- N/Ref.: **CO/00276/2020 – A61VM 125988**

RESOLUCIÓN DE ARCHIVO

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 adelante, RGPD) y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 30 de abril de 2020 y número de registro de entrada 015763/2020, tuvo entrada en esta Agencia una reclamación, relacionada con un tratamiento de carácter transfronterizo de datos personales realizado por el responsable de la app **ZOOM**, la empresa estadounidense **ZOOM VIDEO COMMUNICATIONS, INC.**, y el responsable de la red social **FACEBOOK.** La reclamación fue presentada por ***A.A.A.*** (en lo sucesivo, el reclamante) por una presunta vulneración de los arts. 5.1.a, 5.1.b, 5.1.f, 6, 13, 32, y 34 del RGPD (por parte de **ZOOM**), y arts. 6 y 14 del RGPD (por parte de **FACEBOOK**).

Los motivos en que el reclamante basa la reclamación son:

- El responsable de la app **ZOOM** cede a **FACEBOOK** datos personales de usuarios de su versión para el sistema operativo iOS de Apple (“Zoom Cloud Meetings”), sin conocimiento ni el consentimiento de los mismos. Esto se produce incluso sin ser los afectados usuarios de dicha red social.

- La persona que destapó los hechos, los publicó en su blog https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-ifyou-dont-have-a-facebook-account

- A raíz de dicha publicación, el propio responsable dio explicaciones en su portal web (en la dirección https://blog.zoom.us/wordpress/es/2020/03/27/uso-del-sdk-de-facebook-en-el-cliente-de-ios-por-parte-de-zoom/). El origen de la incidencia habría estado en la utilización del kit de desarrollo de Facebook (SDK) con el propósito de ofrecer un método alternativo de autenticación en la app (esto es, a través de las credenciales del usuario como miembro de Facebook). Dicho componente recogía información sobre dispositivos, como el tipo y la versión del sistema operativo móvil, la zona horaria del dispositivo, el sistema operativo del dispositivo, el modelo y el operador del dispositivo, el tamaño de la pantalla, los núcleos del procesador y el espacio en disco; no recogía información ni actividades relacionadas con reuniones, como asistentes, nombres, notas, etc.

- Sin embargo, el reclamante sostiene que sí que se recogían datos como el concreto modelo de dispositivo Apple y su “identificador publicitario único” del

terminal Apple (“ID de anunciante de iOS”), lo cual permite a **FACEBOOK** el poder dirigirse a los usuarios mediante anuncios.

- El responsable no ha comunicado expresamente a los afectados la ocurrencia de esta brecha de datos, ni se ha asegurado de que **FACEBOOK** haya eliminado la información personal recibida a través de este SDK incluido en la app de **ZOOM** para Apple. Igualmente, no ha informado a los titulares de los datos en relación con los propósitos de la cesión de datos a Facebook.

- De la misma manera, el responsable de la red social cesionaria de los datos, **FACEBOOK**, ha realizado un tratamiento del que también se desconoce finalidad, destinatarios, base de legitimación, etc. Además, no ha cumplido con su deber de información a los titulares de los datos personales, de los que ha obtenido datos de forma indirecta.

Junto a la reclamación se aporta certificación electrónica de la publicación de las mencionadas webs, y prueba de la adquisición por parte del reclamante de un terminal Apple en un centro comercial de Madrid.

SEGUNDO: Con fecha 23 de octubre de 2020, esta Agencia emitió resolución de archivo en relación con la parte de la reclamación que involucraba al responsable del tratamiento **ZOOM VIDEO COMMUNICATIONS, INC.**

TERCERO: El responsable de la red social **FACEBOOK** tiene en Irlanda su establecimiento principal para los tratamientos de datos personales de residentes europeos, la compañía **FACEBOOK IRELAND LTD**. Teniendo en cuenta el carácter transfronterizo de la parte de la reclamación restante, que involucra a **FACEBOOK**, la misma fue remitida a la autoridad de control de Irlanda, la *Data Protection Commission (DPC)*, por ser la competente para actuar como autoridad de control principal, a tenor de lo dispuesto en el artículo 56.1 del RGPD. Esta remisión se realizó, a través del “Sistema de Información del Mercado Interior” (IMI).

CUARTO: Para poder aceptar el caso, la autoridad de control de Irlanda requirió del reclamante la siguiente información: copia de la correspondencia intercambiada con **FACEBOOK** para reportar este asunto, aclaración sobre los datos personales suyos que cree que están siendo tratados por **FACEBOOK** (o lo que es lo mismo, que el reclamante acredite que es un afectado por el tratamiento de datos personales que supuestamente realiza **FACEBOOK**), y, por último, que exprese cuál sería su solución deseada en este asunto.

Esta Agencia cursó con fecha 24 de junio de 2020 una solicitud al reclamante solicitando esta información requerida por la DPC, acompañando una carta facilitada por ésta a tal efecto. En ella se indicaba que, en caso de no recibirse contestación en el plazo de 2 meses contados a partir de la fecha de la carta, la DPC consideraría retirada la reclamación.

La solicitud consta como entregada al destinatario con fecha de ese mismo día, pero no se ha recibido en esta Agencia respuesta a la misma por parte del reclamante.

FUNDAMENTOS DE DERECHO

I - Competencia

De acuerdo con lo dispuesto en el artículo 60.8 del RGPD, la Directora de la Agencia Española de Protección de Datos es competente para adoptar esta resolución, de conformidad con el artículo 12.2, apartado i) del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos y la Disposición transitoria primera 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, el responsable de la red social **FACEBOOK** tiene su establecimiento principal o único en Irlanda, por lo que la autoridad de control de este país es la competente para actuar como autoridad de control principal, en la parte de la reclamación que va referida al tratamiento de datos personales transfronterizo realizado por este responsable.

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, únicamente la AEPD actúa en calidad de "autoridad de control interesada".

VI - Cuestión reclamada y razonamientos jurídicos

En este caso, se ha presentado en la AEPD reclamación por una presunta vulneración de los art. 5.1.a, 5.1.b, 5.1.f, 6, 13, 14, 32 y 34 del RGPD en un tratamiento de datos personales realizado por **ZOOM VIDEO,** y de los arts. 6 y 14 del RGPD en uno realizado por **FACEBOOK.**

Con fecha 23 de octubre de 2020, esta Agencia emitió resolución de archivo en relación con la parte de la reclamación que involucraba al responsable del tratamiento **ZOOM VIDEO COMMUNICATIONS, INC.**

Teniendo en cuenta el carácter transfronterizo de la parte restante de la reclamación, que involucra a **FACEBOOK**, la misma fue remitida a la autoridad de control de Irlanda, la *Data Protection Commission (DPC)*, por ser la competente para actuar como autoridad de control principal, a tenor de lo dispuesto en el artículo 56.1 del RGPD.

Para poder aceptar el caso, la autoridad de control de Irlanda requirió del reclamante la siguiente información: copia de la correspondencia intercambiada con **FACEBOOK** para reportar este asunto, aclaración sobre los datos personales suyos que cree que están siendo tratados por **FACEBOOK** (o lo que es lo mismo, que el reclamante acredite que es un afectado por el tratamiento de datos personales que supuestamente realiza **FACEBOOK**), y, por último, que exprese cuál sería su solución deseada en este asunto.

Esta Agencia cursó con fecha 24 de junio de 2020 una solicitud al reclamante solicitando esta información requerida por la DPC, acompañando una carta facilitada por ésta a tal efecto. En ella se indicaba que, en caso de no recibirse contestación en el plazo de 2 meses contados a partir de la fecha de la carta, la DPC consideraría retirada la reclamación. La solicitud consta como entregada al destinatario con fecha de ese mismo día, pero no se ha recibido en esta Agencia respuesta a la misma por parte del reclamante.

En vista de que no se ha podido satisfacer un requerimiento formal que la autoridad principal considera imprescindible para aceptar a trámite el caso, debido a la ausencia de reacción del reclamante a una carta remitida y correctamente notificada en nombre de dicha autoridad, esta Agencia considera que solo cabe la conclusión de las presentes actuaciones y el archivo de la reclamación.

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

PRIMERO: PROCEDER AL ARCHIVO de la reclamación presentada en lo que respecta al tratamiento de datos personales realizado por **FACEBOOK**, con fecha con fecha 30 de abril de 2020 y con número de registro de entrada 015763/2020.

SEGUNDO: NOTIFICAR la presente resolución al RECLAMANTE

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 Directora 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.

1103-070820

Mar España Martí
Directora de la Agencia Española de Protección de Datos