RESOLUCIÓN 413/2023, de 14 de junio

Artículos: 14.1 a) y k) LTAIBG; 24, 35 RGPD;

Asunto: Reclamación interpuesta por *XXX* (en adelante, la persona reclamante), contra la Diputación Provincial de Cádiz (en adelante, la entidad reclamada) por denegación de información pública.

Reclamación: 116/2023

Normativa y abreviaturas: Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (LTPA); Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG); Reglamento General de Protección de Datos (RGPD); Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDL).

ANTECEDENTES

Primero. Presentación de la reclamación.

Mediante escrito presentado el 10 de febrero de 2023 la persona reclamante, interpone ante este CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA (en adelante Consejo) Reclamación en materia de acceso a la información pública contra la entidad reclamada, al amparo del artículo 24 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante LTAIBG) y del artículo 33 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (en adelante LTPA).

Segundo. Antecedentes a la reclamación.

1. La persona reclamante presentó el 13 de diciembre de 2022 ante la entidad reclamada, solicitud de acceso a información en los siguientes términos:

> *"1º. Copia del documento en el que conste el análisis de riesgos y la Evaluación de Impacto realizados, en garantía de los derechos y libertades de los interesados cuyos datos son tratados, ya como Responsable o como Encargado, por EPICSA, a tenor de lo dispuesto en el Manifiesta segundo.*
>
> *"2º. Copia del documento en el que conste el análisis de la comparativa entre el análisis de riesgos del RGPD y del ENS para la determinación de las medidas técnicas u organizativas que EPICSA debe adoptar en garantía de los derechos y libertades de los datos personales tratados, a tenor de lo dispuesto en el Manifiesta tercero.*
>
> *"3º. Copia de las Actas de las Reuniones celebradas por el Comité de seguridad desde su constitución en 2019."*

2. La entidad reclamada contestó la petición mediante Decreto de la Presidencia de la Diputación de Cádiz de 24 de enero de 2023, con el siguiente contenido, en lo que ahora interesa:

"(...)

"Tercero. Sobre la seguridad de la información.

"La normativa de esta materia se encuentra regulada entre otras en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

"Como expresa el apartado segundo del artículo primero de dicho Real Decreto, el ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, (en el que se encuentra todo el sector público), con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

"Asimismo el apartado tercero del mismo artículo del RD311/2022, expone que lo dispuesto en el mismo, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

"Por otro lado, el artículo 14 de la Ley 19/2013, establece las causas para poder limitar el derecho de acceso y entre ellas se encuentran tanto la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión, como la seguridad nacional.

"Por todo ello, se concluye que lo requerido por el solicitante en los apartados 1º y 2º de su escrito, al constituir documentación referida a seguridad de la información, ha de limitarse su acceso, por confidencialidad y seguridad.

(...)

"Por todo lo anteriormente expuesto, vengo en RESOLVER,

"PRIMERO: Estimar parcialmente la solicitud de acceso a la información de [se identifica a la persona solicitante] *dándole acceso a la documentación referida en el apartado tercero de su solicitud, así como a los informes mencionados, mediante el siguiente enlace:*

[se facilita enlace electrónico]

"(La documentación estará disponible en el enlace durante 15 días naturales contados a partir del día siguiente al acceso a la notificación).

"Indicarle asimismo que el documento con la Política de Seguridad de la Diputación de Cádiz y sus modificaciones, se encuentran publicadas en la siguiente dirección de la Sede Electrónica, [se facilita enlace electrónico]*."*

Consta la notificación del Decreto el 2 de febrero de 2023.

Tercero. Sobre la reclamación presentada

1. En la reclamación presentada se indica:

"(...) Solicita:

"1º Se determine por este CTPDA, en cuanto autoridad competente, si la presidencia de la DIPUTACIÓN DE CÁDIZ, ha aplicado correctamente los límites regulados en el art. 14.1 de la ley 19/2013 de TIBG.

"2º Determine si procede o no la limitación al derecho de acceso a la información pública realizada y, en caso de no proceder, obligue a dicha Presidencia a conceder el acceso solicitado.

"3º En caso, de que dicho acceso no se conceda y al margen de las posibles responsabilidades en la que pueda incurrir al amparo del art.52.1, b) y c) de la LTPA 1/2014, se dé traslado al área de Protección de Datos de este CTPDA, a los efectos de determinar una posible infracción de la normativa de Protección de datos por parte de la Empresa Pública de Información de la Diputación de Cádiz (EPICSA)."

Cuarto. Tramitación de la reclamación.

1. El 21 de febrero de 2023 el Consejo dirige a la persona reclamante comunicación de inicio del procedimiento para la resolución de la reclamación. El mismo día se solicitó a la entidad reclamada copia del expediente derivado de la solicitud de información, informe y alegaciones que tuviera por conveniente plantear en orden a resolver la reclamación. En la misma fecha, la solicitud es comunicada por correo electrónico a la Unidad de Transparencia respectiva.

2. El 9 de marzo de 2023 la entidad reclamada presenta escrito de respuesta a este Consejo, en el que se incluye cierta documentación relacionada con la petición de información. La entidad manifiesta lo siguiente, en lo que ahora interesa:

"(...) "Segundo: Sobre el informe solicitado a la entidad competente

"Que se solicita con fecha 22 de diciembre de 2022 informe al respecto de lo solicitado a la empresa EPICSA, la cual remite con fecha 17 de enero de 2023, tanto informe del Responsable de Seguridad, como del Delegado de Protección de Datos de EPICSA, (el cual lo es igualmente de la propia Diputación Provincial de Cádiz).

"A la vista del contenido de dichos informes, en los que se califica la información solicitada por el reclamante como confidencial, esta unidad de transparencia, siguiendo las directrices indicadas por las personas competentes en la materia, propone resolver la estimación parcial, aplicando la limitación prevista en el artículo 14 de la ley 19/2013, en relación con la seguridad de la información.

"Tercero: Sobre la Resolución aprobada por la Presidencia

"Que con fecha 24 de enero de 2023, se aprueba por Decreto TRANS-00004- 2023, la estimación parcial de la solicitud de acceso a información pública de [se identifica a la persona solicitante].

"Por todo ello, se CONCLUYE:

"Que la solicitud ha sido tramitada y resuelta conforme a la normativa aplicable y procede por tanto remitir al Consejo el expediente completo de acuerdo al requerimiento de éste."

FUNDAMENTOS JURÍDICOS

Primero.Sobre la competencia para la resolución de la reclamación.

1. De conformidad con lo previsto en los artículos 24 LTAIBG y 33 LTPA, en relación con lo dispuesto en el artículo 3.1.d) de la LTPA, al ser la entidad reclamada una entidad local de Andalucía el conocimiento de la presente reclamación está atribuido a la competencia de este Consejo.

2. La competencia para la resolución reside en el Director de acuerdo con lo previsto en el artículo 48.1. b) LTPA.

3. Debe destacarse a su vez que, en virtud del artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, *"[e]l personal funcionario del Consejo, cuando realice funciones de investigación en materias propias de la competencia del Consejo, tendrá el carácter de agente de la autoridad"*, con las consecuencias que de aquí se derivan para los sujetos obligados en relación con la puesta a disposición de la información que les sea requerida en el curso de tales funciones investigadoras.

Segundo. Sobre el cumplimiento del plazo en la presentación de la reclamación.

1. De conformidad con lo dispuesto en el artículo en el artículo 24.2 LTAIBG la reclamación se interpondrá en el plazo de un mes a contar desde el día siguiente al de la notificación del acto impugnado o desde el día siguiente a aquel en que se produzcan los efectos del silencio administrativo, sin perjuicio de lo dispuesto en el artículo 124 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común (LPAC).

Sobre el plazo máximo de resolución, el artículo 32 LTPA establece que las solicitudes deberán resolverse y notificarse en el menor plazo posible. En el ámbito de la entidad reclamada, el plazo máximo para dictar y notificar la resolución será de un mes desde la recepción de la solicitud por el órgano competente para resolver, salvo que la entidad hubiera establecido uno menor.

Sobre el silencio administrativo, establece el artículo 20.4 LTAIBG que transcurrido del plazo máximo de resolución sin que se haya dictado y notificado resolución expresa se entenderá que la solicitud ha sido desestimada. A su vez, los artículos 20.1 LTAIBG y artículo 32 LTPA establecen que el plazo máximo de resolución podrá ampliarse por el mismo plazo, respectivamente, en el caso de que el volumen o la complejidad de la información que se solicita así lo hagan necesario y previa notificación al solicitante.

2. En el presente supuesto la solicitud fue respondida el 2 de febrero de 2023 y la reclamación fue presentada el 10 de febrero, por lo que la reclamación ha sido presentada en plazo, conforme a lo previsto en el artículo 24.2 LTAIBG y el artículo 124 LPAC.

Tercero. Consideraciones generales sobre el derecho de acceso a la información pública

1. Constituye "información pública" a los efectos de la legislación reguladora de la transparencia, *"los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguna de las personas y entidades incluidas en el presente título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*" [art. 2 a) LTPA].

Según establece el artículo 24 LTPA, "*[t]odas las personas tienen derecho de acceder a la información pública veraz [...] sin más limitaciones que las contempladas en la Ley*". Y el artículo 6 a) LTPA obliga a que su interpretación y aplicación se efectúe tomando en consideración el "*principio de transparencia, en cuya virtud toda la información pública es en principio accesible y sólo puede ser retenida para proteger otros derechos e intereses legítimos de acuerdo con la Ley*".

La legislación reguladora de la transparencia, pues, se fundamenta y estructura en torno a una regla general de acceso a la información pública, que únicamente puede ser modulada o limitada si se aplican, motivadamente y de forma restrictiva, alguno de los supuestos legales que permiten su restricción o denegación.

2. Las causas de inadmisión se encuentran enumeradas en el artículo 18 («Causas de inadmisión») LTAIBG, y su aplicación debe ser objeto de una interpretación restrictiva y el supuesto de hecho de su concurrencia debe ser acreditado por el órgano reclamado (Resolución CTPDA 451/2018, FJ 5º).

Sobre ello nos dice el Tribunal Supremo en la Sentencia n.º 1547/2017, de 16 de octubre (Sala de lo Contencioso-Administrativo, Sección Tercera):

> *"La formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva, tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1 de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1, sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información. [...] Asimismo, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración o entidad a la que se solicita información, pues aquél es un derecho reconocido de forma amplia y que sólo puede ser limitado en los casos y en los términos previstos en la Ley...*" (Fundamento de Derecho Sexto).

3. Los límites al derecho de acceso están contenidos en el artículo 14 LTAIBG, y al igual que las causas de inadmisión, deben ser interpretados restrictivamente y el supuesto de hecho de su concurrencia debe ser acreditado por el órgano reclamado en cada caso concreto.

Cuarto. Consideraciones de este Consejo sobre el objeto de la reclamación.

1. A los efectos de resolver sobre la reclamación formulada, conviene con carácter previo hacer algunas consideraciones sobre el el objeto de la información pública solicitada (*Copia del documento en el que conste*

el análisis de riesgos y la Evaluación de Impacto realizados, en garantía de los derechos y libertades de los interesados cuyos datos son tratados, ya como Responsable o como Encargado, por EPICSA) .

Todas las actividades de tratamiento de datos personales implican un riesgo para las personas cuyos datos son tratados y, en particular, para sus derechos y libertades. Incluso, en aquellos casos en los que el responsable, ya sea por la tipología del dato o por el tipo de actividad de la organización, pudiera asumir la existencia de un riesgo escaso para los interesados o incluso la inexistencia de riesgo.

El 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 (Reglamento General de Protección de Datos, en adelante RGPD) establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento de datos personales. En particular, el artículo 24.1 establece: "*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".*

Por su parte, el artículo 25 del mismo texto legal determina que: *"(...) el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".*

Según estos preceptos, y conforme al Considerando 74 del RGPD: *"(...), 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."*

El Considerando 75 del RGPD desarrolla el concepto de riesgo para los derechos y libertades como cualquier efecto o consecuencia no deseados sobre los interesados o no previsto en el propio tratamiento de datos personales, capaz de generar daños o perjuicios sobre sus derechos y libertades, particularizando, entre otros: los daños y perjuicios físicos, materiales o inmateriales, problemas 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, perjuicios económicos o sociales, privación a los interesados de sus derechos y libertades, que se les impida ejercer el control sobre sus datos personales, etc.

El RGPD no obliga a que para cualquier tratamiento de datos personales sea necesario realizar una EIPD, pero sí establece que es obligatorio que se realice cuando hay una probabilidad de que entrañe un alto riesgo. Las obligaciones relativas a la evaluación de impacto relativa a la protección de datos (EIPD), fundamentalmente, se establecen en los artículos 35 y 36. Como establece el artículo 35: *"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."

El proceso de gestión del riesgo comprende al menos las siguientes etapas:

Descripción del tratamiento, tanto en lo que respecta a su naturaleza, como al ámbito, contexto y fines del mismo.

Identificación y análisis de los riesgos en el tratamiento.

Evaluación del nivel de riesgo y determinación de si procede o es necesario realizar una EIPD.

Tratamiento del riesgo, lo que supone tomar medidas e implementar garantías que disminuyan específicamente el nivel de riesgo para los derechos y libertades, ejecutando acciones para reducir, eliminar o asumir de forma controlada los riesgos identificados.

Seguimiento y verificación de la eficacia de las medidas adoptadas y decisión sobre cuándo es necesario realizar un proceso de revisión y reevaluación de las medidas.

Por otro lado el Esquema Nacional de Seguridad —Real Decreto 311/2022, de 3 de mayo por el que es regula el Esquema Nacional de Seguridad— (ENS en adelante), resulta de aplicación a sistemas de información de todas las entidades que conforman el sector público, entre las que se encuentran las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas —como es el caso que nos ocupa—.

En su artículo 3 establece que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDL), o, en su caso, 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, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el real decreto.

A su vez, la disposición adicional primera de la LOPDPGDL remite al ENS para la determinación de las medidas que deban implantarse en caso de tratamientos de datos personales para evitar su pérdida, alteración o acceso no autorizado, entendiéndose como un criterio de mínimos, puesto que en último

extremo las medidas determinadas en el ENS debe verse incrementadas si el resultado del análisis de riesgos en protección de datos así lo determina.

2. Entrando en el fondo del asunto, procede recordar que el objeto de la reclamación ante este Consejo es la información relativa a*l "análisis de riesgos y la Evaluación de Impacto realizados" y "el análisis de la comparativa entre el análisis de riesgos del RGPD y del ENS para la determinación de las medidas técnicas u organizativas que EPICSA debe adoptar en garantía de los derechos y libertades de los datos personales tratados". Y* que el Decreto de 24 de enero de 2023 ha denegado el acceso a esta información invocando la aplicación de los límites previstos en las letras a) y k) del artículo 14.1LTAIBG, que disponen que: "*El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: a) La seguridad nacional y k) La garantía de la confidencialidad o el secreto requerido en tomas de decisión.*

Tal y como se ha expuesto en los antecedentes de hecho, y se deduce de la reclamación, el Decreto se limita a invocar los mencionados límites:

> " (...) *el apartado tercero del mismo artículo del RD311/2022, expone que lo dispuesto en el mismo, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. (...)*
>
> *Por todo ello, se concluye que lo requerido por el solicitante en los apartados 1º y 2º de su escrito, al constituir documentación referida a seguridad de la información, ha de limitarse su acceso, por confidencialidad y seguridad*."

3. A la hora de valorar si se ha dado correcta aplicación a los límites al derecho de acceso a la información pública contemplados en la LTAIBG, conviene volver a incidir en que conforme al criterio seguido por este Consejo — Resolución CTPDA 451/2018—, y conforme a la jurisprudencia imperante —STS 1547/2017, reproducida en el FJ 3º—, las causas de inadmisión deben ser objeto de una interpretación restrictiva, y su concurrencia debe ser acreditada por el órgano reclamado.

La valoración de aplicación de los límites debe resolverse de conformidad con lo que dispone el apartado 2 del art. 14 LTAIBG: "*La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso"*. Disposición que reproduce en términos literales el artículo 25.3 LTPA.

Pues bien, según viene sosteniendo de forma constante este Consejo, de la lectura conjunta de tales preceptos (art. 14.1 y 2 LTAIBG y art. 25.3 LTPA) se desprende que la aplicación de los límites se articula como un proceso argumentativo que se despliega en tres fases o momentos sucesivos:

> *"(...) la aplicación de los límites previstos en el art. 14.1 LTAIBG ha de efectuarse en el curso de un proceso integrado por los siguientes pasos: en primer término, debe constatarse que los "contenidos o documentos" [art. 2.a) LTPA] a los que se quiere acceder inciden realmente en la materia definitoria del límite en cuestión (...); acto seguido, ha de identificarse el riesgo de un perjuicio "concreto, definido y evaluable" en el supuesto de concederse el acceso, así como argumentarse la existencia de una relación de causalidad entre el perjuicio*

y la divulgación de la información solicitada; y finalmente, una vez superado este test, aún habría de determinarse, atendiendo a las circunstancias concurrentes en el caso concreto, si los beneficios derivados de la evitación del perjuicio han de prevalecer sobre los intereses públicos o privados que pueda conllevar la difusión de la información" (así, entre otras, las Resoluciones 81/2016, FJ 6º; 120/2016, FJ 3º, 31/2017, FJ 4º; 52/2017, FJ 4º y 143/2019, FJ 5º).

Por consiguiente, el primer paso que el operador jurídico ha de emprender para valorar adecuadamente la aplicabilidad de los límites a los casos concretos reside en comprobar si cabe identificar "*el riesgo de un perjuicio «concreto, definido y evaluable» en el supuesto de concederse el acceso*", así como la existencia de "*una relación de causalidad entre el perjuicio y la divulgación de la información solicitada*" (Resoluciones 81/2016, Página 19 de 30 Resolución 812/2022, 120/2016, 31/2017 y 52/2017). Según viene puntualizando de modo constante la jurisprudencia acuñada en el marco de la Unión Europea, para que pueda legítimamente restringirse el derecho de acceso ha de invocarse el riesgo de un menoscabo al interés protegido por el límite que "*debe ser razonablemente previsible y no puramente hipotético*" [Sentencia de 15 de septiembre de 2016 (Herbert Smith Freehills/Consejo), apartado 33; Sentencia de 17 de octubre de 2013 (Consejo/Access Info Europe), apartado 31; Sentencia de 21 julio de 2011 (Suecia/ MyTravel y Comisión), apartado 76; Sentencia de 1 de julio de 2008 (Suecia y Turco/Consejo), apartado 43; asimismo, la Sentencia de 13 de abril de 2005 (Verein für Konsumenteninformation/Comisión), apartado 69]. O para decirlo en los términos que ya empleó este Consejo en la Resolución 42/2016, "*la aplicación de este límite exige que se argumente la existencia de un riesgo real, actual y concreto para tales intereses, no bastando la exposición de meras conjeturas ni la mención de remotas o hipotéticas posibilidades de que se irrogue un perjuicio con motivo de la divulgación de la información*" (FJ 9º).

Procede analizar si concurren estas circunstancias para los límites invocados en este supuesto por la entidad reclamada.

4. En relación al límite relativo a la seguridad nacional aplicado—art. 14.1 a) LTAIBG—, se justifica por parte de la entidad reclamada que:

" (...) el apartado tercero del mismo artículo del RD311/2022, expone que lo dispuesto en el mismo, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. (...)

Efectivamente, el artículo 1.3 de Real Decreto 311/2022, de 3 de mayo establece que:

"Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional."

Sin perjuicio de de lo anterior, no puede admitirse que un límite del artículo 14 LTAIBG, sea de aplicación automática, pues se estaría excluyendo un bloque completo de información. En efecto, de aceptarse la posibilidad de denegar el acceso de manera genérica en su consideración de que forma parte de los recursos y procedimientos integrantes del Sistema de Seguridad Nacional, esta sola justificación ampararía la

denegación de toda la información que obrase en poder de sus órganos. Al respecto, el artículo 18 de la Ley 36/2015 define al Sistema de Seguridad Nacional como:

> "*(...) el conjunto de órganos, organismos, recursos y procedimientos, integrados en la estructura prevista en el artículo 20 de esta ley, que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones*."

La pretendida aplicación automática del límite establecido en el artículo 14.1 a) LTAIBG ampararía la denegación de todas la información que obra en poder de cualquiera de estos órganos que forman parte del Sistema Nacional de Seguridad. Así las cosas, este Consejo entiende que el límite establecido en el artículo 14.1 a) LTAIBG no puede ser aplicado de manera indiscriminada a la totalidad de recursos y procedimientos integrantes del Sistema de Seguridad Nacional.

Ahondando esta idea, como ya se indicó por este Consejo —por todas, Resolución 727/2021—, que aun aceptando que la solicitud de información pública que ahora nos ocupa pudiera estar parcialmente incluidos por el citado límite o por otros de los establecidos en el artículo 14 LTBG, no se satisface el resto de los requisitos precisos para la aplicación del límite. No se explicita ni concreta por la entidad reclamada el eventual perjuicio a la seguridad nacional que acarrearía facilitar esta concreta información; por todo ello, a juicio de este Consejo, la entidad reclamada no ha argumentado de forma suficiente y convincente que conceder el acceso a la información entrañe un riesgo de perjuicio de tal naturaleza que permita la aplicación del límite en cuestión.

5. Por otro lado la entidad reclamada para no facilitar la información contenida en el primer punto de la solicitud de información alega la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión, considerando que lo requerido por el solicitante en los apartados 1º y 2º de su escrito, al constituir documentación referida a seguridad de la información, ha de limitarse su acceso, por confidencialidad y seguridad.

Respecto a la aplicación del límite "*la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión*", resulta evidente que la LTAIBG se inspiró en el artículo 3 1 k) del Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos, de 18 de junio de 2009, que contempla como un límite del acceso "las deliberaciones dentro o entre autoridades públicas en lo referente al examen de un asunto". Un límite que, según la Memoria Explicativa del citado Convenio, persigue "p*roteger la confidencialidad de los procedimientos dentro o entre autoridades públicas*", y cuya finalidad reside -como precisa a continuación- en "preservar la calidad del proceso de toma de decisiones al permitir un cierto libre `*espacio para pensar´*" (`*space to think´*). Y, tomando en consideración este precedente, ya tuvimos ocasión de señalar a propósito del límite del artículo 14.1 k) LTAIBG que, con su instauración, ha sido "o*bjetivo del legislador básico preservar el normal desenvolvimiento del proceso de toma de decisiones*" (Resolución 112/2017, FJ 4º).

Teniendo en cuenta estas consideraciones, este Consejo considera que la entidad reclamada se limita a invocar el límite recogido en el artículo 14.1.k) de la LTAIBG pero no ha acreditado en modo alguno que el acceso a la documentación sobre el análisis de riesgos realizado suponga un riesgo real, actual y concreto para el bien jurídico a proteger a través del citado artículo 14.1. k), ya que no ha concretado los posibles

efectos negativos en los procesos vigentes o futuros de toma de decisiones que pudieran verse afectados por el acceso.

6. Aunque este Consejo considera que la aplicación de los límites invocados del artículo 14 LTAIBG no ha sido debidamente fundamentada conforme a lo establecido en la doctrina jurisprudencial y de este Consejo al respecto, al mismo tiempo no puede desconocer que el acceso a la información solicitada supondría conocer documentación relacionada con los sistemas de información de la entidad reclamada, de sus organismos y entidades dependientes a los que la empresa municipal preste asistencia técnica informática integral.

Este Consejo desconoce el concreto contenido del análisis de los riesgos que haya podido llevarse a cabo en la entidad reclamada, pero pudiera suceder que proporcionar toda la información contenida en el análisis de riesgos y, en su caso, en la EIPD, y conocer qué factores de riesgo se han detectado, el impacto que pueden tener sobre las libertades y derechos de las personas, o las medidas y garantías establecidas para disminuir el nivel de riesgo, implicara poner al descubierto algunas debilidades de los sistemas de información de la entidad reclamada y exponerla a la aplicación de contramedidas que dejaran sin efecto o disminuyeran la protección de las garantías adoptadas, lo que indudablemente podría afectar a la seguridad pública.

En tal caso, este Consejo considera que el riesgo real de afección a la seguridad de la Entidad reclamada, y de los datos personales que la misma trata (relacionados con servicios sociales, gestión tributaria, gestión del personal ...) es superior al interés en conocer el contenido íntegro del análisis de riesgos.

Esto justificaría la aplicación parcial del límite contenido en el artículo 14.1. d) ("*La seguridad pública*"), que tal y como indicábamos en la Resolución 737/2022, citando la doctrina elaborada por el Tribunal Constitucional al respecto al interpretar el art. 104.1 CE y el título competencial del Estado ex art.149.1.29ª CE:

> *"[...] según la jurisprudencia constitucional, por seguridad pública ha de entenderse la 'actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano', la cual incluye 'un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido' (baste citar las SSTC 33/1982, FJ 3º, 154/2005, FJ 5º y, más recientemente, la STC 184/2016, FJ 3º). Actividades de protección entre las que hay que incluir, lógicamente, de forma predominante, las que corresponden a las Fuerzas y Cuerpos de seguridad a que se refiere el art. 104.1 CE (STC 104/1989, FJ 3º)".*

Esto supondría que la entidad debe facilitar la información solicitada si el acceso no supone un riesgo a la seguridad de los sistemas de información de la entidad reclamada y a los datos, personales o no, almacenados en ellos, al exponerse debilidades o deficiencias que puedan ser usadas por terceras personas para el acceso indebido, mala utilización o afectación de dichos sistemas.

Por el contrario, la entidad podrá proporcionar aquella información que cuyo acceso no supong el riesgo indicado anteriormente.

Y en la hipótesis de que no exista alguna de la información solicitada, la entidad reclamada deberá transmitir expresamente esta circunstancia a la persona reclamante

7. Por último, y en cuanto a la solicitud formulada por la persona recurrente para que: "*se dé traslado al área de Protección de Datos de este CTPDA, a los efectos de determinar una posible infracción de la normativa de Protección de datos por parte de la Empresa Pública de Información de la Diputación de Cádiz (EPICSA)",* se da traslado del escrito de reclamación al Área de Protección de Datos para su tramitación.

Quinto.Cuestiones generales sobre la formalización del acceso.

La entidad reclamada ha de ofrecer a la persona reclamante la información objeto de su solicitud, previa disociación de los datos personales que pudiera contener (art. 15.4 LTAIBG). La entidad reclamada deberá tener en cuenta que la disociación de datos personales implica no solo la supresión de la identificación concreta de las personas físicas o aquellos otros datos que pudieran permitir la misma (DNI, dirección, número de teléfono…), sino también de otra información que permitiera igualmente la identificación de alguna persona física. En este sentido, el artículo 4.1 del Reglamento General de Protección de Datos define dato personal como:

> "*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 entidad reclamada, por tanto, ha de ofrecer a la persona reclamante la información objeto de su solicitud, ocultando los datos personales que eventualmente pudieran aparecer en la misma y que excedan de la información solicitada, como pudieran ser datos sobre domicilios o teléfonos particulares, números de identificación, estado civil, etc.; todo ello en aplicación del principio de minimización establecido en el artículo 5.1c) RGPD (datos adecuados, pertinentes y limitados a lo necesario). La entidad reclamada deberá tener en cuenta que la disociación de datos personales implica no solo la supresión de la identificación concreta de las personas físicas o aquellos otros datos que pudieran permitir la misma (DNI, dirección, número de teléfono…), sino también de otra información que permitiera igualmente la identificación de alguna persona física. En este sentido, el artículo 4 del Reglamento General de Protección de Datos define dato personal como:

> *"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".*

Igualmente, el Considerando 26 afirma:

> *"(…). 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. (...)"

En el caso de que en algunos de los documentos solicitados ni siquiera la supresión u ocultación de información llegara a impedir la identificación de la persona, la entidad reclamada no pondrá a disposición de la persona reclamante aquellos documentos afectados por dicha circunstancia.

A los efectos de la adecuada disociación u ocultación de los datos que puedan aparecer en los documentos, es preciso reseñar que la firma manual también se considera un dato personal y está sujeta a lo expresado anteriormente. Por otra parte, el código seguro de verificación (CSV) de los documentos firmados electrónicamente deberá ser ocultado en caso de que se haya suprimido algún dato del documento en cuestión cuya copia se facilite como respuesta a la solicitud de acceso a la información, o bien cuando el acceso a la correspondiente verificación pueda permitir la consulta de algún dato personal, no revelado en el documento, de la persona firmante, como puede ser, por ejemplo, el DNI.

Y en la hipótesis de que no exista alguna de la información solicitada, la entidad reclamada deberá transmitir expresamente esta circunstancia a la persona reclamante.

La información obtenida podrá usarse sin necesidad de autorización previa, con las únicas limitaciones de las que se deriven de la LTPA y otras leyes, según lo previsto en el artículo 7 d) LTPA.

Asimismo, según el artículo 8 a) LTPA, las personas que accedan a información pública en aplicación de la normativa de transparencia deberán ejercer su derecho con respeto a los principios de buena fe e interdicción del abuso del derecho.

En el caso de que la información a la que se concede el acceso contuviera datos personales, el artículo 15.5 LTAIBG establece que la normativa de protección de datos será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

En virtud de los Antecedentes y Fundamentos Jurídicos citados se dicta la siguiente

RESOLUCIÓN

Primero. Estimar parcialmente la Reclamación en cuanto a la solicitud de:

"análisis de riesgos y la Evaluación de Impacto realizados" y "el análisis de la comparativa entre el análisis de riesgos del RGPD y del ENS para la determinación de las medidas técnicas u organizativas que EPICSA debe adoptar en garantía de los derechos y libertades de los datos personales tratados".

La entidad reclamada deberá facilitar a la persona reclamante la información solicitada teniendo en cuenta lo indicado en los Fundamento Jurídicos Cuarto —apartados 4, 5, 6 y 7— y Quinto, todo ello en el plazo de diez días a contar desde el día siguiente al que se le notifique esta Resolución.

Segundo. Instar a la entidad reclamada a que remita a este Consejo en el plazo de diez días a contar desde el día siguiente al que se le notifique esta Resolución, las actuaciones realizadas, incluyendo la acreditación del resultado de las notificaciones practicadas.

Contra esta resolución, que pone fin a la vía administrativa, cabe interponer recurso contencioso-administrativo ante el Juzgado de lo Contencioso-Administrativo de Sevilla que por turno corresponda en el plazo de dos meses a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 8.3 y 46.1, respectivamente, de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López

Esta resolución consta firmada electrónicamente.