Ref. entrada: 00001-00101343

A.A.A.
x.x.x.

Resolución sobre solicitud de acceso a la información pública

I. Objeto de la Solicitud

A.A.A. (en adelante, la solicitante) presentó una solicitud de acceso a la información pública ante la Agencia Española de Protección de Datos (en adelante, AEPD) el 14 de febrero de 2025, cuyo objeto es:

"*Detecté un delito de fraude en tarjeta de uso no autorizado con denuncia policial reclamado a la entidad BBVA y a su financiera.*
(…)
Entre enero de 2023 y diciembre de 2024 solicito esta información: si hay antecedentes de bugs, fallos de seguridad, violaciones de seguridad, hacking, mala praxis empresarial, fuga de datos o comportamientos ilegítimos relacionados con el Banco BBVA o su filial Tarjeta Renfe MasterCard Clásica.
Necesito esta información para comprender el alcance del incidente, evaluar si mis datos personales han estado expuestos y tomar las medidas necesarias para protegerme y ejercer mis derechos como consumidor y persona."

II. Normativa aplicable

1. El artículo 12 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, (en adelante, LTAIBG) reconoce el derecho de acceso a la información pública, de manera que "*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 la mencionada Ley*".

2. El artículo 13 de la LTAIBG define la información pública 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".

3. El artículo 14.1 de la LTAIBG establece que el derecho de acceso podrá ser limitado "*cuando acceder a la información suponga un perjuicio para (…) la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios*" (14.1.e), "*las funciones administrativas de vigilancia, inspección y control*" (14.1.g) o "*los intereses económicos y comerciales*" (14.1.h).

4. El artículo 20.1 de la LTAIBG determina que *"La resolución en la que se conceda o deniegue el acceso deberá notificarse al solicitante y a los terceros afectados que así lo hayan solicitado en el plazo máximo de un mes desde la recepción de la solicitud por el órgano competente para resolver."*

III. Fundamentos jurídicos

1. La solicitante pide acceso a los antecedentes relativos a "*bugs, fallos de seguridad, violaciones de seguridad, hacking, mala praxis empresarial, fuga de datos o comportamientos ilegítimos relacionados con el Banco BBVA o su filial Tarjeta Renfe MasterCard Clásica*" obrantes en la AEPD.

2. En primer lugar, cabe señalar que no todas las brechas de seguridad implican, necesariamente, una brecha de datos personales. El artículo 33 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 (RGPD) solo obliga a notificar a la Autoridad de Control las brechas que puedan suponer un riesgo a los derechos y libertades de las personas.

   Por tanto, en esta Agencia tan solo obra la información relativa a aquellas brechas de datos personales que hubieran sido notificadas a la AEPD y no la relativa a todas aquellas brechas de seguridad u otro tipo de incidentes de seguridad que hubieran tenido lugar.

3. En cuanto a la solicitud de información respecto a la existencia de brechas de datos personales, entendiendo por tales las reguladas en el artículo 33 del RGPD, y, en particular, si las mismas hubieran dado lugar a alguna actuación conducente a la adopción de una decisión por parte de esta autoridad de control, a la revelación de su existencia y contenido a terceros le serían de aplicación los límites establecidos en los apartados e), g) y h) del artículo 14 de la LTAIBG.

4. La prevención, investigación y sanción de los ilícitos administrativos (art. 14.1.e) competencia de la AEPD, podría verse afectada, en la medida en que una violación de seguridad de los datos podría poner de manifiesto la falta de adopción, por parte del responsable o del encargado, de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos del tratamiento de datos personales que el artículo 32 del RGPD les 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.

5. Las funciones administrativas de vigilancia, inspección y control (art. 14.1.g) asignadas a la AEPD podrían verse afectadas dado que, de conformidad con el considerando 87 del RGPD, 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*". La difusión de la información sobre productos y medidas de seguridad que conforman la base sobre la que se han de llevar a cabo las actuaciones conducentes a la adopción de una decisión por parte de la autoridad de control, afectaría a las funciones administrativas de control encomendadas a esta Agencia.

   Así lo manifestó el Consejo de Transparencia en su Resolución 195/2022 en la que se señala expresamente "*es objetivamente indiscutible que revelar la información solicitada en la fase procedimental en la que se encuentran las actuaciones de investigación en el momento de formularse la solicitud comportaría un perjuicio real, no meramente hipotético, para el desarrollo de las mismas en la medida en que dificultaría el normal desenvolvimiento de las funciones de inspección, instrucción y valoración de las eventuales evidencias obtenidas con el fin de determinar si se ha producido o no una infracción de la normativa reguladora de la protección de datos de carácter personal*".

6. Asimismo, el acceso a esta información podría ocasionar perjuicios a los intereses económicos y comerciales del autor de la notificación (art.14.1.h), en tanto que hacer pública la información sobre las brechas de datos personales podría afectar negativamente a su imagen en el mercado.

7. Por otro lado, el RGPD regula un régimen específico para las brechas de seguridad de los datos de carácter personal y, además de establecer la obligación de notificar a la autoridad de control (Art. 33 del RGPD), prevé los casos en que se deberá comunicar a los propios afectados (Art. 34 del RGPD), cuando sea probable que la brecha de seguridad entrañe un alto riesgo para los derechos o libertades de los mismos, de forma que en dichos casos los afectados conozcan las violaciones de seguridad de los

datos personales producidas lo que, en su caso, les permitirá ejercer las acciones que estimen oportunas.

8. Asimismo, hay que poner de manifiesto que el derecho de acceso a la información pública no es un derecho absoluto, la propia LTAIBG regula los límites al derecho de acceso por lo que de conformidad con lo establecido en los apartados e), g) y h) de su artículo 14.1 y en su artículo 15, procede denegar el acceso a la información solicitada.

9. Una vez constatada la concurrencia de los citados límites, la AEPD debe examinar, de conformidad con el artículo 14.2 de la LTAIBG, si la aplicación de estos límites entra en colisión con un interés público o privado superior que justifique el acceso. La solicitante justifica su petición en la necesidad de "*comprender el alcance del incidente, evaluar si mis datos personales han estado expuestos y tomar las medidas necesarias para protegerme y ejercer mis derechos como consumidor y persona*."

   A este respecto, el artículo 34 del RGPD establece que "*Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas*" es el responsable del tratamiento quien lo comunicará al interesado sin dilación indebida.

   La AEPD estima que la información sobre la existencia de una notificación de brecha de datos personales iría contra el espíritu de este artículo y, además, no permitiría a la solicitante alcanzar los objetivos que pretende.

10. Conviene, además, mencionar el criterio mantenido por la AEPD sobre el acceso a esta información, que ha sido avalado por el Consejo de Transparencia y Buen Gobierno en su Resolución 103/2019, de 9 de mayo de 2019. Según este criterio, la notificación a la autoridad de control, en este caso la AEPD, de que se ha producido una violación de la seguridad de los datos de carácter personal se enmarca, *"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."*

Con base en lo anterior, se resuelve lo siguiente,

IV. Resolución

Se deniega el acceso a la información solicitada en virtud de lo dispuesto en el artículo 14.1., apartados e), g) y h) de la LTAIBG.

Contra la presente resolución, que pone fin a la vía administrativa, podrá interponerse potestativamente reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de un mes, o presentar directamente recurso Contencioso-Administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, conforme al artículo 25 y apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses.

NOTA INFORMATIVA SOBRE TRATAMIENTO DE DATOS PERSONALES

Los datos de carácter personal serán tratados por la Agencia Española de Protección de Datos e incorporados a la actividad de tratamiento "Transparencia: acceso a la información", cuya finalidad es tramitar las peticiones de acceso a la información realizadas por los ciudadanos al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. Finalidad basada en el cumplimiento de una obligación legal por la Agencia Española de Protección de Datos. Los datos de carácter personal pueden ser comunicados al Consejo de Transparencia y Buen Gobierno, órganos jurisdiccionales y a la Abogacía General del Estado. Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se han recabado y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación la normativa de archivos y patrimonio documental español.

Para solicitar el acceso, la rectificación, supresión o limitación del tratamiento de los datos personales o a oponerse al tratamiento, en el caso de se den los requisitos establecidos en el Reglamento General de Protección de Datos, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personal y garantía de los derechos digitales, puede dirigir un escrito al responsable del tratamiento, en este caso, la AEPD, dirigiendo el mismo a la Agencia Española de Protección de Datos, C/Jorge Juan, 6, 28001- Madrid o en el registro electrónico de la AEPD

https://sedeagpd.gob.es/sede-electronica-web/vistas/formProcedimientoEntrada/procedimientoEntrada.jsf?coe=c

Datos de contacto del DPD: dpd@aepd.es