Resolución 163/2019

S/REF: 001-032453

N/REF: R/0163/2019; 100-002247

Fecha: 30 de mayo de 2019

Reclamante: [redacted]

Dirección: [redacted]

Administración/Organismo: Agencia Española de Protección de Datos

Información solicitada: Notificaciones violación de seguridad de datos personales

Sentido de la resolución: Desestimatoria

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el reclamante solicitó a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, con fecha 30 de enero de 2019 y al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante LTAIBG), la siguiente información:

   - *Detalle de todas y cada una de las notificaciones de brechas de seguridad recibidas por la Agencia Española de Protección de Datos Personales, desde el 1 de mayo de 2018 hasta el 30 de enero de 2019, ambas fechas inclusive.*
   - *En concreto, para cada una de las brechas de seguridad notificadas solicito la siguiente información:*
     - *Tipo de notificación: inicial, adicional, completa.*
     - *Identificación del responsable del tratamiento: nombre de la organización, tipo de organización (privada o pública), CIF, provincia.*
     - *Información temporal de la brecha: fecha detección de la brecha, fecha inicio de la brecha, fecha de resolución de la brecha.*

- *Sobre la brecha: tipología, medio por el que se ha materializado la brecha, contexto.*
- *Sobre los datos afectados: categoría de datos afectados, categorías especiales de datos.*
- *Sobre los sujetos afectados: perfil de los sujetos afectados.*
- *Posibles consecuencias: brecha de confidencialidad, naturaleza del impacto potencial sobre los sujetos, severidad de las consecuencias para los individuos.*
- *Comunicación a los interesados.*
- *Implicaciones trasfronterizas.*
- *Clasificación, análisis y riesgo del incidente.*

- *Todas estas categorías de información forman parte del formulario de notificación para brechas de seguridad descrito por la AEPD en su guía para la gestión y notificación de brechas de seguridad (enlace: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf). Cabe deducir que esta información se vuelca en una base de datos informatizada con todos y cada uno de los campos de este formulario de todas y cada una de las notificaciones de brechas de seguridad.*
- *Solicito que me remitan la información solicitada en formato accesible (archivo .csv, .txt, .xls, .xlsx o cualquier base de datos), extrayendo las categorías de información concretas solicitadas para evitar así cualquier acción previa de reelaboración, tal y como es considerada por el Consejo de Transparencia y Buen Gobierno en el criterio interpretativo CI/007/2015.*

2. Con fecha 13 de febrero de 2019, la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS dictó resolución comunicando a [redacted] lo siguiente:

   El artículo 12 de la Ley 19/2013, de 9 de diciembre, reconoce el derecho de acceso a la información pública. No obstante, no se trata de un derecho absoluto, ya que la propia ley regula los límites al derecho de acceso en sus artículos 14 y 15 y el artículo 18 establece las causas de inadmisión.

   Entre estas causas de inadmisión, el citado artículo 18.1. e) dispone que se inadmitirán aquellas peticiones "Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley".

[redacted]

Respecto de este carácter abusivo, procede remitirse al criterio interpretativo 3/2016, del Consejo de Transparencia y Buen Gobierno. Teniendo en cuenta lo establecido en el mencionado criterio interpretativo, procede evaluar si la solicitud de información objeto de esta resolución presenta un carácter abusivo no justificado con la finalidad de transparencia de la Ley 19/2013, de 9 de diciembre. En primer lugar, la solicitud puede entenderse abusiva "cuando, de ser atendida, requiriera un tratamiento que obligara a paralizar el resto de la gestión de los sujetos obligados a suministrar la información, impidiendo la atención justa y equitativa de su trabajo y el servicio público que tienen encomendado, y así resulte de acuerdo con una ponderación razonada y basada en indicadores objetivos". En este sentido, la solicitud de información se refiere a todas y cada una de las notificaciones de brechas de seguridad recibidas por la Agencia Española de Protección de Datos desde el 1 de mayo de 2018 hasta el 30 de enero de 2019, ambas fechas inclusive. En total, en el periodo señalado, esta Agencia recibió 625 notificaciones de violaciones de seguridad de los datos personales.

Es necesario evaluar si en cada una de las 625 notificaciones recibidas operaría alguno de los límites y, en ese caso, aplicarlos de manera justificada y proporcional, atendiendo a las circunstancias concretas.

Algunos de estos límites serían los siguientes:

- *Los intereses económicos y comerciales (artículo 14.1. h) de los responsables de los tratamientos que realizan la notificación. En este sentido, por un lado, podría verse afectada de manera negativa su reputación de cara a los consumidores y usuarios. Por otro lado, la difusión de esta información podría situar a los responsables de los tratamientos en una situación de vulnerabilidad, al poder verse afectada la seguridad de sus sistemas. Es frecuente que estas notificaciones incluyan datos e informes forenses sobre los motivos por los que la violación de seguridad de los datos tuvo lugar, incorporándose información sobre productos y medidas de seguridad, y ello no necesariamente en el campo del formulario habilitado para tal finalidad ("medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados"), que no forma parte del objeto de la solicitud, sino en cualquiera de ellos. Entre estas informaciones se encontrarían, por ejemplo, mecanismos de seguridad tales como firewalls, antivirus o mecanismos de detección de intrusiones; información sobre topología de red (direccionamiento IP, direcciones MAC, sistemas de seguridad perimetral, etc.); versiones de productos y servicios utilizados (bases de datos, servicios web, etc.). No se puede establecer, a priori, una lista cerrada, sino que sería necesario analizar caso a caso las 625 notificaciones recibidas, sin que se pudiera garantizar que tras la aplicación del límite de forma ponderada no se facilitara información útil para un posible atacante.*

[redacted]

- *El secreto profesional y la propiedad intelectual e industrial (artículo 14.1. j). En este sentido, nuevamente se tendría que valorar de manera individual la concurrencia de este límite en las 625 notificaciones recibidas, analizando si en ellas se ha incluido información cuya divulgación pudiera afectar al secreto profesional o la propiedad intelectual o industrial. Por ejemplo, es frecuente que las notificaciones contengan códigos fuentes propiedad del responsable.*

- *Las funciones administrativas de vigilancia, inspección y control (artículo 14.1. g). En este sentido, el considerando 87 del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) señala que una notificación de violación de la seguridad de los datos personales "puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento". Por tanto, este límite también podría verse afectado en determinados casos, por lo que habría que valorar individualmente la concurrencia del mismo.*

- *La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios (artículo 14.1. e), en la medida en que una violación de seguridad de los datos podría poner de manifiesto la falta de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que el artículo 32 del RGPD obliga a aplicar, pudiendo, en su caso, constituir una infracción tipificada en el artículo 73. g) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que se sancionaría según lo recogido en el artículo 83.4. a) del RGPD.*

- *Sería necesario, para dar respuesta a la solicitud, evaluar cada una de las notificaciones a fin de conocer si constan en las mismas categorías especiales de datos o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, en cuyo caso habría que obrar conforme establece el apartado primero. En este sentido, ya se ha señalado que la violación de seguridad de los datos puede poner de manifiesto una falta de medidas de seguridad, lo que, en caso de que el responsable fuera una persona física, podrían llegar a constituir datos personales relativos a la comisión de una infracción administrativa por su parte que no conllevaría amonestación pública. De no existir este tipo de datos, sería necesario realizar, caso por caso, la ponderación a la que se refiere el apartado tercero. Alternativamente, se podría conceder el acceso previa*

[redacted]

disociación de los datos de carácter personal de los afectados, lo cual exigiría examinar cada una de las 625 notificaciones para proceder a la eliminación de los datos personales en ellos obrantes. Entre estos datos personales, puede constar la identidad de técnicos y demás personal de la organización del responsable, o incluso los datos personales de los propios afectados por la violación de seguridad de los datos.

De lo anterior se deriva que la admisión de la solicitud formulada requeriría un tratamiento que obligaría a paralizar el resto de la gestión propia de los sujetos obligados a suministrar dicha información, al ser necesaria la evaluación de cada una de las notificaciones recibidas a efectos de llevar a cabo la valoración de la concurrencia de los diferentes límites de los transcritos artículos 14 y 15 de la Ley 19/2013, de 9 de diciembre, a los que se acaba de aludir.

Todo ello impediría, en conclusión, la atención justa y equitativa del trabajo y servicio público que tienen encomendados los sujetos obligados a suministrar esa información, pues supondría la paralización en el desempeño de sus funciones durante el tiempo necesario para la revisión de todos y cada uno de los documentos solicitados a los solos efectos de atender la solicitud formulada, entorpeciendo completamente su actividad.

En segundo lugar, la solicitud podrá entenderse igualmente abusiva "cuando suponga un riesgo para los derechos de terceros". En este sentido, ya se ha apuntado cómo, entre la información que se incluye con frecuencia en las notificaciones de violaciones de seguridad de los datos, se encuentra aquélla relativa a información sobre productos y medidas de seguridad. La difusión de la misma supondría un posible perjuicio no sólo para los intereses económicos y comerciales de los responsables de los tratamientos, que podrían quedar en una situación de vulnerabilidad al darse a conocer información relativa a la seguridad de sus sistemas, sino también para los propios afectados por los tratamientos de datos personales llevados a cabo por los responsables que realizan las notificaciones, por este mismo motivo.

De esta manera, el cumplimiento de la obligación de notificación de violaciones de la seguridad de los datos por parte de los responsables a esta Agencia, que tiene como objetivo la mayor protección a los afectados, tal y como señala el Considerando 85 del RGPD ("Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas […] Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos

[redacted]

personales a la autoridad de control competente […]"), podría acabar produciendo, de manera paradójica, un perjuicio a los afectados por dicha violación de la seguridad, así como al resto de personas físicas cuyos datos personales sean tratados por el responsable, al poderse ver afectada, como se ha señalado, la seguridad de sus sistemas de información.

Habiéndose determinado el carácter abusivo de la solicitud, procede determinar si ésta está justificada con la finalidad de la Ley. En este sentido, observamos que la solicitud no puede ser reconducida a ninguna de las siguientes finalidades:

- *Someter a escrutinio la acción de los responsables públicos.*
- *Conocer cómo se toman las decisiones públicas.*
- *Conocer cómo se manejan los fondos públicos.*
- *Conocer bajo qué criterios actúan las instituciones públicas.*

En efecto, la respuesta a la solicitud no permitiría someter a escrutinio la acción de los responsables públicos, puesto que no se refiere a documentos emitidos por esta Agencia, sino por terceros que notifican la violación de la seguridad de los datos personales, de suerte que la acción sometida a escrutinio no sería la de los responsables públicos sino, en todo caso, la de los responsables de los tratamientos. Por el mismo motivo, tampoco permitiría conocer cómo se toman las decisiones públicas ni bajo qué criterios actúan las instituciones públicas, pues en los documentos solicitados no se contiene ninguna decisión adoptada por esta Agencia y, por tanto, tampoco se pone de manifiesto en los mismos ningún criterio de actuación de esta Agencia. Por último, la respuesta a la solicitud tampoco permitiría conocer cómo se manejan los fondos públicos, al no referirse a esta cuestión.

Es necesario, por último, aludir al hecho de que el propio RGPD regula un régimen específico de publicidad de las violaciones de seguridad de los datos. En este sentido, contempla en su artículo 33 aquellos casos en que existe la obligación de notificar dicha violación a la autoridad de control, mientras que en su artículo 34 prevé aquéllos en que se deberá comunicar a los interesados, comunicación que tendrá lugar en los casos en que sea probable que la violación de seguridad entrañe un alto riesgo para los derechos o libertades de los mismos, de forma que la notificación a la autoridad de control deberá complementarse con una notificación dirigida a los afectados con el objetivo de permitir que puedan tomar medidas para protegerse de sus consecuencias. El RGPD no prevé, por tanto, un régimen de publicidad de estas violaciones más allá de los dos casos citados.

De todo lo anterior se concluye que la solicitud formulada reviste un carácter abusivo no justificado con la finalidad de transparencia de la Ley 19/2013, de 9 de diciembre, y cuya

[redacted]

atención resultaría imposible en el plazo legalmente establecido a menos que se perjudicara gravemente el funcionamiento de esta Agencia.

Por todo ello, la Directora de la Agencia Española de Protección de Datos resuelve declarar la INADMISIÓN de la solicitud de información presentada, al amparo de lo dispuesto en el artículo 18.1. e) de la Ley 19/2013, de 9 de diciembre.

3. Ante esta contestación, el reclamante presentó, mediante escrito de entrada el 11 de marzo de 2019, al amparo de lo dispuesto en el artículo 24[1] de la LTAIBG, una reclamación ante el Consejo de Transparencia y Buen Gobierno, con el siguiente contenido:

Primero, llama la atención que la Agencia Española de Protección de Datos inadmita mi solicitud de acceso a la información en aplicación del artículo 18.1. e) de la Ley 19/2013 pero toda su argumentación jurídica consista en realizar los test de daño oportuno de los límites plasmados en los artículos 14.1. e), h), g), j) y 15 de la Ley 19/2013 (5 de los 13 contemplados en la Ley 19/2013, nada mal).

Cabe recordar que el Consejo de Transparencia y Buen Gobierno, en su resolución R-0439-2018, ha censurado reiteradamente esta práctica al asegurar que "resulta de todo punto irregular la aplicación simultánea de una causa de inadmisión de la solicitud- que, por su propia naturaleza implica que la misma no ha sido examinada en cuanto al fondo– conjuntamente con un límite al acceso –que, igualmente por su propia naturaleza implica que la solicitud es examinada en cuando al fondo– ".

El artículo 13 de la Ley 19/2013 establece que "se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones". En cambio, la AEPD hace una interpretación 'sui generis' de esta definición al entender que "la solicitud no permitiría someter a escrutinio la acción de los responsables públicos, puesto que no se refiere a documentos emitidos por esta Agencia, sino por terceros". Sin embargo, al ser la depositaria de esta información, obligada a ello por el RGPD, conocer la información recabada por la AEPD en esta función sí serviría para someter a escrutinio la AEPD.

De todos las causas de inadmisión y límites alegados por la AEPD para denegar la solicitud de información, insto al Consejo de Transparencia y Buen Gobierno a que solo analice la

[1] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

[redacted]

aplicación del artículo 18.1. e), toda vez que es a la que hace referencia la AEPD en su resolución final.

Asimismo, cabe señalar que de acuerdo a la resolución R-0394-2018 del Consejo de Transparencia, "el volumen de la información y la falta de medios no operan en la LTAIBG como causa de inadmisión de la solicitud ni como límite al derecho de acceso".

También cabe destacar lo considerado en la sentencia 184/2018 del Juzgado Central de lo Contencioso-Administrativo número 8 de Madrid, donde se afirma que "es una obviedad que, para poder obtener una información global, previamente se ha contado con la información desglosada o desagregada de cada uno de los Centros Penitenciarios, y contando con esta última información, debe de rechazarse que estemos ante un supuesto de reelaboración". En este sentido, es indudable que la AEPD está en poder de la información solicitada, como se deduce del hecho de que haya aportada la cifra global de incidencias notificadas.

Por todo ello, INSTO al Consejo de Transparencia y Buen Gobierno a que estime esta reclamación y me dé acceso a la información solicitada.

Otrosí solicito que inmediatamente antes de redactar la propuesta de resolución, el Consejo de Transparencia y Buen Gobierno me dé traslado de los documentos incorporados al expediente, incluyendo las alegaciones de la Agencia Española de Protección de Datos, y se me otorgue trámite de audiencia, de conformidad con lo dispuesto en el artículo 82.1 de la Ley 39/2015.

4. Con fecha 11 de marzo de 2019, el Consejo de Transparencia y Buen Gobierno remitió el expediente a la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS al objeto de que se pudieran hacer las alegaciones que se considerasen oportunas. El escrito de alegaciones tuvo entrada el 15 de abril de 2019 e indicaba lo siguiente:

   Cabe hacer referencia a que la argumentación de esta Agencia no ha consistido en realizar los mencionados tests de daño, algo que, por otro lado, no era procedente, tal y como el propio reclamante indica, pues la resolución ha inadmitido a trámite su solicitud. Por el contrario, la argumentación ha consistido en poner de manifiesto el carácter abusivo de la solicitud: se pedía acceso a 625 notificaciones de violaciones de seguridad de los datos en las que, de admitirse su solicitud, debería procederse a realizar los citados tests de daño, de manera individual para cada una de ellas. Así se contempla en el artículo 14.2 de la Ley 19/2013, de 9 de diciembre, "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

[redacted]

acceso". Es precisamente la necesidad de evaluar las circunstancias de cada caso concreto lo que justifica que la solicitud de acceso a 625 notificaciones de violaciones de seguridad sea abusiva, tal y como se señaló en la resolución objeto de reclamación. De los ocho fundamentos jurídicos que contiene la resolución objeto de la reclamación, a esta circunstancia se hace referencia en tan solo uno de ellos, el tercero, de lo que se desprende que no es cierta la afirmación del reclamante cuando señala que "toda la argumentación" de la resolución se ha limitado a esta cuestión.

La resolución no discutía el carácter de "información pública" de lo solicitado, lo que se discutía era que la solicitud estuviera "justificada con la finalidad de transparencia de esta Ley". Esto mismo es lo que ha señalado ese Consejo de Transparencia y Buen Gobierno en su resolución 621/2018, en su fundamento jurídico tercero. En este sentido, lo que en esta resolución afirma ese Consejo de Transparencia y Buen Gobierno, con carácter previo a la consideración transcrita, es que "lo primero que debe valorarse a nuestro juicio es si lo solicitado por el interesado constituye información pública o no". Por tanto, ese Consejo de Transparencia y Buen Gobierno sí parece realizar esta interpretación que el reclamante califica de "sui generis" y que negaría el carácter de "información pública" al objeto de su solicitud.

También afirma el reclamante que, según ese Consejo de Transparencia y Buen Gobierno, "el volumen de la información y la falta de medios no operan en la LTAIBG como causa de inadmisión de la solicitud ni como límite al derecho de acceso". En ningún caso esta Agencia ha esgrimido ese argumento y lo que ha puesto de manifiesto la resolución objeto de reclamación es que la solicitud tiene un carácter abusivo no justificado con la finalidad de transparencia de la Ley 19/2013, de 9 de diciembre, lo que constituye una causa de inadmisión, según su artículo 18.1. e).

Por lo tanto, y a la vista de las alegaciones esgrimidas por esta Agencia Española de Protección de Datos, se insta a ese Consejo de Transparencia y Buen Gobierno a que proceda a desestimar la reclamación interpuesta.

5. El 16 de abril de 2019, en aplicación del art. 82 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se concedió Audiencia del expediente a [redacted] para que, a la vista del mismo, presentase las alegaciones que estimara pertinentes en defensa de su pretensión. Dichas alegaciones tuvieron entrada el 23 de abril de 2018 y tenían el siguiente contenido:

   Debido a que la Agencia Española de Protección de Datos reincide en los argumentos en su resolución objeto de mi reclamación, reitero los argumentos esgrimidos en mi reclamación e insto al Consejo de Transparencia y Buen Gobierno a que la estima completamente.

[redacted]

II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 24 de la LTAIBG[2], en relación con el artículo 8 del Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno[3], la Presidencia de este Organismo es competente para resolver las reclamaciones que, con carácter previo a un eventual y potestativo Recurso Contencioso-Administrativo, se presenten en el marco de un procedimiento de acceso a la información.

2. La LTAIBG, en su artículo 12[4], regula el derecho de todas las personas a acceder a la información pública, entendida, según el artículo 13 de la misma norma, como "*los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones".*

   Por lo tanto, la Ley define el objeto de una solicitud de acceso a la información en relación a información que ya existe, por cuanto está en posesión del Organismo que recibe la solicitud, bien porque él mismo la ha elaborado o bien porque la ha obtenido en ejercicio de las funciones y competencias que tiene encomendadas.

3. En cuanto al fondo de la cuestión planteada, ha de señalarse en primer lugar que el mismo supuesto ya ha sido analizado previamente por este Consejo de Transparencia en el procedimiento R/0103/2019, en el que se razonaba lo siguiente:

   "En efecto, a LTAIBG, dispone en el mencionado precepto lo siguiente:

   1. Se inadmitirán a trámite, mediante resolución motivada, las solicitudes:

   e) Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley.
   Como se desprende de las alegaciones de la AEPD, la aplicación de la mencionada causa de inadmisión se encuentra vinculada con el carácter abusivo que, a juicio de dicho Organismo,

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[3] https://www.boe.es/buscar/act.php?id=BOE-A-2014-11410&tn=1&p=20141105#a8
[4] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

[redacted]

tiene la solicitud. En este sentido, debemos indicar que según el criterio interpretativo nº 3 de 2016, aprobado por este Consejo de Transparencia y Buen Gobierno en ejercicio de las competencias legalmente atribuidas en el art. 38.2 a) de la LTAIBG

El artículo 18.1.e) de la LTAIBG asocia el carácter abusivo de la solicitud a la condición de que la petición "no esté justificada con la finalidad de la Ley".

De este modo hay dos elementos esenciales para la aplicación de esta causa de inadmisión:

A) Que el ejercicio del derecho sea abusivo cualitativamente, no en sentido cuantitativo: el hecho de que una misma persona presente un número determinado de solicitudes no determina necesariamente un ejercicio abusivo del derecho, y

B) Que el ejercicio del derecho pueda considerarse excesivo, es decir, cuando no llegue a conjugarse con la finalidad de la Ley.

1. Así, una solicitud puede entenderse ABUSIVA cuando se encuentre en alguno de los supuestos o se den alguno de los elementos que se mencionan a continuación:

- *Con carácter general, en aquellos casos en que pueda considerase incluida en el concepto de abuso de derecho recogido en el artículo 7.2 del Código Civil y avalado por la jurisprudencia, esto es: "Todo acto u omisión que por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho".*
- *Cuando, de ser atendida, requiriera un tratamiento que obligara a paralizar el resto de la gestión de los sujetos obligados a suministrar la información, impidiendo la atención justa y equitativa de su trabajo y el servicio público que tienen encomendado, y así resulte de acuerdo con una ponderación razonada y basada en indicadores objetivos*
- *Cuando suponga un riesgo para los derechos de terceros.*
- *Cuando sea contraria a las normas, las costumbres o la buena fe.*

2. Se considerará que la solicitud está JUSTIFICADA CON LA FINALIDAD DE LA LEY cuando se fundamenta en el interés legítimo de:

- *Someter a escrutinio la acción de los responsables públicos*

[redacted]

- *Conocer cómo se toman las decisiones públicas*
- *Conocer cómo se manejan los fondos públicos*
- *Conocer bajo qué criterios actúan las instituciones públicas*

Consecuentemente, NO ESTARÁ JUSTIFICADA CON LA FINALIDAD DE LA LEY cuando:

- *No pueda ser reconducida a ninguna de las finalidades señaladas con anterioridad y así resulte de acuerdo con una ponderación razonada y basada en indicadores objetivos.*
- *Cuando tenga por finalidad patente y manifiesta obtener información que carezca de la consideración de información pública de acuerdo con la definición del artículo 13 de la LTAIBG.*
- *Cuando tenga como objeto o posible consecuencia la comisión de un ilícito civil o penal o una falta administrativa.*

1. *En cuanto al objeto de la solicitud de información, la misma viene referida a datos sobre las notificaciones de violación de la seguridad de los datos personales a la Autoridad de Control reguladas en el art. 33 del RGPD. Dicho precepto se pronuncia en los siguientes términos:*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

[redacted]

b) *comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*

c) *describir las posibles consecuencias de la violación de la seguridad de los datos personales;*

d) *describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Podemos concluir, por lo tanto, que en dicho precepto se contempla la puesta en conocimiento de la Autoridad de Control- en el caso que nos ocupa, es la AEPD la que tiene tal condición-, de los supuestos en los que se haya producido una violación de la seguridad de los datos de carácter personal. Dicha notificación se enmarca, por lo tanto, en las facultades de control para la protección de los datos de carácter personal y a los efectos de investigar las circunstancias en las que se ha producido esa quiebra en la seguridad debida respecto del tratamiento de los datos personales así como, en su caso, en la depuración de responsabilidades por incumplimiento de la normativa de protección de datos que pudiera derivarse de los hechos acontecidos.

Asimismo, cabe destacar que, según manifiesta la AEPD, en criterio que ya adelantamos es compartido por este Consejo de Transparencia y Buen Gobierno, que la información cuyo acceso se solicita está a disposición de la AEPD- encuadrándose, por lo tanto, en el concepto de información pública al que se refiere el art. 13 de la LTAIBG- pero no guarda relación con el conocimiento de la actuación pública y la rendición de cuentas por las decisiones adoptadas por los Organismos Públicos que constituye la ratio iuris de la LTAIBG tal y como se predica en su Preámbulo: La transparencia, el acceso a la información pública y las

[redacted]

normas de buen gobierno deben ser los ejes fundamentales de toda acción política. Sólo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos.

2. *En este sentido, ha de analizarse si, tal y como defiende la AEPD, el acceso a la información solicitada puede considerase encuadrable dentro del supuesto de solicitud abusiva al que se refiere el art. 18.1 e). Una condición, la de abusiva, que la AEPD contextualiza señalando el número de comunicaciones recibidas en el período temporal indicado en la solicitud de información- 499-, la necesidad de analizar, en cada una de estas notificaciones, la posible aplicación de alguno de los límites al acceso previstos en el art. 14 de la LTAIBG y, finalmente, la ausencia de conexión entre la información cuyo acceso se solicita y el conocimiento y control de las decisiones públicas que afectan a los ciudadanos.*

   Es criterio de este Consejo de Transparencia y Buen Gobierno que la condición abusiva de una solicitud de información no puede conectarse directamente con el número de solicitudes que un mismo interesado haya realizado o, como ocurre en este caso, con el volumen de información que se vería afectada por el acceso.

   No obstante, nuestra posición ha sido favorable a tener en cuenta el volumen de información solicitada, conectando este criterio con la relevancia de su conocimiento para alcanzar las finalidades perseguidas por la LTAIBG, a la hora de entender de aplicación la causa de inadmisión prevista en el art. 18.1 e).

   Así, en el expediente R/0053/2018[5], se razonaba lo siguiente:

   A pesar de que la interpretación del art. 18.1 e) de la LTAIBG antes reproducido no conecta el ejercicio abusivo del derecho a un criterio cuantitativo (número de solicitudes presentadas) sino cualitativo (características de la solicitudes presentadas y antecedentes de la misma), no es menos cierto que ambos aspectos deben cohonestarse en casos como el presente en que el volumen de solicitudes es un reflejo del ejercicio abusivo del derecho desde una perspectiva cualitativa.

5 https://www.consejodetransparencia.es/ct_Home/Actividad/Resoluciones/resoluciones_AGE/AGE_2018.html

[redacted]

En este punto, resultan especialmente clarificadoras las apreciaciones de la Administración y, sobre todo, el detalle y la especificidad con la que se dimensionan- en términos de recursos necesarios- las implicaciones de atender solicitudes de información como las planteadas. Es decir, a nuestro juicio, no se hace una apreciación general o en abstracto de una situación, sino que se aportan detalles, concretos y determinados, del alcance que para la organización implica atender las peticiones del solicitante.

Así, a nuestro juicio, todas estas manifestaciones de la Administración han de ser acogidas favorablemente, debiendo entenderse que se dan las circunstancias citadas por los Tribunales de Justicia y por el Criterio Interpretativo de este Consejo de Transparencia para considerar que las solicitudes del Reclamante participan de la condición de abusivas y son contrarias al ordenamiento jurídico, puesto que pueden considerase incluidas en el concepto de abuso de derecho, han sido presentadas antes de que finalice el plazo normal de contestación a la anterior y requieren un tratamiento que obliga a paralizar el resto de la gestión de los sujetos obligados a suministrar la información, impidiendo la atención justa y equitativa de su trabajo y el servicio público que tienen encomendado, puesto que el Ministerio carece de medios personales suficientes para atenderlas todas a la vez o en los plazos resultantes.

Añadido a lo anterior, las solicitudes planteadas deben analizarse desde la perspectiva del control de la acción de la Administración y la rendición de cuentas por las decisiones públicas, toda vez que, en no pocas ocasiones como ha quedado destacado en los antecedentes de hecho y atendiendo al tipo de información requerida, ciertamente podría cuestionarse su utilidad para garantizar el interés común en conocer la actuación pública, poder participar en la misma y exigir responsabilidades por las decisiones de los organismos públicos; todos ellos, pilares fundamentales y ratio iuris de la LTAIBG. Así, debe recordarse que es la protección del interés general en la transparencia pública, como bien común de nuestra sociedad, la que debe prevalecer frente a solicitudes de información que persiguen otros intereses, de carácter privado o profesional, que no encajan en la finalidad perseguida por la LTAIBG y, por tanto, no pueden ser considerados superiores.

En definitiva, a nuestro juicio y en atención a las circunstancias planteadas en el expediente, el acceso a la información solicitada implicaría la exigencia de un tratamiento desmesurado por parte de la AEPD al objeto de garantizar que dicho acceso no implique la vulneración de alguno de los derechos e intereses legítimos que se ven reflejados en el art. 14 de la LTAIBG bajo la forma de restricciones al acceso. Un tratamiento que entendemos no se ve justificado por la finalidad de transparencia de la actuación pública en la que se basa la LTAIBG y que

[redacted]

implica que, en consecuencia, entendamos que la presente reclamación deba ser desestimada."

Dada la coincidencia con el objeto de la solicitud, todos los argumentos expuestos en este precedente son igualmente aplicables al presente supuesto, por lo que la reclamación presentada ha de ser desestimada.

III. RESOLUCIÓN

En atención a los Antecedentes y Fundamentos Jurídicos descritos, procede **DESESTIMAR** la Reclamación presentada por [redacted], con entrada el 11 de marzo de 2019, contra la resolución, de fecha 13 de febrero de 2019, de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

De acuerdo con el artículo 23, número 1, de la Ley 19/2013, de 9 de diciembre[6], de Transparencia, Acceso a la Información Pública y Buen Gobierno, la Reclamación prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de conformidad con lo dispuesto en el artículo 112.2 de la Ley 39/2015, de 1 de octubre[7], de Procedimiento Administrativo Común de las Administraciones Públicas.

Contra la presente Resolución, que pone fin a la vía administrativa, se podrá interponer Recurso Contencioso-Administrativo, en el plazo de dos meses, ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid, de conformidad con lo previsto en el artículo 9.1 c) de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa[8].

EL PRESIDENTE DEL CTBG
P.V. (Art. 10 del R.D. 919/2014)
EL SUBDIRECTOR GENERAL DE
TRANSPARENCIA Y BUEN GOBIERNO

Fdo: Francisco Javier Amorós Dorda

[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a23
[7] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&tn=1&p=20181206#a112
[8] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&tn=1&p=20181206#a9

[redacted]