N/REF: 0046/2019

La consulta plantea la adecuación al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD en los sucesivo) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo) de la puesta en marcha del programa de ACCESO A FONDOS DOCUMENTALES Y OBRAS (ATOPO) de la Diputación de Pontevedra.

I

Según manifiesta la consultante, la ejecución del programa ATOPO, supone la publicación, -y por tanto el acceso de los ciudadanos- de información proveniente de diversas fuentes, tales como repositorio de colecciones y fondos documentales, bibliográficos, cartográficos y audiovisuales, depositados en el Museo de Pontevedra, en el Servicio de Patrimonio Documental y Bibliográfico, e incluso procedentes (a través de los correspondientes convenios) de los archivos municipales y de otras instituciones, públicas o privadas, de la provincia.

Asimismo se pretende facilitar el acceso de modo universal, directo, sin identificación ni autorización, previa definición de los límites y condiciones de otras normativas aplicables entre las que se encuentra la de protección de datos personales. Para lo que centra la consulta en los siguientes aspectos:

a) El tratamiento de datos personales de fallecidos;

b) La integración y aplicación del artículo 12 y siguientes, de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG) en relación con el RGPD y LOPDGDD, y en relación con el régimen de plazos establecido en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE) y la Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia;

c) La publicación de imágenes con carácter general y la publicación de imágenes de menores de edad.

II

Como punto de partida debe acudirse a la definición de tratamiento a los efectos si la ejecución del programa ATOPO puede considerarse como tal.

El artículo 4. 2 RGPD cuando define tratamiento de datos, incluye la *(…)consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión(…).*

Por tanto, una vez considerada la existencia de tratamiento debe analizarse lo dispuesto en el artículo 6 del RGPD que determina aquellos supuestos en que el tratamiento de datos personales se considera lícito:

> *1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
>
> *a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
>
> *b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
>
> *c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
>
> *d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
>
> *e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
>
> *f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*
>
> *Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.*

La consultante indica, en síntesis, que la ejecución del programa ATOPO, forma parte de un *mandato legal* que se encuentra en la (i) Directiva 2003/98/CE del Parlamento Europeo y del Consejo (y su transposición a través de la *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público*), (ii) en las distintas leyes de transparencia de ámbito estatal y autonómica, y (iii) en la normativa que regula el acceso a documentos y archivos.

En base a dicha consideración podría legitimarse el tratamiento consistente en la puesta en marcha del programa ATOPO, en los supuestos previstos en las letras c) y e) del apartado 1 del artículo 6, referidos al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. A ese respecto los apartados 2 y 3 del citado artículo establecen lo siguiente:

> *2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras*

c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX.

El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Teniendo en cuenta lo indicado en dichos apartados, conviene analizar las disposiciones del Derecho de la Unión y del Derecho nacional que son de aplicación a las posibles bases jurídicas que, a priori, podrían considerarse adecuadas.

III

En primer lugar, debe tenerse en cuenta lo indicado en el Considerando 154 RGPD que dispone lo siguiente:

El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. (…). La Directiva 2003/98/CE del Parlamento Europeo y del Consejo (14) no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los

> *Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.*

Por su parte, el articulo 86 RGPD dispone que:

> *Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.*

De acuerdo con lo expuesto, conviene adelantar ya que si bien el principio de acceso público a los documentos oficiales puede considerarse de interés público, la ejecución de dicho principio ha de realizarse teniendo en cuenta el Derecho de la unión o el derecho nacional, siempre y cuando se observen las garantías y niveles de protección que el propio RGPD otorga a los titulares de los datos.

En ese sentido, se ha de poner de manifiesto que la Directiva 2003/98/CE del Parlamento Europeo y del Consejo sobre reutilización de informacion del sector público, no merma la eficacia de la protección que el RGPD establece.

IV

En cuanto al régimen jurídico de la reutilización de informacion del sector público, debe partirse de la citada *Directiva 2003/98/CE*, *relativa a la reutilización de la información del sector público (Directiva ISP)* que la consultante invoca para la ejecución del programa ATOPO:

Conviene destacar lo indicado en los considerandos 9 y 21:

> *(9)La presente Directiva no contiene la obligación de autorizar la reutilización de documentos. La decisión de autorizar o no la reutilización corresponderá a los Estados miembros o al organismo del sector público que corresponda.*
>
> *(21) La presente Directiva se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

Por su parte, en el artículo 1 apartados 2 y 4 dispone lo siguiente:

2. La presente Directiva no se aplicará a: (…)los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales;

4. La presente Directiva no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y nacional, y, en particular, no altera las obligaciones ni los derechos establecidos en la Directiva 95/46/CE.

Conviene citar lo indicado en el *Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público*, del Grupo de Trabajo del artículo 29 (en la actualidad sustituido por el Comité Europeo de Protección de Datos) que recoge lo siguiente:

(…)La Directiva ISP obliga ahora a los organismos del sector público a permitir la reutilización de toda la información pública que posean. Sin embargo, como se expondrá a continuación, no impone a estos organismos la obligación de divulgar públicamente información personal. Únicamente prevé la reutilización de la información si ya es de acceso público con arreglo a la legislación nacional, e incluso entonces, solamente si dicha reutilización no va en detrimento de las disposiciones de la legislación de protección de datos aplicable(…)

(…)el «principio de reutilización» no es automático cuando está en juego el derecho a la protección de los datos personales, y no anula las disposiciones aplicables de la normativa sobre protección de datos. Cuando los documentos en poder de los organismos del sector público contienen datos personales, su reutilización está incluida en el ámbito de aplicación de la Directiva 95/46/CE y, por tanto, está sujeta a la normativa sobre protección de datos aplicable.

Por tanto, en los casos en que la reutilización incluye datos personales, el organismo del sector público no puede invocar sistemáticamente la necesidad de cumplir con la Directiva ISP como razón legítima para facilitar datos para su reutilización. (…)

(…)El artículo 1, apartado 2, letra c quater, contempla los tres siguientes casos, todos ellos excluidos del ámbito de aplicación de la Directiva *ISP:*

-los documentos a los que no pueda accederse en virtud de regímenes de acceso por motivos de protección de los datos personales;

-los documentos cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales;

> *-y «las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales». (…)*
>
> *(…)Las decisiones relativas a la reutilización de datos personales de conformidad con las disposiciones de la Directiva ISP deberán tomarse caso por caso, y también es preciso establecer medidas legales, técnicas u organizativas adicionales para proteger a las personas interesadas.*
>
> *La reutilización de los datos personales está y debe estar limitada por:*
>
> *-disposiciones generales de la legislación aplicable en materia de protección de datos; (en su caso) restricciones jurídicas adicionales específicas;*
>
> *-garantías técnicas y organizativas que se hayan establecido para proteger los datos personales. (…)*

La transposición al derecho nacional de la citada Directiva se recoge en la *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público,* que en su exposición de motivos nos indica:

> *El régimen de reutilización garantiza el pleno respeto de los principios que consagran la protección de datos personales, en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo.*

Conviene destacar lo indicado en los *apartados 3 y 4 de su artículo 3* que disponen lo siguiente:

3. La presente Ley no será aplicable a los siguientes documentos que obren en las Administraciones y organismos del sector público previstos en el artículo 2:

> *a) Los documentos sobre los que existan prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico.*
>
> *(…)*
>
> *j) Los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, de conformidad con la normativa vigente y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la*

legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(…)

4. En ningún caso, podrá ser objeto de reutilización, la información en que la ponderación a la que se refieren los artículos 5.3 y 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, arroje como resultado la prevalencia del derecho fundamental a la protección de datos de carácter personal, a menos que se produzca la disociación de los datos a la que se refiere el artículo 15.4 de la citada Ley.

Por último, en cuanto al *régimen administrativo* de la reutilización, el articulo 4 en su apartado 6 dispone lo siguiente:

6. La reutilización de documentos que contengan datos de carácter personal se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

V

Por su parte, la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno* (LTAIBG) en cuanto a la *publicidad activa*, en su artículo 5 apartados 1 y 3 bajo la rúbrica "*Principios generales"* nos indica:

1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos

En cuanto al acceso a la información respecto del derecho de acceso previsto en el artículo 12, y el régimen de *protección de datos personales*, dispone en su artículo 15 lo siguiente:

1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el ***consentimiento expreso y por escrito del afectado****, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.*

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el

*acceso solo se podrá autorizar en caso de que se cuente **con el consentimiento expreso** del afectado o si aquel estuviera **amparado por una norma con rango de ley.***

2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

*Para la realización de la citada **ponderación**, dicho órgano tomará particularmente en consideración los siguientes criterios:*

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

Procede citar a continuación lo recogido en el Informe CI/001/2020 de 5 de marzo de 2020 del Consejo de Transparencia y Buen Gobierno y la AEPD, sobre los distintos niveles de protección que ofrece la LTAIBG para los datos de carácter personal:

(…)El artículo 15 de la LTAIBG reconoce pues, un distinto nivel de protección en función de la naturaleza de los datos personales que contenga la información que vaya a ser objeto de publicación2 o a la que se solicita acceso.

Así, para las actualmente denominadas "categorías especiales de datos personales", el artículo 9 del RGPD realiza una diferenciación entre

— Datos relativos a la ideología, afiliación sindical, religión o creencias. El acceso a estos datos requerirá el consentimiento expreso y por escrito de su titular salvo que éste los haya hecho manifiestamente públicos con anterioridad a la solicitud de acceso.

— Datos relacionados con el origen racial, la salud o la vida sexual, o incluyese datos genéticos o biométricos, o relativos a la comisión de infracciones penales o administrativas que no conlleven amonestación pública al infractor, en cuyo caso será necesario el consentimiento expreso del titular de los datos, salvo que el acceso esté amparado en una Ley.

Por otra parte, con carácter general, cuando la información personal venga referida a datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano, será posible el acceso salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida (art. 15.2 LTAIBG). En este sentido, y a efectos aclaratorios, debe recordarse lo ya indicado en el criterio interpretativo nº 1 ya citado, CI/0014/2015, de 24 de junio de 2015.

El art. 5.3 de la LTAIBG dispone que "Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos".

Finalmente, en el caso en que la información afecte a datos de carácter personal que no tengan esa consideración de meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano ni pueda predicarse de ellos la naturaleza de categorías especiales de datos (art. 9 RGPD) o relativos a la comisión de infracciones penales o administrativas que no conlleven amonestación pública al infractor, será necesaria la debida ponderación entre derechos que viene referenciada en el apartado 3 del art. 15 de la LTAIBG. (…)

Teniendo en cuenta lo anterior, la ponderación entre el derecho a la protección de datos y el acceso a la información pública podrá diferir en los supuestos en que una determinada información fuera objeto de *publicidad activa (artículo 5.3 LTAIBG)*o de una concreta *solicitud de acceso (artículo 15.3 LTAIBG)*, por cuanto el efecto intrusivo del conocimiento de los datos sería distinto atendiendo a su publicación generalizada

o a su conocimiento limitado a un destinatario concreto de la información. De ello se desprende lo siguiente:

> La reutilización de la información objeto de publicidad activa, siempre y cuando se haya efectuado correctamente la ponderación entre la finalidad de transparencia y la garantía del derecho fundamental a la protección de datos de carácter personal, conforme a lo exigido por el artículo 5.3 de la LTAIBG, podrá, como regla general, llevarse a cabo.
>
> Por el contrario, esta regla no operará necesariamente en los supuestos en que la información pueda ser objeto de comunicación ante una solicitud individual de acceso a la misma, debiendo en ese caso tenerse en cuenta si los criterios aplicados para considerar procedente la solicitud podrían ser igualmente tenidos en cuenta en caso de que se pretendiese la reutilización de la información.
>
> Finalmente, como última consecuencia de lo mencionado, en caso de que no procediera la comunicación del dato por aplicación de los criterios establecidos en el artículo 15 de la LTAIBG, incluso en los supuestos de petición individualizada de acceso, la información no podría ser objeto de reutilización salvo que se procediera a su previa disociación, conforme a los artículos 15.4 de la LTAIBG y 3.4 de la Ley 37/2007.

Por lo tanto cabe concluir ,en primer lugar, que la Directiva ISP y la Ley 37/2007, no legitiman por sí mismas la difusión de datos personales ya que su tratamiento se rige por la normativa de protección de datos, es decir, el RGPD y la LOPDGDD.

Y en segundo lugar, que la decisión sobre la reutilización de la información del sector público está condicionada por las limitaciones incluidas en la LTAIBG, en lo que afectan al tratamiento de datos personales, tal y como exige el artículo 3.4 de la Ley 37/2007.

Es decir, al contrario de lo que se indica en la consulta, no existe la obligación de publicar "*el proyecto que se está tramitando"* y tampoco frente a los limites indicados, *cabe oponer* el artículo 15 de la LTAIBG como propone la consultante, en cuanto a que *se permite el acceso a datos de carácter personal especialmente protegidos si se encuentra amparado por una ley* por remisión a la LPHE (artículo 57) o a la Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia, pues como más adelante se analizan, precisamente estos preceptos establecen límites y salvaguardas cuando la publicación contenga datos personales.

VI

Procede a continuación a analizar lo dispuesto en la normativa referente a los archivos y documentos que forman parte del patrimonio documental. Establece la Ley 16/1985, de 25 de junio, del Patrimonio Histórico, en sus artículos 49, 59 y 57 lo siguiente:

Artículo 49

1. Se entiende por documento, a los efectos de la presente Ley, toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos. Se excluyen los ejemplares no originales de ediciones.

2. Forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios.

Artículo 59

1. Son Archivos los conjuntos orgánicos de documentos, o la reunión de varios de ellos, reunidos por las personas jurídicas, públicas o privadas, en el ejercicio de sus actividades, al servicio de su utilización para la investigación, la cultura, la información y la gestión administrativa. Asimismo, se entienden por Archivos las instituciones culturales donde se reúnen, conservan, ordenan y difunden para los fines anteriormente mencionados dichos conjuntos orgánicos.

Artículo 57

1. La consulta de los documentos constitutivos del Patrimonio Documental Español a que se refiere el artículo 49.2 se atendrá a las siguientes reglas:

a) Con carácter general, tales documentos, concluida su tramitación y depositados y registrados en los Archivos centrales de las correspondientes entidades de Derecho Público, conforme a las normas que se establezcan por vía reglamentaria, serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la Defensa del Estado o la averiguación de los delitos.

b) No obstante lo dispuesto en el párrafo anterior, cabrá solicitar autorización administrativa para tener acceso a los documentos excluidos de consulta pública. Dicha autorización podrá ser concedida, en los casos de documentos secretos o reservados, por la Autoridad que hizo la respectiva declaración, y en los demás casos, por el Jefe del Departamento encargado de su custodia.

c) Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años a partir de la fecha de los documentos.

Por su parte, el *Real Decreto 1708/2011, de 18 de noviembre, del Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso*, establece en sus artículos 23, 26 y 28 lo siguiente:

Artículo 23 Derecho de acceso a documentos y archivos

> *1. Toda persona tiene derecho a acceder a los documentos conservados en los archivos incluidos en el ámbito de aplicación de esta norma, en los términos establecidos en el presente capítulo sin perjuicio de las exclusiones y limitaciones previstas en la Constitución y en las leyes.(…)*

Artículo 26 Acceso restringido

> *1. Los documentos conservados en los archivos incluidos en el ámbito de aplicación de esta norma serán de libre acceso, salvo cuando les afecte alguna de las limitaciones previstas en la Constitución y en las Leyes. En particular, serán de acceso restringido los documentos clasificados según lo dispuesto en la normativa sobre secretos oficiales, los documentos que contengan información cuya difusión pudiera entrañar riesgos para la seguridad y la defensa del Estado o interferir en la averiguación de los delitos o la tutela judicial efectiva de ciudadanos e instituciones, así como los declarados reservados por una norma con rango de Ley y aquellos que contengan datos personales a los que se refiere el artículo 28.(…)*

Artículo 28 Solicitud de consulta de documentos de acceso restringido por contener datos personales

> (…)*2. El acceso a los documentos que contengan datos personales que puedan afectar a la intimidad o a la seguridad de las personas, o que tengan la consideración de especialmente protegidos en los términos de la normativa de protección de datos personales, incluyendo los que se encuentren en procedimientos o expedientes sancionadores, será posible siempre que medie el consentimiento expreso y por escrito de los afectados.*
>
> *No obstante, serán accesibles los documentos con datos personales que puedan afectar a la seguridad o intimidad de las personas cuando hayan transcurrido veinticinco años desde el fallecimiento de los afectados. (…)*
>
> *3. El acceso a documentos que contengan datos nominativos o meramente identificativos de las personas que no afecten a su seguridad o su intimidad, será posible cuando el titular de los mismos haya fallecido o cuando el solicitante acredite la existencia de un interés legítimo en el acceso.*
>
> *A estos efectos, se entenderá que poseen interés legítimo quienes soliciten el acceso para el ejercicio de sus derechos y los investigadores que acrediten que el acceso se produce con una finalidad histórica, científica o estadística.*
>
> *4. Se concederá el acceso a documentos que contengan datos de carácter personal, sin necesidad de consentimiento de sus titulares, cuando se proceda*

previamente a la oportuna disociación, de los datos de modo que se impida la identificación de las personas afectadas.

5. La información que contenga datos de carácter personal únicamente podrá ser utilizada para las finalidades que justificaron el acceso a la misma y siempre de conformidad con la normativa de protección de datos.

En cuanto a lo establecido en la normativa autonómica aludida por la consultante, la *Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia* establece en su artículo 23 bajo la rúbrica del "derecho de acceso" apartados 1 y 6, lo siguiente:

1. Todas las personas tienen derecho a acceder a los documentos que forman parte de procedimientos terminados que se custodien en el Sistema de Archivos de Galicia, excepto en aquellos casos en que concurran las excepciones o límites previstos en la Constitución y en las leyes.

(…)

6. Si se trata de documentos que contienen datos personales que puedan afectar a la seguridad, honor, salud, intimidad o imagen de las personas y, en todo caso, a los supuestos de violencia de género, podrán ser objeto de consulta pública si media consentimiento de las personas afectadas, o una vez transcurridos veinticinco años desde su muerte o, si no se conoce la fecha del fallecimiento, cincuenta años desde la producción del documento.

Por lo tanto, la consideración de estar *amparado en una ley* que propone la consultante para permitir la publicación de datos personales debe matizarse en que dicha publicación debe respetar los límites que recoge la propia ley en que pretende ampararse. No es posible realizar una *aplicación parcial* de un texto normativo a satisfacción de la finalidad que se pretenda.

VII

De acuerdo con lo expuesto y como respuesta a la cuestión planteada por la consultante, referida a si prevalece la normativa citada (límites y plazos) o lo indicado en el artículo 12 de la LTAIBG, a cuyo tenor *Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley,* la respuesta ha de ser que si bien el mencionado artículo 12 contiene una formulación general de un derecho, no puede dejar de observarse los límites y plazos que contienen las leyes y reglamentos citados en el presente informe.

Es decir no es admisible, como propone la consultante que por las dificultades para la ejecución del programa ATOPO que supone dar cumplimiento a requisitos de plazos y consentimiento, se establezca la aplicación *ad livitum* del artículo 12 de la LTAIBG, obviando las salvaguardas establecidas en la propia ley de transparencia y en el resto de los cuerpos normativos aplicables.

Asimismo debe indicarse que el tratamiento de datos personales que lleve aparejado la ejecución del programa ATOPO, como los límites y salvaguardas que

recogen las disposiciones aplicables, encuentra su base jurídica, no en el apartado c) del artículo 6.1 RGPD, ya que no estamos ante un" mandato legal" pues las normas que cita en la consulta sirven a la promoción – que no obligación- de la reutilización de información pública, por lo que la base jurídica la encontramos en el apartado e) referido al *tratamiento necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

En este sentido el artículo 8.2 de la LOPDGDD establece: *2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.*

En el presente caso son las distintas leyes de transparencia (estatal y autonómica), la LPHE y su normativa de desarrollo y la Ley 37/2007 de reutilización de información del sector público, las que atribuyen la competencia a la consultante como organismo que se somete al ámbito subjetivo de aplicación de las mismas.

VIII

En cuanto al tratamiento de datos personales de fallecidos, procede citar lo indicado en el Informe 115/2019 que da respuesta a la consulta hoy planteada:

> *Establece el Considerando 27 del RGPD que "El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas." (en términos similares figura en los Considerandos 158 y 160)*
>
> *Consecuencia de esa habilitación, establece el artículo 2 LOPDGDD bajo la rúbrica "Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94" en su apartado 2 lo siguiente:*
>
> > *2. Esta ley orgánica no será de aplicación:*
> >
> > *a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.*
> >
> > *b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.*
> >
> > *c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.*
>
> *Y añade en el artículo 3 de la LOPDGDD, bajo la rúbrica "Datos de las personas fallecidas" en sus apartados 1 y 2 lo siguiente:*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

De lo indicado se desprende que la LOPDGDD no se aplica, al tratamiento de los datos de las personas fallecidas, sin perjuicio de que en su artículo 3 se faculte a determinadas personas el ejercicio de los derechos de acceso, rectificación y supresión, como depositarios de un mandato que el finado hizo en vida, a los efectos de maximizar el derecho a la protección de datos personales.

Como se indicaba en el Informe número 20/2016 de este Gabinete Jurídico la (…)determinación de la muerte de las personas (…) es (…)causa de extinción del derecho a la protección de datos, ya que el artículo 32 del Código Civil dispone que "la personalidad civil se extingue por la muerte de las personas", lo que determinaría, en principio, la extinción con la muerte de los derechos inherentes a la personalidad. (…)

Teniendo en cuenta la inaplicación de la LOPDGDD en el artículo 2.2 y la excepción parcial a esta inaplicación, que propone en su artículo 3, debe acudirse a la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, para determinar en qué medida afecta esa disposición a la consulta planteada.

La Sentencia concreta el contenido del derecho a la protección de datos, indicando que " el derecho a la protección de datos atribuye a su titular un conjunto de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceras obligaciones jurídicas y que sirven a la función que desempeña este derecho fundamental, que es la de garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible imponiendo al tercero los mencionados deberes. Estos son el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos

personales, el derecho a ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales".

De la lectura de la STC 292/2000, podemos afirmar que el contenido del derecho a la protección de datos contempla de un lado, un conjunto de facultades del titular del derecho, y de otro, una serie de obligaciones jurídicas que recaen sobre los terceros que van a tratar los datos personales. Como facultades podemos citar a los efectos pretendidos en la presente consulta, los derechos, como por ejemplo el derecho de acceso y entre las obligaciones o deberes jurídicos, podemos citar que el tratamiento de datos encuentre su base jurídica en algún supuesto del artículo 6 del RGPD y en caso contrario calificarlo como ilícito.

Pues bien, el citado artículo 3 LOPDGDD no hace otra cosa que ampliar o extender en el tiempo algunas de las facultades que forman parte del contenido del derecho a la protección de datos y el artículo 2.2 LOPDGDD, que recoge la inaplicación de la normativa cuando sean datos personales de una persona fallecida, supone el decaimiento de las obligaciones jurídicas (de los terceros) que también forman parte del contenido del derecho a la protección de datos.

(…)

Pero sobre la base de la no aplicación de la LOPDGDD al tratamiento de datos personales de fallecidos, tampoco sería necesario buscar una base jurídica de acuerdo con el artículo 6 del RGPD para avalar la comunicación de datos personales. (…)

De lo expuesto se puede concluir que cuando se trate de datos personales de personas fallecidas, el tratamiento de datos personales que se daría con la publicación no está sometido ni al RGPD ni a la LOPDGDD, sin perjuicio del derecho de los herederos o *autorizados* a ejercer los derechos de acceso, rectificación y supresión en caso de que se den los supuestos legalmente establecidos y los limites referidos al transcurso de los plazos previstos en la LPHE y su normativa de desarrollo y en la Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia.

IX

Otro aspecto que abarca la consulta es la forma de acceso a la información del programa ATOPO, es decir, o bien a través de un acceso generalizado, universal o bien a través de petición individualizada.

De los distintos cuerpos normativos analizados en el presente informe, se deduce que deben coexistir ambos tipos de accesos, el acceso **universal** (*artículo 57.1 a) LPH, y articulo 5.1 LTAIBG,)* y el acceso través de **petición individualizada** (*de un lado el previsto en el artículo 57. 1 b) LPH y el articulo 28 Real Decreto 1708/2011, y de otro el previsto en el artículo 12 LTAIBG),* según nos encontremos ante los distintas normas y supuestos que requieren determinados niveles de protección.

No obstante lo anterior y en relación con el procedimiento puesto en marcha a raíz de una petición individualizada al amparo del derecho de acceso previsto en el artículo 12 de la LTAIBG, debe citarse el artículo 19.3 referido al trámite de audiencia de los afectados que es un aspecto que se cita en la consulta:

> *3. Si la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El solicitante deberá ser informado de esta circunstancia, así como de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación.*

A este respecto, procede citar el Informe CI/001/2020 de 5 de marzo de 2020 del Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos que indican lo siguiente:

> *Relacionado con el mismo (el artículo 19.3) , el apartado 2 del art. 22 LTAIBG, relativo a la formalización del acceso señala que "Si ha existido oposición de tercero, el acceso sólo tendrá lugar cuando, habiéndose concedido dicho acceso, haya transcurrido el plazo para interponer recurso contencioso administrativo sin que se haya formalizado o haya sido resuelto confirmando el derecho a recibir la información".*
>
> *De la lectura conjunta de ambos preceptos y del ya indicado art. 15, puede concluirse lo siguiente:*
>
> > *Cuando el acceso a la información solicitada pueda afectar a derechos o intereses de terceros- siendo el derecho a la protección de datos personales uno de ellos, pero no el único posible- los gestores de solicitudes de información deben proceder a la apertura de un trámite de audiencia de quince días a los terceros afectados por la información que se solicita. Dicho trámite deberá llevarse a cabo en los días inmediatamente posteriores a la recepción de la solicitud de información.*
> >
> > *No obstante lo anterior, debe tenerse en cuenta que ya el art. 15.2 LTAIBG prevé que, en el caso de datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano la regla general es la publicidad de dicha información, pero sin que se excluya la realización del trámite de audiencia al objeto de tener constancia de la existencia de circunstancias o situaciones que debieran tenerse en cuenta al decidir sobre el acceso.*
> >
> > *Dichos terceros deben estar debidamente identificados (art. 19.3 LTAIBG), de tal manera que el trámite de audiencia no devenga en impracticable pero, al mismo tiempo, con la práctica del mismo no se obstaculice el derecho de acceso a la información pública.*
> >
> > *El plazo para dictar la resolución queda suspendido durante la práctica del trámite de audiencia (art. 19.3, segundo inciso, LTAIBG) hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación. La suspensión del plazo para resolver debe ser notificada*

al reclamante para evitar que considere que su solicitud ha sido desestimada por silencio.

La suspensión del plazo para dictar resolución se mantiene hasta que se hayan recibido las alegaciones de los terceros interesados- en el supuesto que dichas alegaciones se reciban antes de la finalización del plazo concedido al efecto- o bien haya transcurrido el plazo concedido para la formulación de alegaciones. Es decir, transcurrido el plazo de quince días indicado en el art. 19.3 LTAIBG sin que los interesados contactados hayan formulado alegaciones, o presentadas estas antes del vencimiento de dicho plazo, se reanuda el plazo para dictar resolución.

En consecuencia, los plazos previstos en el art. 20.1 LTAIBG han de considerarse ampliados por el tiempo que ha durado la suspensión.

El trámite de audiencia se lleva a cabo para proporcionar a los órganos tramitadores la información necesaria para cumplir lo indicado por el art. 15,.esto es:

— Recibir el consentimiento expreso para aquellos supuestos en los que sea necesario (art. 15.1 LTAIBG).

— Ser informado de las circunstancias presentes en cada caso concreto en los supuestos en los que sea requerida la ponderación entre derechos indicada en el apartado 3 del artículo 15. Ello implica que, cuando sea requerida dicha ponderación y no el consentimiento expreso del interesado, una negativa de éste a la cesión a un tercero de su información personal, si bien puede ser considerada como oposición al tratamiento de datos que implica la cesión de la información, tendrá los efectos que correspondan en la ponderación que el órgano competente haya de realizar en cada caso concreto. Todo ello sin que estos supuestos lleguen a equipararse al tratamiento de los datos especialmente protegidos- categorías especiales de datos- que, como hemos indicado, requieren el consentimiento expreso del afectado.

Recibida respuesta al trámite de audiencia, el órgano encargado de resolver la solicitud de información deberá decidir sobre el acceso en función de la naturaleza de los datos personales recogidos en la información solicitada y las circunstancias planteadas por el interesado en su escrito de alegaciones.

A la hora de decidir sobre la petición de acceso, si se trata de alguno de los supuestos previstos en el art. 15, apartado 1, LTAIBG, habrá de verificarse por el órgano gestor del acceso si existe el consentimiento expreso, y en su caso por escrito, del interesado, y si no fuera así, salvo que concurran las excepciones previstas en el propio art. 15.1 (que el interesado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso, en el apartado primero del art. 15.1, o que el acceso estuviese amparado por una norma con rango de ley, en el apartado segundo del art. 15.1), habrá de denegarse el acceso.

Si no fuera aplicable dicho apartado 1 del artículo 15, si la decisión fuere favorable al acceso, en aquellos casos en los que haya habido oposición de un tercero, la información no será proporcionada al solicitante hasta que la resolución sobre el acceso deviniera firme porque haya transcurrido el plazo

para presentar recurso judicial contencioso-administrativo sin haberlo formalizado o porque, presentado el mismo, éste hubiera confirmado por sentencia firme la resolución administrativa favorable al acceso (art. 20.2, in fine, en relación con el art. 22.2).

2.5. CONCLUSIONES

Aplicando las anteriores consideraciones a las cuestiones planteadas en la solicitud realizada por la DG de Gobernanza Pública, se señala lo siguiente como conclusiones:

I. Las causas específicas que pueden ser alegadas por los afectados para oponerse a la comunicación de sus datos (si se limitan a las expresadas en párrafos anteriores o pudieran ser otras) y que desaconsejen el suministro de la información, y cómo deben ponderarse tales alegaciones a la luz de lo establecido en el art. 15.3 LTAIBG.

Tal y como se indica en los antecedentes recogidos en la solicitud de informe, el criterio interpretativo CI/001/2015 recoge las circunstancias que deberán ser tenidas en cuenta a la hora de realizar esta ponderación. Con carácter preliminar, debe no obstante recordarse que i) en la ponderación deben también tenerse en cuenta los criterios señalados por el propio art. 15.3, y ii) la ponderación debe ser realizada, en todo caso, por el órgano competente para responder la solicitud de información en tanto en cuanto dispone de todos los elementos de juicio necesarios para ello.

Sentado lo anterior, y en relación con el concreto supuesto planteado, debe señalarse que el criterio ya aprobado en 2015 señalaba expresamente que deberá atenderse a la posible situación de protección especial del titular de los datos indicando, a título meramente ejemplificativo, una situación de violencia de género o de amenaza terrorista. Sin que esas hayan de ser las únicas razones que puede alegar el interesado, puesto que la ley no limita las razones que puede aducir.

En ambos casos citados a título de ejemplo debe señalarse que el bien superior que se pretende proteger es el de la propia integridad física del afectado, pero pueden existir otros igualmente dignos de protección (como podrían ser, igualmente con carácter no exhaustivo, las señaladas en el apartado d) del art. 15.3 LTAIBGH, esto es, que los datos personales contenidos en la información a revelar afecten a su intimidad, a su seguridad, o se refieran a menores de edad). A este respecto, no es posible determinar a priori las circunstancias que, siendo planteadas por los interesados, llevaran a concluir que prevalece el derecho a la protección de datos de carácter personal frente al derecho a la información pública. Y ello es así por cuanto, además de la dificultad, cuando no imposibilidad, de fijar circunstancias apriorísticas que puedan darse en la práctica, lo contrario, desvirtuaría la llamada al caso concreto que realiza la norma en la aplicación de los límites al acceso.

No obstante, sí puede afirmarse que las circunstancias planteadas por el interesado deben ser de suficiente entidad y relevancia como para que se concluya que sus derechos o intereses legítimos puedan verse perjudicados. Esta referencia al perjuicio es establecida expresamente en la LTAIBG a la hora de determinar la aplicación de los límites.

En todo caso, en la apreciación de las circunstancias del caso concreto debe recordarse la interpretación restrictiva de los límites al derecho de acceso por la que aboga el Tribunal Supremo (sentencia de 16 de octubre de 2017 dictada en el Recurso de Casación nº 75/2017) así como a la relevancia en la transparencia por el uso de fondos públicos que también ha sido puesta de manifiesto por los Tribunales de Justicia, y la general prevalencia del interés público respecto del personal eventual conforme a la sentencia del Tribunal Supremo de 16 de diciembre de 2019 (Recurso de Casación nº 316/2018), sin que pueda entenderse que dicha concepción estricta pueda equivaler a dejar desprotegidos los bienes y derechos constitucionales dignos de salvaguarda contenidos en el art. 14.1 LTAIBG, ni tampoco los criterios de exigencia de consentimiento expreso, o ponderación, según los casos, recogidos en el art. 15 LTAIBG.

(…)

III. La forma de actuar en el caso de que en la audiencia previa el personal eventual afectado no proceda realizar ninguna alegación en el plazo concedido al efecto o no sea posible contactar con el interesado.

En este caso hay que distinguir entre los casos previstos en el artículo 15.1 y los que no se incluyen en dicho precepto. En el primero de ellos es necesario el consentimiento expreso del interesado (salvo el caso de que exista una ley o haya hecho manifiestamente públicos los datos), por lo que, si el afectado no procede a realizar ninguna alegación en el plazo concedido al efecto o no es posible contactar con él, no existe dicho consentimiento, y no será posible conceder el derecho de acceso solicitado.

En cambio, cuando la información solicitada no contuviera categorías especiales de datos relativos a la comisión de infracciones penales o administrativas que no conlleven amonestación pública al infractor , el órgano al que se dirija la solicitud deberá ponderar de manera suficientemente razonada el interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, conforme a los criterios, no exhaustivos, establecidos en el art. 15.3 LTAIBG, y ello tanto si se ha podido contactar con el interesado, y este ha dado su parecer, o no, o no se hubiera podido entablar contacto.

Como se ha indicado anteriormente, el plazo de quince días al que se refiere el art. 19.3 de la LTAIBG implica la suspensión del plazo para resolver la solicitud de información hasta que las alegaciones hubiesen sido recibidas- con anterioridad al cumplimiento de dicho plazo- o el mismo hubiera transcurrido sin que se recibieran alegaciones. La interpretación contraria implicaría en nuestra opinión la suspensión sine die y vinculada a la voluntad del tercero, que puede no desear realizar alegaciones sin comunicarlo expresamente, que no sería compatible con la debida garantía del derecho de acceso a la información pública.

En lo relativo al contacto del interesado, debe también recordarse que el art. 19.3 hace referencia expresa a que el trámite de audiencia deberá tramitarse respecto de terceros debidamente identificados, lo que implica que el contacto debe razonablemente ser posible.

IV. La necesidad de volver a pedir el consentimiento al interesado cuando se ha realizado un trámite de audiencia sobre la misma cuestión a raíz de otra solicitud de acceso presentada en un breve espacio de tiempo por un solicitante diferente.

En atención a lo indicado anteriormente, se señala que esta cuestión no se encuentra debidamente formulada, porque no se requiere el "consentimiento" del interesado, ya que no se plantearía -en el caso consultado- la solicitud de acceso sobre datos especialmente protegidos. El trámite de alegaciones no se limita a los supuestos en los que se requiere el consentimiento (que afecta a los supuestos especificados con anterioridad) sino que también engloba a aquellos en los que se debe proceder a la ponderación entre derechos y se requiere conocer las circunstancias presentes en el caso concreto.

(…)

Sentado lo anterior, parecería razonable que, aun en el supuesto en el que ya hubiera sido tramitada una audiencia con anterioridad en relación con una solicitud de información previa, en las sucesivas vuelva a realizarse el trámite al objeto de comprobar si hubiera habido algún cambio en las circunstancias señaladas por el afectado

X

En cuanto al tratamiento de imágenes que se indica en la consulta, debe señalarse que en tanto que tienen consideración de dato de carácter personal de acuerdo con el artículo 4.1 del RGPD que considera como tal *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;* la respuesta debe ofrecerse en términos similares a lo ya indicado en el presente informe.

Respecto de la publicación de imágenes en su afección al derecho al honor y a la imagen, debe estarse a lo indicado en la *Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.*

Por otra parte, referido al tratamiento de imágenes de menores de edad, debe acudirse a lo dispuesto en el artículo 8 del RGPD, que si bien analiza el consentimiento como base jurídica del tratamiento en referencia a los servicios de la sociedad de la información, contiene elementos que permiten dar validez al consentimiento prestado por un menor para el tratamiento de sus datos:

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando

tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

La LOPDGDD establece en su artículo 7 bajo la rúbrica "Consentimiento de los menores de edad" lo siguiente:

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Por lo tanto, cuando para el tratamiento de datos personales que suponga la ejecución del programa ATOPO se necesite el consentimiento de acuerdo con las leyes citadas en el presente informe, se estará a los límites de edad y especificidades previstos en el artículo 7 de la LOPDGDD.

Finalmente debe indicarse que la mera condición de menor de edad, debe ser objeto de especial ponderación tal como se exige en el artículo 15.3 d) de la LTAIBG.

XI

Cuando se hayan observado los limites recogidos en las leyes citadas en el presente informe y se proceda a la ejecución del programa ATOPO deben considerarse ciertas salvaguardas a tener en cuenta, referidas a la realización de una evaluación de impacto, a la anonimización y a los riesgos de reidentificación para garantizar el cumplimiento de los principios del RGPD.

Dispone el artículo 35 del RGPD lo siguiente:

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un

alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. (…)

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. (…)

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

En el *Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público del Grupo de Trabajo del artículo 29* se indica lo siguiente:

(…) 4.2. Importancia de una evaluación de impacto de la protección de datos antes de la apertura de los datos para su reutilización

Teniendo en cuenta los riesgos potenciales de la reutilización de la ISP, y, en particular, el hecho de que, una vez que los datos personales se han puesto a disposición del público para su reutilización, será muy difícil controlar eficazmente la utilización de estos datos, el Grupo de trabajo del artículo 29 hace hincapié en la necesidad de respetar los principios de «protección de datos desde el diseño y por defecto» y de garantizar que las cuestiones de protección de datos se abordan en una fase temprana. En particular, el Grupo recomienda encarecidamente la realización de un análisis de impacto exhaustivo sobre la protección de datos por el organismo del sector público antes de facilitar datos personales para su reutilización. Los Estados miembros han de estudiar también la posibilidad de hacer tal evaluación de impacto obligatoria en virtud de la legislación nacional, o de promoverla como buena práctica. En cualquier caso, incluso si ello no está expresamente previsto en la legislación nacional, antes de divulgar la información y de decidir si se facilita para su reutilización, los organismos del sector público deben llevar a cabo una

evaluación exhaustiva para determinar si los datos personales pueden facilitarse para su reutilización y, en caso afirmativo, en qué condiciones y con qué garantías específicas sobre protección de datos puede permitirse la reutilización.

La evaluación debería, entre otras cosas, determinar una base jurídica para la divulgación (y la potencial base jurídica para la reutilización), evaluar los principios de limitación de la finalidad, proporcionalidad y minimización de datos, y considerar la protección particular que requieren los datos sensibles. Para llevar a cabo esta evaluación, deberá analizarse detenidamente el potencial impacto sobre los interesados.

Esta evaluación debe ayudar a decidir qué datos personales, en su caso, pueden facilitarse para su reutilización, y con qué garantías.(…)

(…)6.1. ¿Cuáles son los beneficios de la agregación y la anonimización para la reutilización de la ISP?

Hasta la fecha, las iniciativas sobre reutilización de la ISP lanzadas por los organismos del sector público a través de «portales de datos abiertos» u otras plataformas han tenido generalmente como objetivo facilitar datos agregados y anonimizados para su reutilización, en vez de datos personales como tales. Este planteamiento es más seguro y debe fomentarse.

(…)En vez de datos personales, se facilitan y deberían facilitarse (en principio) datos estadísticos derivados de los datos personales. Esta es la solución más eficaz para minimizar el riesgo de revelación inadvertida de datos personales. Estas series de datos agregados y anonimizados no deberán permitir la reidentificación de las personas y, por tanto, no deben contener datos personales.

Decidir el nivel de agregación adecuado y las técnicas específicas de anonimización que deben utilizarse es una tarea difícil. Si la agregación y la anonimización no se hacen de manera eficaz, esto entraña el riesgo de que los individuos puedan ser reidentificados a partir de estos conjuntos de datos.

(…)Es también importante hacer hincapié en que una vez que los datos se publican para su reutilización, no habrá control alguno sobre quién puede acceder a ellos. La probabilidad de que «cualquier otra persona» tenga los medios y los utilice para reidentificar a los interesados aumentará considerablemente

(…)debe tenerse el mayor cuidado en garantizar que los conjuntos de datos facilitados no incluyan datos que puedan ser reidentificados por medios que puedan ser razonablemente utilizados por cualquier persona, incluidos los reutilizadores potenciales, pero también por otras partes que puedan tener interés en obtener los datos, incluidos los servicios con funciones coercitivas. (…)

Como puede observarse, la relevancia de la evaluación de impacto en la reutilización de información del sector público se tiene en cuenta en el citado *Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público*, no obstante si bien atendiendo a la complejidad que puede tener, opta por fomentar la anonimización de los datos personales (previa valoración del riesgo de reidentificación) como fórmula segura para que coexista el fomento de la reutilización y la normativa reguladora del derecho a la protección de datos.

Respecto de la identificación, y en su caso, la anonimización, el Considerando 26 del RGPD nos indica que:

> *Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.*

Asimismo debe indicarse que las disposiciones objeto de análisis en el presente informe establecen excepciones a la aplicación de la normativa de protección de datos y la exigencia de determinados requisitos como *consentimiento, transcurso de plazos, etc....* cuando los datos hayan sido anonimizados (disociados), cabe citar a título de ejemplo lo dispuesto en la Ley 37/2007 en su artículo 3.4:

> *En ningún caso, podrá ser objeto de reutilización, la información en que la ponderación a la que se refieren los artículos 5.3 y 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, arroje como resultado la prevalencia del derecho fundamental a la protección de datos de carácter personal, a menos que se produzca la disociación de los datos a la que se refiere el artículo 15.4 de la citada Ley.*

Por su parte, la LTAIBG en sus artículos 5.3 y 15.4 que nos indica:

> *5.3.Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de*

la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos

15.4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

El Real Decreto 1708/2011, en su artículo 28.4 dispone que:

Se concederá el acceso a documentos que contengan datos de carácter personal, sin necesidad de consentimiento de sus titulares, cuando se proceda previamente a la oportuna disociación, de los datos de modo que se impida la identificación de las personas afectadas.

En definitiva, es una práctica aconsejable en la ejecución del programa ATOPO el uso de técnicas de anonimización eficaces, que impidan la reidentificación de los titulares de los datos personales.

XII

Como complemento de la evaluación de impacto y de la anonimización, existe la posibilidad de establecer garantías jurídicas adicionales a través de los instrumentos que ofrece la propia Ley 37/2007 de 16 de noviembre.

Si bien la ley se inclina por favorecer fórmulas abiertas de acceso (artículo 5.2) lo cierto es que prevé un sistema de licencias dónde deben plasmarse las condiciones de la reutilización.

El articulo 8 apartado f) introduce una condición a tener en cuenta en relación con el objeto de la consulta, al indicar:

f) Cuando la información, aun siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización, la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes.

Y el artículo 9.2 se establece un contenido de mínimos que ha de tener las licencias:

2. En los casos en los que se otorgue una licencia, ésta deberá reflejar, al menos, la información relativa a la finalidad concreta para la que se concede la reutilización, indicando igualmente si la misma podrá ser comercial o no comercial, para la que se concede la reutilización, la duración de la licencia, las obligaciones del beneficiario y del organismo concedente, las responsabilidades de uso y modalidades financieras, indicándose el carácter gratuito o, en su caso, la tarifa aplicable.

Por lo tanto, existe de la posibilidad de utilizar licencias específicas que permiten establecer garantías específicas adaptadas a la tipología de datos personales objeto de reutilización en cada caso concreto, y compromisos jurídicos dirigidos a evitar la

reidentificación de los interesados, con la ventaja añadida de tener fuerza ejecutoria contractual.

A lo que hay que añadir que las cláusulas sobre protección de datos de las licencias pueden tener un efecto preventivo, contribuyendo a aumentar la sensibilización de los reutilizadores sobre sus obligaciones respecto del tratamiento de datos personales.

XIII

De lo indicado cabe concluir que ni la *Directiva 2003/98/CE del Parlamento Europeo y del Consejo* ni tampoco la *Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público* legitiman por sí mismas la difusión de datos personales ni merma las garantías que establece el RGPD y la LOPDGDD, ya que el tratamiento se rige por esta normativa.

El artículo 12 de la LTAIBG debe interpretarse en relación con los límites y garantías que se establecen en la propia ley referidos a la obtención de consentimiento y al trascurso de plazos.

En el acceso a la información, ya sea a través de la LPH o a través de la LTAIBG deben coexistir tanto formulas abiertas y universales, como peticiones individualizadas según nos encontremos ante determinados supuestos, sin que las dificultades prácticas que puedan plantearse sean oponibles a lo dispuesto en dichas leyes.

La decisión sobre la reutilización de la información del sector público está condicionada por las limitaciones incluidas en la LTAIBG, en lo que afectan al tratamiento de datos personales, tal y como exige el artículo 3.4 de la Ley 37/2007.

Estas limitaciones deben ponderarse de manera diferente según que los datos sean objeto de publicidad activa o estén relacionados con el ejercicio individual del derecho de acceso a la información pública. En la tramitación de este último, debe tenerse en cuenta el trámite de alegaciones previsto en el artículo 19.3 LTAIBG y las consecuencias de la oposición del interesado, ya sea como impedimento para la publicación, ya sea como un elemento más a tener en cuenta en la ponderación.

Para decidir si se facilitan datos personales con fines de reutilización es necesario examinar los riesgos para los interesados y las medidas que pueden minimizarlos mediante una evaluación de impacto sobre los datos personales, siendo la alternativa más apropiada para permitir la reutilización de información pública que contenga datos personales es proceder a su anonimización, de forma que estén excluidos de la aplicación de la normativa de protección de datos personales

La anonimización exige la evaluación de determinados riesgos como que el reutilizador pueda reidentificar a las personas, pudiendo complementarse con compromisos jurídicamente vinculantes a través de la concesión de licencias específicas.