- **Expediente N.º: EXP202311252**

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 27 de junio de 2023, se presentó reclamación con número de registro de entrada REGAGE23e00042081608 ante la Agencia Española de Protección de Datos por parte de ***A.A.A.*** (en adelante, la parte reclamante) contra **XFERA MÓVILES, S.A.U.** con NIF ***A82528548*** (en adelante, XFERA). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que el 19/05/2023, como tras recibir una llamada identificándose como Yoigo (nombre de la marca comercial de XFERA) del número ******TELÉFONO.1***, contrató una rebaja en su factura y adquirió un terminal móvil a coste cero. Señala que la contratación se realizó mediante llamada desde el número de teléfono ******TELÉFONO.1*** y a través de la aplicación WhatsApp por conversación con el número ******TELÉFONO.2***.

Indica también la parte reclamante que le informan, una vez contratada la mejora, de que ha habido un error en el envío, pero que, no obstante, recoja el terminal en la oficina de correos, para que un mensajero pueda ir a recogerlo a su domicilio y que ya le enviarán el terminal correcto posteriormente.

Una vez recogido el terminal de su domicilio, el reclamante comprueba en la web de XFERA que consta que, en realidad, ha adquirido el terminal Xiaomi recogido en su domicilio, y que deberá abonarlo en 24 cuotas. Considera que esta contratación se ha realizado sin su consentimiento, por lo que reclama a XFERA contra la contratación indebida.

Junto a su reclamación aporta conversación a través de WhatsApp mantenida con los números de teléfono indicados, que creía que eran de XFERA, así como el historial de llamadas recibidas desde esos números y la tarifa contratada con XFERA, sin su consentimiento.

Documentación relevante aportada por la parte reclamante:

- Conversación a través de WhatsApp mantenida supuestamente con XFERA con el número ******TELÉFONO.2*** entre los días 23, 26, 30 y 31 de mayo de 2023,
- Número de reclamación interpuesta ante YOIGO, de 9/6/2023,
- Historial de llamadas recibidas del n.º ******TELÉFONO.1*** entre el 19/5/2023 y 12/6/2023, supuestamente de Yoigo, de las que fueron atendidas la llamada de 19/5/2023, dos llamadas de 23/5/2023 y tres llamadas de 26/5/2023.

- Tarifa contratada sin su consentimiento, según indica.

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 dicha reclamación 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.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 22/08/2023 como consta en el acuse de recibo que obra en el expediente.

El 22/09/2023 contesta XFERA al traslado de la reclamación, indicando que la línea ******TELÉFONO.1*** no se corresponde con ninguno de los servicios de fidelización ni de atención al cliente de XFERA, sino que pertenece a un cliente particular, también cliente de XFERA. Según el relato del interesado, la comunicación continúa vía WhatsApp, pero en el canal de Whatsapp original de XFERA son los clientes quienes tienen que iniciar la conversación proactivamente.

Indican que el interesado aporta al expediente una conversación por Whatsapp con el presunto comercial de día 23 de mayo de 2023, en el transcurso de la cual se informa de una oferta (falsa) y, para ganarse la confianza del interesado, le proporciona una factura de Yoigo.

Tras realizar las comprobaciones para este caso, se comprueba que el interesado recibió varias llamadas en aplicaciones tipo Skype coincidentes temporalmente con los hechos. Ningún comercial, ni servicio de XFERA utiliza servicios como Skype o llamadas de WhatsApp para ponerse en contacto con los clientes.

Las horas de los mensajes de WhatsApp que recibe y que aporta en esta reclamación son posteriores o simultáneos a estas llamadas, sin que XFERA pueda certificar el origen al tratarse de llamadas tipo Skype.

Del tráfico del interesado y de los logs del área cliente del interesado, se desprende que se realizó un cambio de contraseña el mismo día 23 de mayo desde una IP sospechosa (distinta a la del resto de accesos al área privada del interesado) con anterioridad a la hora en la que le envían su factura.

A través del área privada se pueden descargar las facturas de los clientes y ***(…).*** En la extracción del tráfico del interesado, se aprecia una llamada por Skype a las 20:51 y a las 21:17 ***(…)***. La factura es proporcionada a las 21:26.

Estos hechos hacen pensar que el interesado proporcionó en algún momento el código para resetear la contraseña del área privada a las personas que se pusieron en contacto con él, pese a que en el SMS que enviamos se indica que ese código no se proporcione a nadie.

XFERA envía los terminales móviles a la oficina de Correos más cercana a su domicilio del interesado, para que aporten la documentación necesaria para llevar a cabo la financiación y así firmar el contrato para el terminal entregado.

Concluye XFERA que existe una alta probabilidad de que el interesado haya sido víctima de un vishing y que se produce después una contratación en nombre del interesado, aportando los suplantadores toda la información requerida para ello. Ni es correcto el código de envío para seguimiento del envío aportado, ni tampoco el nombre por el que la llaman. En la conversación de WhatsApp, los delincuentes convencen incluso al interesado de que el contrato firmado no es válido y el cliente lo firma con esa creencia y les entrega el terminal.

TERCERO: Con fecha 26 de septiembre de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

La contratación de la terminal Xiaomi, se realiza el 23/5/23 como resultado de la llamada por teléfono del mismo número de teléfono del 19/05/2023 y a través de recepción por la aplicación WhatsApp desde los números ******TELÉFONO.2*** y ******TELÉFONO.1.***

Durante las presentes actuaciones previas se ha investigado a XFERA MÓVILES, S.A. con ***NIF A82528548*** con domicilio en AVENIDA DE BRUSELAS, N.º 38 - 28108 ALCOBENDAS (MADRID), para lo que se comprueba en primer lugar la titularidad de las líneas de teléfono desde la que se desde la que se reciben las llamadas y se intercambian los mensajes por WhatsApp.

XFERA no es titular de las 2 líneas de teléfono involucradas, sino que son personas físicas particulares, ***B.B.B.*** y de ***C.C.C.***, de nacionalidad ***(…)***, quienes han contratado con XFERA ambas líneas en modalidad de prepago, utilizando para ello su número de pasaporte. Ambas líneas fueron desactivadas poco después de la contratación del terminal por los interesados.

Tras enviarle XFERA el terminal Xiaomi al cliente, los suplantadores le informan de que se le ha enviado un modelo erróneo, pero que, no obstante, lo retire de Correos y un mensajero irá a recoger el terminal a su domicilio, y le enviarán el terminal correcto posteriormente. Una vez recogido el terminal y firmado el contrato, la parte reclamante comprueba en la web de Yoigo que consta que ha adquirido un terminal Xiaomi con las condiciones asociadas; al llamar a sendos números de teléfono ******TELÉFONO.2*** y ******TELÉFONO.1*** constata que esos números ya no existen.

Concluye XFERA que se trata de un caso “vishing”, una estafa de ingeniería social por teléfono, por la que se obtienen los datos del cliente, primero suplantando la identidad

de XFERA mediante llamadas realizadas en su nombre, para conseguir la información adecuada del propio cliente y para suplantar a su vez también su personalidad y contratar servicios en su lugar, una vez ganada la confianza del cliente.

Por su parte, el reclamante niega categóricamente haber solicitado cambio de contraseña en su área de cliente de XFERA el día 23/05/2023, ni ningún otro día, ni recibir en esa fecha ningún SMS de XFERA con un código válido durante 24 horas, así como haber facilitado su OTP para el cambio de contraseña. También niega haber utilizado Skype en esta acción, y aporta incluso copia de las últimas comunicaciones llevadas a cabo con Skype.

Por ello, la investigación se dirige a comprobar si las medidas aplicadas por XFERA han sido las adecuadas para garantizar la seguridad en el tratamiento de los datos personales de la parte reclamada en esta contratación.

XFERA explica con carácter general la política de seguridad que aplica con carácter general:

1) La política de seguridad de acceso al área privada y para el cambio de contraseña requiere una combinación de ***(…).***

   En caso de no recordar la contraseña, los clientes tienen la opción "¿No puedes entrar?" en la que se abre un cuadro de diálogo donde se requiere introducir ***(…)***, en caso contrario, daría error. En caso de tratarse de un cliente de Yoigo, se envía ***(…).***

2) La política de seguridad aplicada en capas requiere para el proceso de renuevo y firma del contrato: ***(…),*** y como medida reforzada proporcionar un ***(…)***. En este caso, para terminales que incluyen financiación, el terminal es enviado ***(…)***.

XFERA afirma que el proceso y contratación de nuevo terminal solo puede iniciarlo el propio cliente, y no XFERA. Aporta los logs de llamadas y SMS recibidos por el reclamante, relacionados con las capturas de pantalla de las llamadas y los mensajes de WhatsApp aportados por la parte reclamante, que explican (en hora CEST) la cronología sucesiva de los hechos.

XFERA aporta las evidencias sobre el envío del ***(...)***, a la línea telefónica de la parte reclamante y de que firmó un contrato para la nueva tarifa y un terminal Xiaomi, aportando incluso copia de su DNI en la oficina de Correos.

Manifiesta XFERA que las dos llamadas telefónicas 23/5/23, de unos 20 minutos y de unos 5 minutos de duración, tienen lugar en paralelo con una conversación de WhatsApp del interesado con el suplantador; durante estas llamadas conseguiría el suplantador, mediante engaño al cliente, el ***(...)***, el cambio de contraseña remitido al n.º de la parte reclamante, ya que consta en sistemas de XFERA que el cambio de contraseña fue realizado introduciendo el ***(...)*** correcto.

Explica XFERA que, con esta contraseña, consigue la última factura de la parte reclamante, que le reenvía para por WhatsApp, para convencerle de que

efectivamente la transacción se realiza con XFERA, al conocer así exactamente qué servicios tenía contratados. Finalmente, el suplantador llamó a la parte reclamante para informarle que había un error en el dispositivo enviado para que lo recogiera en Correos, donde firma el contrato junto con su DNI, requisito sin el que sería imposible la adquisición de un bien a plazos con XFERA.

Concluye XFERA que el suplantador obtiene el terminal en el domicilio de la parte reclamante y de su propia mano, cargándole también su coste: con ello se cierra el círculo del vishing, haciéndole creer además que el terminal correcto estaba de camino.

Concluye el informe de las actuaciones previas de la AEPD que las evidencias recogidas en la investigación son básicamente coincidentes con las manifestaciones de XFERA y que la conducta del afectado ha podido inducir los hechos investigados.

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
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción por parte de XFERA en el ámbito competencial de la Agencia Española de Protección de Datos.

La parte reclamante ha reconocido la firma del contrato de línea telefónica aportando incluso copia de su DNI, al efecto. También reconoce haber entregado el terminal contratado a los presuntos suplantadores, en la creencia de que se trataba del personal de XFERA y de que el contrato firmado no era válido en ese momento.

Las evidencias y testimonios no aclaran de modo concluyente la manera en la que los presuntos suplantadores consiguieron las claves necesarias para acceder a los datos

personales de la parte reclamante, ni a su cuenta en el Área de Usuario del sitio web de XFERA.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir responsabilidad a XFERA por los hechos objeto de reclamación, 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.U.** y a la parte 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 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.

940-301023

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