Expediente Nº: E/01823/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **GRINDR LLC.** en virtud de denuncia presentada por la **ASOCIACION DE CONSUMIDORES Y USUARIOS EN ACCION FACUA,** la **CONFEDERACIÓN DE CONSUMIDORES Y USUARIOS (CECU)** y la **ORGANIZACION DE CONSUMIDORES Y USUARIOS** y teniendo como base los siguientes

HECHOS

PRIMERO: En abril de 2017, tuvo entrada en esta Agencia escritos de diversas Asociaciones de Consumidores contra la entidad ***GRINDR LLC*** (en lo sucesivo el denunciado) comunicando que los medios de comunicación han difundido una noticia relativa a la investigación realizada por la organización Sintef que habría detectado una posible comunicación de los datos relativos al *"estado de VIH"* y a la ubicación de los usuarios de la aplicación de citas gays GRINDR a dos compañías, contratadas para optimizar su programa informático, y que habría sido confirmada por uno de los responsables de la aplicación, al admitir que se facilitan datos a las entidades Apptimize o Localytics, encargadas de probar la aplicación.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados. Solicitada información a la entidad denunciada se tiene conocimiento de los siguientes extremos:

Grindr es una compañía estadounidense y que actualmente pertenece al 100% a la sociedad Beijing Kunlun Tech Co, Ltd.

La sede central de Grindr se encuentra en 750 N. San Vicente Boulevard, Suite RE#1400, West Hollywood, California 90069 (Estados Unidos). Grindr no cuenta ni con oficinas ni con empleados en España.

La aplicación de Grindr (la "**App de Grinder**" o la "**App**") es una aplicación para dispositivos móviles dirigida a la comunidad gay, de lesbianas, transgénero y bisexual en todo el mundo con el objeto de poner a su disposición una plataforma segura para conectarse y relacionarse.

La App de Grindr cuenta aproximadamente con unos 180.000 usuarios activos mensuales en España.

La voluntad de promover el bienestar de la comunidad LGTB llevó a Grindr a ofrecer a sus usuarios la posibilidad de compartir su estatus respecto al Virus de Inmunodeficiencia Humana ("**VIH**") así como la última fecha en que hubiera realizado

una prueba de VIH, constituyendo una herramienta útil para luchar contra la amenaza mortal que dicha dolencia representa.

El único propósito de Grindr a la hora de recoger información relativa al VIH es permitir a sus usuarios compartir voluntariamente información sobre su situación respecto al VIH por medio de la App de Grindr.

Grindr nunca ha vendido este tipo de información, ni la ha utilizado con fines de marketing o a permitido a tercero alguno utilizar la información referida al VIH para un propósito distinto a asegurar la operativa de la App por parte de Grindr.

Los motivos para la recogida de la fecha en la que un usuario realizó por última vez una prueba médica de VIH son: permitir a la App de Grindr remitir recordatorios periódicos para que tales usuarios realicen de nuevo la prueba; y permitir, a través de la App de Grindr compartir voluntariamente información respecto a la última fecha en que se realizaron la prueba del VIH.

En relación, a una supuesta brecha de seguridad de Grindr y que la entidad habría comunicado información sobre la situación respecto al VIH de sus usuarios a terceros, los representantes de la entidad manifiestan que ambas afirmaciones son erróneas.

Grindr confirma que no ha sufrido brecha de seguridad alguna, tanto en general como respecto a los datos personales que custodia, tampoco tiene conocimiento de la destrucción accidental o ilegal, o de la pérdida, alteración, revelación o acceso no autorizados a tales datos personales.

En relación con la comunicación de datos, la entidad afirma que compartió información relativa al VIH con terceros proveedores de servicios que actuaban como encargados de tratamiento y permitió dicho acceso de forma exclusivamente confidencial, segura, encriptada, legal, leal y transparente, de conformidad con los principios de la normativa de protección de datos personales.

La información relativa al VIH fue compartida con dos proveedores de servicios de la compañía: Apptimize y Localytics. Ambas empresas fueron contratadas por Grindr para ayudarle a comunicarse con sus usuarios y remitir notificaciones periódicas sobre la necesidad de realizarse pruebas de VIH.

Los representantes de la entidad aportan copia del contrato suscrito con APPTIMIZE INC, que contiene un apartado relativo a la confidencialidad y protección de datos.

También aportan copia del contrato suscrito con LOCALYTICS que contiene un apartado relativo a la confidencialidad de los datos a los que tenga acceso.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36,

ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

El artículo 9.1 de la LOPD establece que:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

Y el artículo 10 de la LOPD, relativo al deber de secreto, establece que:

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

IV

El artículo 11. 1 y 2 de la LOPD, relativo a la cesión de datos, señala lo siguiente:

"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica."

Asimismo, el artículo 3. i) de la citada norma define la "cesión o comunicación de datos" como *"toda revelación de datos realizada a una persona distinta del interesado".*

V

El artículo 12 de la LOPD *"acceso a datos por cuenta de terceros",* establece lo siguiente:

"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

El citado artículo 12.1 de la LOPD permite que el responsable del fichero habilite el acceso a datos de carácter personal por parte de la entidad que va a prestarle un servicio –encargado del tratamiento- sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión de datos. La LOPD exige que el acceso a datos por cuenta de terceros figure reflejado en un contrato por escrito o en alguna otra forma que permita acreditar su celebración y contenido, y prevé unos contenidos mínimos, tales como seguir las instrucciones del responsable del tratamiento, no utilizar los datos para un fin distinto, no comunicarlos a otras personas, estipular las medidas de seguridad del artículo 9 y, cumplida la prestación, destruir los datos o proceder a su devolución al responsable del tratamiento.

En el presente caso, ha quedado la entidad denunciada ha confirmado que no ha sufrido brecha de seguridad alguna, tanto en general como respecto a los datos personales que custodia, tampoco tiene conocimiento de la destrucción accidental o ilegal, o de la pérdida, alteración, revelación o acceso no autorizados a tales datos personales.

En relación con la comunicación de datos, la entidad afirma que compartió información relativa al VIH con terceros proveedores de servicios que actuaban como encargados de tratamiento y permitió dicho acceso de forma exclusivamente confidencial, segura, encriptada, legal, leal y transparente, de conformidad con los principios de la normativa de protección de datos personales.

En consecuencia, no ha quedado acreditado que se haya producido vulneración de la normativa de protección de datos en relación con el tratamiento de los datos por parte de las citadas entidades encargadas del tratamiento, en nombre y por cuenta de la entidad denuncia.

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **GRINDR LLC.,** la **ASOCIACION DE CONSUMIDORES Y USUARIOS EN ACCION FACUA,** la **CONFEDERACIÓN DE CONSUMIDORES Y USUARIOS (CECU)** y a la **ORGANIZACION DE CONSUMIDORES Y USUARIOS.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la

LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

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