- **N/Ref.: E/07364/2018 - E/02627/2019**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones seguidas con motivo de la reclamación presentada en la Agencia Española de Protección de Datos, por presunta vulneración 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 (en lo sucesivo, RGPD) y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 11 de septiembre de 2018 y con número de registro de entrada 193823/2018, tuvo entrada en esta Agencia una reclamación, relacionada con un tratamiento de carácter transfronterizo de datos personales realizado por ***SPOTIFY AB***, (en adelante, la parte reclamada) por una presunta vulneración del RGPD.

Los motivos en que la parte reclamante basa la reclamación son la posible revelación de datos de su cuenta de Spotify. Según indica en su reclamación, recibió un WhatsApp de un tercero en el que se le comunicaba que en la página https://nulledbb.com/thread-Spotify--100953 estaban sus datos, junto a los de muchos otros usuarios, y entre los que se encontraban sus datos de usuario, contraseñas, tipo de cuenta, etc.

Junto a la reclamación se aportan una serie de capturas de pantalla en las que pueden observarse los mensajes recibidos por el tercero en los que se informa a la parte reclamante de la disponibilidad de los datos en internet, una captura de la búsqueda de la página en la que se publican los datos y una captura en la que se observan los datos relativos a la cuenta de Spotify supuestamente filtrados.

SEGUNDO: ***SPOTIFY AB*** tiene su establecimiento principal o único en Suecia.

TERCERO: Teniendo en cuenta el carácter transfronterizo de la reclamación, con fecha 11 de marzo de 2019 se acordó el archivo provisional del procedimiento y la remisión de la reclamación a la autoridad de control de Suecia por ser la competente para actuar como autoridad de control principal, a tenor de lo dispuesto en el artículo 56.1 del RGPD.

CUARTO: Esta remisión se realizó, a través del “Sistema de Información del Mercado Interior” (IMI).

La autoridad de control de Suecia aceptó actuar en el procedimiento en calidad de autoridad de control principal y se declararon interesadas en el mismo las autoridades de control de: España, Dinamarca, Bélgica, Francia, Países Bajos, Irlanda, Hungría, Alemania (Berlín, Hesse, Mecklenburg-Pomerania Oeste, Saarland, Renania-Palatinado, Renania Norte-Westfalia y Baja Sajonia), Noruega, Italia, Grecia y Austria.

QUINTO: Siguiendo el procedimiento establecido en el artículo 60 del RGPD y después de que la Autoridad de control principal hubiera acordado desestimar o rechazar la reclamación, comunicó a las autoridades interesadas el proyecto de decisión, que ha sido aceptado.

FUNDAMENTOS DE DERECHO

I: Competencia

De acuerdo con lo dispuesto en el artículo 60.8 del RGPD, la Presidencia de la Agencia Española de Protección de Datos es competente para adoptar esta resolución, según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

II: Sistema de Información del Mercado Interior (IMI)

El Sistema de Información del Mercado Interior se encuentra regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), y su objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información.

III: Determinación del alcance territorial

Según especifica el artículo 66 de la LOPDGDD:

"1. Salvo en los supuestos a los que se refiere el artículo 64.3 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679."

IV: Establecimiento principal, tratamiento transfronterizo y autoridad de control principal

El artículo 4.16 del RGPD define «establecimiento principal»:

“a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento”

Por su parte el artículo 4.23 del RGPD considera «tratamiento transfronterizo»:

“a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro,

o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro”

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

En el caso examinado, como se ha expuesto, ***SPOTIFY AB*** tiene su establecimiento principal o único en Suecia, por lo que la autoridad de control de Suecia es la competente para actuar como autoridad de control principal.

V: Autoridad de control interesada

De conformidad con lo dispuesto en el artículo 4.22) del RGPD, es Autoridad de control interesada, la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a.- El responsable o encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b.- Los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c.- Se ha presentado una reclamación ante esa autoridad de control.

En el presente procedimiento actúan en calidad de "autoridad de control interesada" las autoridades de control de: España, Dinamarca, Bélgica, Francia, Países Bajos, Irlanda, Hungría, Alemania, Noruega, Italia, Grecia y Austria.

VI: Procedimiento de cooperación y coherencia

El artículo 60 del RGPD, que regula el procedimiento de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas, dispone en su apartado 8, lo siguiente:

"8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento."

VII: Cuestión reclamada y razonamientos jurídicos.

En este caso, se ha presentado en la Agencia Española de Protección de Datos reclamación por una presunta vulneración del RGPD, relacionada con un tratamiento de carácter transfronterizo de datos personales, realizado por ***SPOTIFY AB***.

La Autoridad Sueca de Protección de la Privacidad (IMY) considera que la investigación no ha demostrado que ***SPOTIFY AB*** haya incumplido el Reglamento General de Protección de Datos (RGPD), como se alega en la reclamación.

IMY ha iniciado un procedimiento de supervisión de ***SPOTIFY AB*** debido a una reclamación contra la empresa. La reclamación fue transferida de la autoridad de control del Estado miembro en el que la parte reclamante presentó su reclamación (España) de conformidad con las disposiciones del RGPD sobre cooperación en el tratamiento transfronterizo. IMY ha tramitado el caso como autoridad de control responsable de las operaciones de la empresa en virtud de Artículo 56 del RGPD.

El asunto se ha tramitado mediante procedimiento escrito. Dado que la reclamación se refiere a un tratamiento transfronterizo, IMY ha utilizado los mecanismos de cooperación y coherencia regulados en el capítulo VII del RGPD. Las autoridades de control interesadas han sido las autoridades de protección de datos de España, Dinamarca, Bélgica, Francia, Países Bajos, Irlanda, Hungría, Alemania, Noruega, Italia, Grecia y Austria.

A continuación, se describen los argumentos presentados por la parte reclamante y la empresa en relación con la reclamación.

En la reclamación se ponían de manifiesto los siguientes hechos:

Se produjo una filtración de los datos personales de la parte reclamante vinculados a su cuenta de usuario Spotify y se accedió a ellos a través de un enlace en Google. La información filtrada incluye la dirección de correo electrónico del solicitante, la contraseña de su cuenta de Spotify y la información sobre la suscripción del solicitante a Spotify. La reclamación fue recibida por la autoridad española de protección de datos en septiembre de 2018.

SPOTIFY AB (Spotify) ha declarado lo siguiente:

Tan pronto como recibimos el requerimiento de IMY sobre este asunto, iniciamos una investigación interna exhaustiva con nuestro equipo de seguridad para comprender si se habían comunicado datos personales a personas no autorizadas en 2018. Sin embargo, Spotify no dispone de ninguna prueba de vulnerabilidad o incidente de seguridad de Spotify desde el período pertinente que pueda explicar por qué los datos personales de la parte reclamante estaban disponibles en otro sitio web.

Según Spotify, la parte reclamante puede haber sido víctima de un ataque conocido como «reutilización de credenciales» («Credential Stuffing»). Tras las propias búsquedas de Spotify de los datos de la parte reclamante a través de un sitio web que puede utilizarse para investigar si las cuentas de usuario han estado expuestas a riesgos, Spotify considera que esto es muy posible porque la dirección de correo electrónico figura como implicada en cuatro violaciones de datos de terceros diferentes durante el período 2017-2018:

- Onliner Spambot (Agosto 2017)
- MyFitnessPal (Febrero 2018)
- Shein (Junio 2018)
- Kayo.moe (Septiembre 2018)

La «reutilización de credenciales» es un tipo de ataque en el que la dirección de correo electrónico y la contraseña de un individuo están implicadas en una brecha de seguridad de los datos. Cuando las personas reutilizan la misma dirección de correo electrónico y la misma combinación de contraseña a través de múltiples servicios en línea, existe el riesgo de que, si se filtran estos datos en un servicio, los agentes maliciosos puedan utilizar estas credenciales para conectarse a otros servicios en los que también son válidos. Si la parte reclamante en este caso utiliza la misma dirección de correo electrónico y contraseña que se filtró en las brechas, un agente malicioso podría intentar utilizar dichas credenciales para acceder a la cuenta Spotify de la parte reclamante.

Spotify no tiene pruebas de que el acceso no autorizado a los datos personales de la parte reclamante fuera el resultado de un incidente de seguridad de Spotify. IMY ha enviado una declaración de ***SPOTIFY AB*** a la autoridad de control del país en el que la parte reclamante presentó su reclamación (España) para darle la oportunidad de formular observaciones sobre la declaración de Spotify. No consta respuesta de la parte reclamante a esta declaración.

Motivación de la decisión

IMY ha iniciado un procedimiento de supervisión para investigar si Spotify ha adoptado las medidas adecuadas para garantizar un nivel de seguridad de conformidad con el artículo 32 del RGPD para proteger los datos personales de la parte reclamante.

Del artículo 57, apartado 1, letra f), del RGPD se desprende que IMY debe tramitar las reclamaciones de los interesados que consideren que sus datos personales se están tratando infringiendo el RGPD. De esta disposición también se desprende que IMY examinará, en su caso, el objeto de la reclamación. El Tribunal de Justicia de la Unión Europea ha declarado que las autoridades de control deben investigar dichas reclamaciones con la debida diligencia.

El artículo 32 del RGPD obliga a los responsables y encargados del tratamiento a aplicar medidas técnicas y organizativas adecuadas para alcanzar un nivel de seguridad adecuado al riesgo que plantea el tratamiento. Al evaluar el nivel adecuado de seguridad, el artículo 32, apartado 2, del RGPD exige que se preste especial atención a los riesgos que plantea el tratamiento, en particular los derivados de la destrucción accidental o ilícita, la pérdida, la alteración, la comunicación no autorizada o el acceso a datos personales transmitidos, almacenados o tratados de otro modo.

Spotify afirma que no tiene pruebas de que el acceso no autorizado a los datos personales de la parte reclamante fuera el resultado de un incidente de seguridad de Spotify. IMY no encuentra motivos para cuestionar la declaración de Spotify. IMY considera, a la luz de lo anterior, que la investigación no ha demostrado que ***SPOTIFY AB*** haya incumplido el artículo 32 del Reglamento General de Protección de Datos (RGPD), como se alega en la reclamación.

En el supuesto examinado, una vez analizadas las razones expuestas por ***SPOTIFY AB*** se constata la falta de indicios racionales de la existencia de una infracción, procediendo, en consecuencia, el archivo de las actuaciones realizadas, en aplicación del principio de presunción de inocencia que impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se derive la existencia de infracción.

Por lo tanto, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de la reclamación presentada, con fecha 11 de septiembre de 2018 y con número de registro de entrada 193823/2018

SEGUNDO: NOTIFICAR la presente resolución a la parte RECLAMANTE

TERCERO: INFORMAR a ***SPOTIFY AB*** sobre la decisión adoptada en la presente resolución

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el 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 a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1103-21112023

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos