- **Expediente N.º: EXP202201227**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 10/12/2021 y fecha 21/12/2021, se presentaron 2 reclamaciones ante la Agencia Española de Protección de Datos contra ***XFERA MÓVILES, S.A.*** con NIF ***A82528548*** (en adelante, XFERA).

Los motivos en que se basa la primera reclamación (en lo sucesivo, reclamación nº1) son los siguientes:

Afirma la parte reclamante que se habría producido el día 9/12/2021 un tratamiento sin consentimiento de sus datos personales, con la consecuencia que un tercero habría obtenido un duplicado de su tarjeta SIM vulnerando las medidas de seguridad.

Junto a la notificación se aporta pantallazo del SMS recibido, en el que la entidad bancaria indica que un dispositivo no autorizado se ha conectado a la cuenta online del reclamante, pantallazo del área de cliente en el que consta una dirección de correo electrónico incorrecta asociada a los datos del reclamante y denuncia ante la Policía, de fecha 10 de diciembre de 2021.
Con fecha 21/12/2021, se presentó la segunda reclamación contra XFERA (en lo sucesivo, reclamación nº2) por hechos similares.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de ambas reclamaciones a XFERA, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

TERCERO: Con fechas 10/03/2022 y 21/03/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las reclamaciones presentadas

CUARTO: Con fecha 14/03/2022 se recibe en esta Agencia escrito de respuesta al traslado relativo a la parte reclamante nº1 y con fecha 22/03/2022 a la parte reclamante nº2, siendo una parte general de ambas contestaciones idéntica, porque los hechos descritos tienen su origen en un incidente de seguridad y en la que se indica lo siguiente:

El día 07/12/2021 detectó XFERA un incidente de seguridad, consistente en que una banda de ciberdelincuentes realizaba duplicados de tarjetas SIM de forma fraudulenta,

y que fue reportado a esta Agencia el día 10/12/2022. El incidente fue puesto en conocimiento de XFERA el 07/12/2021 por ***EMPRESA.1** (en lo sucesivo ***EMPRESA.1), proveedor del sistema vulnerado.

***EMPRESA.1 detecta un incremento del umbral de consultas legítimas de la base de datos, en relación con un incidente sobre la disponibilidad de la aplicación Terminal Punto de Venta (TPV), utilizado por las tiendas para la gestión de sus servicios a usuarios finales de la marca Yoigo; los atacantes no consiguieron acceso a los privilegios en el sistema por la contención temprana del incidente y no hay evidencia exfiltración alguna de los datos contenidos en la base de datos.

Los atacantes acceden al sistema TPV con usuarios y contraseñas válidos que usan para la generación de las solicitudes de duplicado de SIM, sustituyendo la dirección email de contacto del cliente para generar una solicitud de duplicado con los datos que previamente ya tenían del cliente. Evitan así los delincuentes la primera capa de identificación y controles con los que XFERA lleva trabajando desde 2019. Este incidente de seguridad tiene lugar entre los días 7/12/2022 y 23/12/2022, fecha en la que XFERA considera cerrada la brecha de seguridad; en este lapso atacantes adoptan una serie de medidas y XFERA las contramedidas oportunas para neutralizar el ataque.

XFERA declara que lleva años implementando mejoras en el proceso de solicitud de duplicados de tarjeta SIM. El sistema TPV cuenta con auditorías periódicas y medidas de seguridad robustas, y fue vulnerado sirviéndose de credenciales legítimas, presuntamente extraídas mediante ataques de phishing a las tiendas afectadas, que llegaron a recibir hasta 9.000 correos en los días del incidente. Tan pronto fue detectado el fraude, se fueron implementando medidas de seguridad en base a la información obtenida en tiempo real, las cuales eran superadas, también en tiempo real, por los ciberdelincuentes, hasta el mismo día 23/12/2021, fecha de cierre de la brecha de seguridad. Aporta como Documento n.º 1 el informe de cierre del mencionado incidente, remitido a esta Agencia con fecha 10 de enero de 2022.

QUINTO: En la respuesta al traslado relativo de XFERA, recibida en esta Agencia en fecha 14/03/2024, se concreta para el reclamante nº1, que fue víctima del ciberataque el día 9/12/2021 y que el duplicado de su tarjeta SIM fue detectado por análisis de fraude a las 19:19 h bloqueado a las 19:42 h. El interesado fue informado de lo sucedido por Control de Servicio con la información disponible en ese momento, condición necesaria para proceder a enviar un nuevo duplicado de tarjeta SIM, el cual se llevó a cabo en los días sucesivos. Con posterioridad se han intentado comunicaciones con la parte reclamante sin éxito.

Concluye XFERA que los ciberdelincuentes debían de disponer previamente de información sobre la parte reclamante nº1 para poder realizar el cambio de la dirección de correo electrónico del interesado directamente en el sistema, porque los cambios no se llevaban a cabo aleatoriamente, ni los atacantes accedían a sistemas que permitieran extraer información del cliente. Con esa información, lograron modificar el correo electrónico y hacerse con el código QR necesario para activar la tarjeta SIM. Con la SIM y las credenciales de acceso a la entidad bancaria (cuyo origen XFERA desconoce) consiguen los delincuentes la confirmación de las operaciones bancarias denunciadas de sustracción de las cantidades.

SEXTO: En la respuesta al traslado relativo de XFERA, recibida en esta Agencia en fecha 22/03/2024, se concreta para el reclamante nº2 que fue víctima del ciberataque de 9/12/2021 y que el duplicado de tarjeta SIM de la interesada se llevó a cabo a las 16:55h y fue detectado aplicado bloqueo por análisis de fraude a las 17:37h. La interesada fue informada de lo sucedido por Control de Servicio, condición necesaria para proceder a enviar un nuevo duplicado de tarjeta SIM, el cual se llevó a cabo en los días sucesivos. Con posterioridad, XFERA se puso en contacto con ella el 23/12/2021 para completar la información proporcionada. Señala XFERA que la cuenta de ******EMPRESA.2***, se vulnera con carácter previo a la realización del duplicado de tarjeta SIM, con algo más de 5 minutos de diferencia, según la denuncia, lo cual acredita que los ciberdelincuentes cuentan de antemano con información de los interesados, incluido acceso a su cuenta bancaria, con carácter previo a la realización del duplicado.

Concluya XFERA que los ciberdelincuentes debían de disponer previamente de información también sobre la parte reclamante nº2 para poder realizar el cambio de la dirección de correo electrónico del interesado directamente en el sistema, porque los cambios no se llevaban a cabo aleatoriamente, ni los atacantes accedían a sistemas que permitieran extraer información del cliente. Con esa información, lograron modificar el correo electrónico y hacerse con el código QR necesario para activar la tarjeta SIM. Con la SIM y las credenciales de acceso a la entidad bancaria (cuyo origen XFERA desconoce) consiguen los delincuentes la confirmación de las operaciones bancarias denunciadas de sustracción de las cantidades.

.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

III
Integridad y confidencialidad

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

IV
Prescripción de las posibles infracciones

El RGPD tipifica el tratamiento de datos de personales sin contar con base de legitimación y sin respetar los principios relativos al tratamiento en el artículo 83.5 al señalar:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"

Por su parte, la LOPDGD, en sus artículos 72, 73 y 74, califica a efectos de prescripción las infracciones al RGPD estableciendo que las infracciones muy graves prescriben a los tres años, las graves a los dos años y las leves transcurrido un año desde que se cometieron.

En concreto, el artículo 72 señala (se subraya lo relevante al caso):

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:
a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.

Por su parte el Artículo 72 establece lo siguiente (se subraya lo relevante al caso):

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

A su vez, la Ley 39/2015 Procedimiento Administrativo Común establece en el apartado 1º Artículo 21. La obligación de resolver los procedimientos por prescripción del siguiente modo: "*1. La Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación. En los casos de prescripción, (…), la resolución consistirá en la declaración de la circunstancia que concurra en cada caso, con indicación de los hechos producidos y las normas aplicables."*

V
Conclusión

A tenor de lo dispuesto en los artículos 72 y 73 de la LOPDGDD antes citados, las infracciones de los artículos 32.1 y 5.1 del RGPD, prescriben respectivamente a los 2 y 3 años desde que tuvieron lugar los hechos.

En el caso que nos ocupa, los hechos objeto de las reclamaciones nº1 y número 2 contra XFERA se remontan al 9/12/2021 y tienen como causa una brecha de confidencialidad de datos que se considera terminada el 23/12/2021. Esto significa que han transcurrido
ya más de tres años contados desde el 9/12/2021, día en el que se produce el incidente de seguridad y la suplantación sufrida por los reclamantes, con lo que cualquier posible infracción derivada de tales hechos habría prescrito ya el día 09/12/2024.

En definitiva, en base a lo indicado en los párrafos anteriores, habiendo transcurrido ya más de tres años desde los hechos reclamados, habría prescrito cualquier presunta infracción del RGPD.

Atendiendo a lo anterior, al haber prescrito las posibles infracciones del RGPD, procede dictar resolución en los términos previstos por el artículo 21 de la LPACAP.

En consecuencia, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución **a XFERA MÓVILES, S.A.** y a la parte reclamante Nº1 y Nº2.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará 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.

940-101025

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