciso recordar lo indicado en el Considerando 81 del RGPD:

Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable.

Teniendo en cuenta lo anterior, se observa que en la regulación sometida a informe se hace especial hincapié en la adopción de medidas que garanticen que el encargado ofrece en las “garantías suficientes” de cara al cumplimiento de la normativa de protección de datos, lo que se valora positivamente.

Ahora bien, y sin perjuicio de lo indicado en el artículo 28.3 h) del RGPD, sería recomendable para dar efectivo cumplimiento al principio de responsabilidad activa, que dichas medidas se documentasen a los efectos de darle mayor efectividad y ser susceptibles de control y evaluación posterior. Ya que de otro modo se asume el riesgo de que dicha mención se reduzca a un mero formalismo. Por lo que, se propone la siguiente inclusión en el precepto:

(...) deberán adoptarse y documentarse, las medidas que garanticen que el encargado del tratamiento ofrece garantías suficientes de cumplimiento de la normativa de protección de datos y se formalizará de acuerdo con lo previsto en el artículo 28 del Reglamento (UE) 2016/679.
(...)

En el apartado 3 se aborda la transitoriedad de los contratos anteriores que puedan no cumplir el régimen jurídico del encargado del tratamiento, estableciendo la obligación de adoptar una resolución o acto jurídico con el contenido del artículo 28 del RGPD.

Pues bien, debe recordarse lo dispuesto en la Disposición Transitoria Quinta de la LOPDGDD que a tal efecto dispone que:

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022. Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Por lo tanto, y teniendo en cuenta que ya se ha sobrepasado la fecha indicada en la citada Disposición Transitoria Quinta de la LOPDGDD, los contratos celebrados a partir de la misma deben cumplir lo dispuesto en el artículo 28 del RGPD, por lo que se propone la eliminación del apartado 3 del proyecto de decreto sometido a informe.

Finalmente, los artículos 13 y 14 están dedicados a las “Auditorías” y a las “obligaciones del personal en relación con la protección de datos” respectivamente.

Únicamente se realizan la siguientes consideraciones del artículo 13 a cuyo tenor:

En las políticas internas de protección de datos se adoptará un plan de auditorías interno, con la finalidad de comprobar el cumplimiento de la normativa de protección de datos dentro de su organización.

Asimismo, se deberá tener a disposición de la autoridad de control y de la Delegación de Protección de Datos de la Generalitat toda la información que acredite el cumplimiento del Reglamento (UE) 2016/679 y de la ley Orgánica 3/2018, de 5 de diciembre.

Frente a ello debe indicarse señalarse que el cumplimiento normativo corresponde a cada responsable del tratamiento y no a un plan de auditorías interno, ya que éste debería definirse de acuerdo a las necesidades de cada tratamiento y no a una política general o específica de cada consejería.

El actual modelo de responsabilidad activa demanda que se pueda dar respuesta caso a caso de cada tratamiento en función de su naturaleza, ámbito o alcance, contexto y fines.

Por lo que tal como está redactado el precepto, parece que, de nuevo, se vuelve al modelo anterior de cumplimiento propio de la Directiva 95/46 y de la LOPD de 1999.

X

El Título III aborda la “Estructura en materia de protección de datos”, respecto del que se realizan las siguientes consideraciones:

Se observa que el Decreto distingue dos grandes elementos en la estructura que pretende regular, por un lado el responsable del tratamiento, con sus distintos niveles de responsabilidad y competencia (Capítulo I “Organización en las consellerías y en el sector público instrumental; Capítulo II “Organización de la protección de datos de carácter personal en los centros sanitarios, docentes y de servicios sociales”) y por otro lado, el referido al Delegado de Protección de Datos (Capítulo III “Delegación de Protección de Datos”; Capítulo IV “Grupos de trabajo en materia de protección de datos).

Como punto de partida debe tenerse en cuenta lo indicado en las Directrices “Sobre los Delegados de Protección de Datos” de 05/04/2017 del Grupo de Trabajo del Artículo 29 actualmente sustituido por CEPD, que indica que:

Los DPD no son personalmente responsables en caso de incumplimiento del RGPD. El RGPD deja claro que es el responsable o el encargado del tratamiento quien está obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con sus disposiciones (artículo 24, apartado 1). El cumplimiento de las

normas sobre protección de datos es responsabilidad del responsable o del encargado del tratamiento.

Esto significa que, en el desempeño de sus tareas con arreglo al artículo 39, no debe instruirse a los DPD sobre cómo abordar un asunto, por ejemplo, qué resultado debería lograrse, cómo investigar una queja o si se debe consultar a la autoridad de control. Asimismo, no se les debe instruir para que adopten una determinada postura con respecto a un asunto relacionado con la ley de protección de datos, por ejemplo, una interpretación concreta de la ley.

No obstante, la autonomía de los DPD no significa que tengan poder para adoptar decisiones más allá de sus funciones, definidas con arreglo al artículo 39. El responsable o el encargado del tratamiento sigue siendo responsable del cumplimiento de la normativa de protección de datos y debe ser capaz de demostrar dicho cumplimiento (...)

Asimismo, otro aspecto fundamental a tener en cuenta se encuentra en el artículo 38.3 y 6 del RGPD, a cuyo tenor:

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

En este sentido, en las citadas Directrices “Sobre los Delegados de Protección de Datos” de 05/04/2017, se indica que:

La ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso. Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director

de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento.

Asimismo, la STJUE de 9 de febrero de 2023, Asunto C-453/21, indica lo siguiente:

33. (...) el RGPD tiene por objeto garantizar un nivel elevado de protección de las personas físicas dentro de la Unión por lo que respecta al tratamiento de sus datos personales, y que, para lograr ese objetivo, el delegado de protección de datos debe estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

41 (...) conforme al objetivo perseguido por el artículo 38, apartado 6, del RGPD, no se puede encomendar al delegado de protección de datos la ejecución de funciones o de cometidos que puedan perjudicar el desempeño de las funciones que ejerce como delegado de protección de datos.

44 (...) no se pueden encomendar a un delegado de protección de datos funciones o cometidos que le lleven a determinar los fines y los medios del tratamiento de datos personales del responsable del tratamiento o de su encargado. En efecto, conforme al Derecho de la Unión o al Derecho de los Estados miembros en materia de protección de datos, el control de esos fines y medios debe ser efectuado de manera independiente por dicho delegado.

45. La determinación de la existencia de un conflicto de intereses, en el sentido del artículo 38, apartado 6, del RGPD, debe efectuarse caso por caso, sobre la base de una apreciación del conjunto de las circunstancias pertinentes, en particular, de la estructura organizativa del responsable del tratamiento o de su encargado y a la luz de toda la normativa aplicable, incluidas las eventuales políticas de estos últimos.

Sobre las relaciones entre el responsable del tratamiento y el delegado de protección de datos, el Informe 38/2023 indica, entre otras cuestiones lo siguiente:

(...) conforme al principio de responsabilidad proactiva, es el responsable del tratamiento o, en su caso, el encargado del tratamiento, el obligado a garantizar y ser capaz de demostrar que el tratamiento se realiza de conformidad con las disposiciones del RGPD (artículo 5.2 y 24.1 del RGPD). Asimismo, es a ellos a quienes el RGPD impone

obligaciones específicas, jurídicamente exigibles y cuyo incumplimiento genera la correspondiente responsabilidad, a diferencia del DPD quien no es personalmente responsable en caso de incumplimiento del RGPD.

En este sentido nos pronunciamos ya en nuestro Informe 37/2020:

En relación con la primera de las distinciones, el RGPD es claro a la hora de imponer al responsable del tratamiento la obligación de cumplimiento de las medidas que el mismo prevé. Será así el responsable quien deba mantener un registro de operaciones de tratamiento, evaluar el riesgo concurrente en un determinado tratamiento de datos o desarrollar en su caso a evaluación de impacto exigida por el reglamento. Del mismo modo, será el que habrá de determinar las medidas técnicas y organizativas que hayan de adoptarse para garantizar la seguridad del tratamiento. Lógicamente, estas medidas se desarrollarán por quienes las tuvieran atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos que participen activamente en la implantación de las medidas de seguridad de la información y, particularmente, el responsable de seguridad.

Frente a lo que acaba de indicarse, la función del delegado de protección de datos será la de prestar al responsable la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas y supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el delegado de protección de datos asesora al responsable y controla el cumplimiento de las obligaciones establecidas por la normativa de protección de datos de carácter personal.

En este sentido, el documento de directrices WP243, adoptado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, señala que “El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar «medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (artículo 24, apartado 1). El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD”.

Por consiguiente, corresponde al responsable o al encargado del tratamiento adoptar las decisiones oportunas para garantizar el cumplimiento del RGPD, estableciendo, en virtud de su autonomía organizativa, la estructura que estime adecuada a estos efectos.

Asimismo, corresponde al responsable velar por el cumplimiento de las disposiciones del RGPD relativas al nombramiento, posición jurídica y funciones que corresponden al DPD, quien deberá contar con la autonomía y los recursos suficientes para desarrollar su labor de forma efectiva.

En este sentido, tal y como ha señalado reiteradamente esta Agencia, el DPD está llamado a desempeñar un papel fundamental dentro del nuevo modelo de responsabilidad proactiva, si bien sus funciones deben ajustarse a la naturaleza asesora y supervisora que al mismo le corresponde (...)

(...) tanto en el ejercicio de sus funciones asesoras y supervisoras, si el responsable o encargado no atiende a los criterios del DPD recogidos en sus informes o en sus recomendaciones, las Directrices sobre delegados de protección de datos recomiendan, como buena práctica *“documentar los motivos por los que no se sigue el consejo del DPD”*.

(...) la asignación de otras tareas deberá respetar, en todo caso, el carácter asesor y supervisor del DPD, sin que puedan implicar la intervención directa en la toma de decisiones referidas a los fines y medios del tratamiento, que afectaría a su independencia e implicarían la existencia de un conflicto de intereses. De este modo, la necesaria independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estaría sujeto a instrucciones de otros órganos.

(...) Por consiguiente, deben diferenciarse claramente dentro de una organización el ejercicio de las funciones de carácter decisorio que le corresponden en su condición de responsable o encargado del tratamiento, evitando los conflictos de interés al DPD en el ejercicio de sus funciones asesoras y supervisoras, quien precisamente por la naturaleza de estas funciones no está sujeto a responsabilidad por el incumplimiento del RGPD.

Teniendo en cuenta lo que se acaba de indicar, del texto del proyecto de Decreto se observa que se mezclan y solapan funciones por parte del “aparato

organizativo” del responsable del tratamiento que serían propias del Delegado de Protección de Datos.

A tal efecto, debe tenerse claro que, a grandes rasgos, el responsable del tratamiento toma decisiones sobre el tratamiento de datos personales y el delegado de protección de datos, asesora y propone a aquel en la toma de dichas decisiones, y a tal efecto, realiza una labor de supervisión para fundamentar dicho asesoramiento.

En este sentido en el Informe 11/2019 se indica que: *las principales funciones de los Delegados de Protección de Datos se refieren a la información, asesoramiento y supervisión en los tratamientos de datos de carácter personal realizados por las organizaciones -públicas y/o privadas- en las que se enmarque su actividad, así como de relación, interlocución y contacto con las autoridades de control, con los responsables y encargados de los tratamientos, y con los propios afectados por dichos tratamientos.*

Así se desprende de lo indicado en el artículo 39.1 del RGPD a cuyo tenor:

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:
 - a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
 - b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
 - c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
 - d) cooperar con la autoridad de control;
 - e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a

que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Título III del proyecto sometido a informe lleva por denominación “Estructura en materia de Protección de Datos” en el que se establece el aparato administrativo en que se articula el responsable del tratamiento.

Como punto de partida debe indicarse que las obligaciones del responsable del tratamiento en materia de protección de datos (que no funciones) ya están previstas tanto en el RGPD como en la LOPDGDD. Es decir, en el marco jurídico actual se define la posición jurídica del responsable y las obligaciones que le son inherentes a tal condición, sin que existan como tal una serie de funciones que deba tener.

Dicho esto, las funciones descritas en los artículos 16 a 21 que se atribuyen a los órganos y titulares que se citan (todos ellos dependientes del responsable del tratamiento), son de supervisión, asesoramiento y propuesta, y, además, teniendo en cuenta el principio de jerarquía, y sin perjuicio de que no son formalmente un DPD, pero podría considerarse que actúan como tal, puede resultar contraria al conflicto de intereses e independencia, pues en definitiva asesoran a órganos superiores respecto de los que dependen jerárquica y funcionalmente.

Sirva citar algunos ejemplos de lo indicado, el artículo 16, bajo la denominación “órganos con funciones directivas en materia de protección de datos” indica lo siguiente (el subrayado es nuestro):

1. Corresponde a la persona titular de la Subsecretaría, así como a la persona con capacidad de dirección y funciones transversales que designe el órgano competente de cada entidad del sector público instrumental, las siguientes funciones en el ámbito de la protección de datos:

a) Proponer al responsable del tratamiento la política interna de protección de datos de carácter personal de su organización.

b) Supervisar la adecuada gestión y cumplimiento de la política interna de protección de datos en su organización, así como la correcta implantación de las medidas técnicas y organizativas necesarias para cada tratamiento, de acuerdo con el resultado de los análisis de riesgos y, en su caso, las evaluaciones de impacto realizadas. (...)

3. Los órganos superiores y directivos, incluidos los de los apartados 1 y 2 de este artículo, y en el ámbito material asignado en el correspondiente reglamento orgánico y funcional, deberán garantizar

que los tratamientos de datos personales cumplen las condiciones que establece la normativa en esta materia y, en particular, desarrollar las siguientes funciones:

- a) Supervisar que sus unidades dependientes realizan los análisis de riesgos y, en su caso, las evaluaciones de impacto de los tratamientos de su ámbito de competencia.
- b) Velar por el cumplimiento de las medidas técnicas y organizativas apropiadas que garanticen los derechos de la ciudadanía en lo relativo al tratamiento de sus datos de carácter personal.
- c) Supervisar que sus unidades dependientes participan en el cumplimiento de los principios de protección de datos, la gestión del deber de informar, el mantenimiento del Registro de Actividades de Tratamiento, el ejercicio de derechos de la ciudadanía y la gestión de las violaciones de la seguridad de los datos de carácter personal.

En términos similares se encuentra lo indicado en el artículo 17 al regular “las unidades de protección de datos” y en los sucesivos sobre la organización en los centros sanitarios, docentes y de servicios sociales.

A lo que hay que añadir que, los órganos y/o sus titulares de los sujetos mencionados en los preceptos a los que se ha hecho la oportuna remisión, derivado de su posición en la organización, no dejan de tener poder de decisión en determinados ámbitos, confluyendo en las mismas personas y/o organismos la toma de decisiones que tengan influencia en el tratamiento de datos con las figura de asesor sobre protección de datos. (aún sin dicha designación formal).

En definitiva, las funciones descritas en los artículos 16 a 21, son más propias del aparato organizativo de un delegado de protección de datos, que de un responsable del tratamiento.

Si bien es cierto que el DPD *no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales* (Directrices Sobre los Delegados de Protección de Datos” de 05/04/2017) a la inversa no existe una prohibición en ese sentido, que es lo que sucede en la regulación sometida a informe. Es decir, que parte del aparato administrativo del responsable del tratamiento ejerza funciones propias de un DPD.

Así, no se deduce con absoluta claridad cómo coexisten los “criterios” de supervisión de estas unidades, con los “criterios” de supervisión y asesoramiento del propio DPD.

Finalmente, y también en relación con esta asunción de funciones propias del responsable del tratamiento por parte de terceros, hemos de detenernos en el artículo 25 que bajo la denominación “Seguridad de los datos” nos indica lo siguiente:

1. En el ámbito de sus competencias, la Delegación de Protección de Datos y los órganos con competencias en materia de seguridad de la información, establecerán directrices claras e integradas respecto a la seguridad de los tratamientos de los datos de carácter personal.

Frente a ello debe señalarse que tal como está redactado el precepto, parece que son el DPD y el responsable de seguridad quien adopta decisiones, y debe recordarse que éstos cometidos corresponden únicamente al responsable del tratamiento, que es el obligado por la norma.

En efecto, los órganos con competencia en seguridad no pueden tomar decisiones, sino que, en su caso, realizarán propuestas para someterlas al responsable.

En relación con esto, también debe traerse a colación lo dispuesto en la Disposición Transitoria Segunda que bajo la denominación “Comunicación a la Delegación de Protección de Datos, dispone lo siguiente:

La designación de la unidad administrativa que se constituya como unidad de protección de datos deberá ser comunicada a la Delegación de Protección de Datos de la Generalitat en el plazo máximo de dos meses desde la entrada en vigor de este decreto.

Si transcurrido dicho plazo no se ha producido dicha comunicación, se entenderá que asume las funciones de la unidad de protección de datos el Administrador de Seguridad de los Ficheros de Datos de Carácter Personal, nombrado de conformidad con el artículo 15 del Decreto 130/2012, de 24 de agosto, salvo en la conselleria competente en materia de sanidad, que será el órgano con funciones análogas previsto en la Orden 9/2012, de 10 julio, de la Conselleria de Sanidad, por la que establece la organización de la seguridad de la información.

De la lectura de la disposición se infiere, de nuevo, la posibilidad de que el responsable de seguridad asuma las funciones de Delegado de Protección de Datos, lo que resulta contrario al esquema básico de funciones, competencias y relaciones entre el responsable del tratamiento, el delegado de protección de datos, y el responsable de seguridad.

En conclusión, visto que se plantean más dificultades que ventajas o soluciones, la valoración de los preceptos analizados referidos al apartado

administrativo en protección de datos, en el proyecto sometido a informe ha de ser desfavorable.

Por tanto, la regulación analizada resulta contraria al espíritu de la norma, es decir, del RGPD que, como se ha dicho antes “tiene por objeto garantizar un nivel elevado de protección de las personas físicas dentro de la Unión por lo que respecta al tratamiento de sus datos personales, y que, para lograr ese objetivo, el delegado de protección de datos debe estar en condiciones de desempeñar sus funciones y cometidos de manera independiente” (STJUE de 9 de febrero de 2023, Asunto C-453/21).

Al atribuirse funciones de asesoramiento y supervisión a una estructura administrativa en la que no se incardina el “asesor cualificado” en materia de protección de datos, (esto es, al Delegado de Protección de Datos) se está avalando jurídicamente, a través de una norma reglamentaria de ámbito autonómico, la asunción por parte de terceros de las funciones del Delegado de Protección de Datos previstas en un Reglamento Europeo, cuyo rango normativo y posición en nuestro ordenamiento jurídico no puede dejar de observarse.

De la regulación analizada podría quebrarse el esquema básico del modelo de responsabilidad activa, en el que corresponde en última instancia al responsable del tratamiento la toma de decisiones en materia de protección de datos, previo asesoramiento en su caso del delegado de protección de datos y con las recomendaciones del personal responsable de la seguridad de la información.

De ahí que debe rechazarse cualquier disposición que implique que las atribuciones de éstos no estén perfectamente delimitadas o que puedan solaparse unas con otras.

Dicho lo anterior, en cuanto al Capítulo III del proyecto de Decreto, se considera conforme a los límites de la potestad de autoorganización de las administraciones públicas, y de los criterios establecidos en el Informe 38/2023, en el sentido de que **el responsable del tratamiento ha de haber proporcionado al Delegado de Protección de datos, de los medios adecuados, entre los que se encuentra la creación de una estructura administrativa** como la que consta en el texto analizado.

El modo o manera de configurar la figura del Delegado de Protección de datos, en cuanto a estructura, vínculo jurídico, etc.... responde al criterio del responsable del tratamiento como otra manifestación más del principio de responsabilidad activa.

Ejemplo de esta libertad de configuración del delegado de protección de datos lo encontramos en el artículo 34.5 de la LOPDGDD que dispone que:

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Así, resultan válidas múltiples fórmulas, siempre que se cumpla lo indicado en el RGPD en cuanto al estatus, posición y funciones del Delegado.

En este sentido en el Informe 37/2020 se extraen las siguientes conclusiones:

En conclusión, dichas funciones podrán desarrollarse eficazmente si se cumple con los requisitos de capacitación al proceder a la designación del DPD y se le dota de los recursos necesarios, incluido, como señala el Grupo del Artículo 29 un equipo de DPD (un DPD y su personal), equipo que deberá ser proporcional al tamaño y estructura de la organización, así como a la sensibilidad, complejidad y cantidad de los datos que una organización trata, debiendo garantizarse la disponibilidad del DPD de modo que los interesados puedan contactar con él, así como comunicarse con las autoridades de protección de datos.

(...)

Finalmente, en el citado Informe 38/2023, y en cuanto a la posición en la organización y los elementos que debe tener en cuenta el responsable del tratamiento, se indicaba lo siguiente:

(...) en relación con el encuadramiento del DPD dentro de la estructura del responsable, se trata, de nuevo, de una cuestión organizativa que puede adoptarse libremente por el responsable o encargado del tratamiento, con el único límite de respetar la independencia funcional del DPD, que exige que el delegado no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones y rinda cuentas directamente al más alto nivel jerárquico del responsable o encargado del tratamiento.

(...) No obstante, la necesidad de rendir cuentas directamente al más alto nivel jerárquico, así como ese apoyo que debe prestar la alta dirección, no implica necesariamente que el DPD deba depender directamente del máximo órgano de dirección o administración, sino que podrá depender de otros órganos siempre que tenga el nivel adecuado

dentro de la estructura del responsable o encargado para permitirle el adecuado ejercicio de sus funciones y se garantice su independencia funcional y la ausencia de conflictos de interés.

En conclusión, dentro de la libertad que confiere la potestad autoorganizativa de la administración pública, nada obsta a que se determine en la estructura que conforma el responsable del tratamiento, otros niveles o departamentos que puedan participar en la determinación de los fines y de los medios del tratamiento y que en cierta medida asesoren y propongan al responsable la adopción de las medidas que estimen adecuadas, pero siempre tendrán que estar perfectamente diferenciadas de las del Delegado de Protección de datos, para así evitar que se confundan con las propias de asesoramiento de éste.