Expediente N.º: EXP202403230

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: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 19 de enero de 2024 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra XFERA MÓVILES, S.A.U. con NIF A82528548 (en adelante, la parte reclamada o Xfera). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 27 de junio de 2021, sustraen su DNI de su vehículo, presentando denuncia policial. Señala que la persona que realiza el robo acude a un establecimiento de la parte reclamada, solicitando una tarjeta SIM de su teléfono. Indica que le entregan copia de la tarjeta SIM, siendo objeto de robo de ***XXX*** euros en su cuenta bancaria.

Junto a su reclamación aporta:

-Denuncia ante la Guardia Civil, con fecha 28 de junio de 2021. -Puesto Utebo- Atestado nº ******ATESTADO.1***, a través de la cual el reclamante manifiesta el robo de teléfono móvil, el cual portaba tarjeta SIM con número ******TELÉFONO.1,*** tarjetero metálico el cual contenía el DNI a su nombre y las tarjetas de crédito.

-Ampliación de denuncia, con fecha 8 de julio de 2021, ante la Guardia Civil -Puesto Utebo-, subsanando el error del número de móvil, siendo el ******TELÉFONO.2***, manifestando que accedieron a su teléfono móvil principal al ******TELÉFONO.3***, que clonaron la SIM del ******TELÉFONO.3*** y realizaron a través de la aplicación BIZUM, una sustracción de ***XXX euros***.

-Anexa los documentos que detallan las operaciones de BIZUM, en los que se muestran los datos del beneficiario y las horas a las que se realizan estas operaciones.

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 la parte reclamada, 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 11 de marzo de 2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 14 de abril de 2024 se recibe en esta Agencia escrito de respuesta indicando

"Como conoce esta Agencia, a quien hemos proporcionado nuestros procedimientos en varias ocasiones, para realizar un duplicado de tarjeta SIM es necesario aportar documento de identidad original, lo cual, en el caso del interesado, se explica con el desafortunado robo de su documento nacional de identidad unos días antes de los hechos denunciados. En este sentido, el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica establece en su artículo 1.1 que "Su titular estará obligado a la custodia y conservación del mismo". En este sentido, mi representada, no tenía posibilidad de conocer que el DNI del interesado había sido sustraído, por lo que la primera capa de seguridad en la realización de duplicados de tarjeta SIM se superó por este motivo. Siguiendo con el caso que nos ocupa, aporta el interesado información sobre los movimientos realizados a través de Bizum, constando actividad en su cuenta desde las 20:17:32 del 7 de julio de 2021.

A las 20:22:20, saltó alarma en el sistema de fraude de mi representada, ***(…).*** *Aportamos a continuación detalle de la alarma. A las 20.25.25, tres minutos después de la detección, se produjo en la línea del interesado bloqueo de recepción SMSs por parte de uno de los agentes de control de servicio, impidiéndose la recepción de SMS por la línea afectada desde ese momento. El bloqueo fue levantado el 8 de julio de 2021, una vez la línea fue recuperada por el interesado y se realizaron las comprobaciones oportunas por parte del personal de control de servicio con el interesado.*

En lo que se refiere a la sustracción de dinero a través de BIZUM, hay elementos que desconocemos y que consideramos relevantes de cara a entender qué ha sucedido realmente en el caso que nos ocupa, particularmente en lo relativo a los tiempos de detección del duplicado fraudulento por parte de los sistemas de fraude. Estas cuestiones serían necesarias de cara a determinar si las medidas de seguridad implementadas por mi representada funcionaron correctamente de cara a la prevención y detección de la realización del duplicado de tarjeta SIM objeto de este caso, ya que, como sabe esta Agencia, mi representada cuenta con un sistema de seguridad por capas en la que la solicitud del DNI, que en un caso como este, en el que el DNI ha sido sustraído, es una medida más.

Por ejemplo, conforme informa BIZUM en su página web en relación con su funcionamiento, indica que la transferencia la realiza directamente el banco, en quien se delega la función de autenticar al cliente. En este sentido, indican que tienen que autenticar la compra desde la aplicación bancaria.

En el caso que nos ocupa no se proporciona información de la aplicación bancaria que se vio afectada. Si, como indica BIZUM, para confirmar las operaciones es necesario completar la operación en la aplicación bancaria, esto implica que los

ciberdelincuentes tenían acceso a la aplicación bancaria del interesado, la cual debería contar con un doble factor de autenticación: usuario y contraseña y un segundo factor desconocido, que podría ser un SMS u otro como por ejemplo, biometría.

(…).

Desafortunadamente, debido al tiempo transcurrido, no disponemos de información del tráfico del día 7 de julio de 2021, el cual habría ayudado a esclarecer, junto con los logs del sistema, los hechos experimentados por el interesado y a evaluar la efectividad de las medidas de seguridad implementadas por mi representada.

Otra opción podría ser que el segundo factor de autenticación para acceder a la aplicación del banco no consistiera en un SMS, lo que supondría que los ciberdelincuentes tenían conocimiento al menos, del número de cuenta del interesado y sus credenciales de acceso a tal cuenta, incluido el doble factor. Otra cuestión que nos planteamos es si el delincuente tenía acceso a la aplicación bancaria, así como al segundo factor de autenticación (SMS) por qué optó por enviar dinero a través de BIZUM, cuando esta plataforma tiene un límite y no realizar una transferencia bancaria, lo cual podría explicarse si el SMS no fuera el segundo factor de autenticación para acceder a la aplicación bancaria y, por tanto, el ciberdelincuente dispusiera de bastante más información del interesado y del segundo factor desconocido, de forma completamente ajena a mi representada".

TERCERO: Con fecha 17 de abril de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 Directora 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

Licitud del tratamiento

El artículo 6 del RGPD detalla en su apartado 1 los supuestos en los que el tratamiento de datos de terceros es considerado lícito:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

III

Prescripción

El artículo 83.5 del RGPD indica lo siguiente:

"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."

La LOPDGD, a efectos de la prescripción de la infracción, califica en su artículo 72.1 de

infracción muy grave, siendo en este caso el plazo de prescripción de tres años, *"b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidos en el artículo 6 del Reglamento (UE) 2016/679"*.

III
Reclamación

En el presente caso, la parte reclamante presenta reclamación contra la parte reclamada, por una presunta vulneración del artículo 6 del RGPD en relación con la licitud del tratamiento de sus datos personales porque se han utilizado sus datos personales sin su consentimiento, para la obtención de un duplicado de su tarjeta SIM, tras haberle sustraído su DNI.

IV
Conclusión

De las actuaciones realizadas y las informaciones obtenidas no se infiere por la parte reclamada una conducta negligente en la facilitación del duplicado de la tarjeta SIM de la línea de la parte reclamante. De las informaciones obtenidas se desprende que la parte reclamada ha seguido el protocolo previsto a la hora de identificar al solicitante de la tarjeta SIM, sin perjuicio de la posibilidad de que dicho solicitante pudiera haber suplantado la identidad de la parte reclamante debido a la sustracción del DNI de ésta.

Teniendo lo anterior en cuenta, la parte reclamada actuó poniendo las medidas adecuadas, pero el resultado no fue el esperado.

Todas estas actuaciones indican el cumplimiento de una diligencia razonable por parte de la reclamada, no pudiendo exigir a esta responsabilidad respecto a tratamientos realizados en virtud de una suplantación de identidad si han seguido los protocolos de seguridad establecidos.

Por tanto el tratamiento realizado por la parte reclamada se ajusta a lo establecido en el artículo 6 del RGPD y, sin perjuicio que dicha relación pueda ser cuestionada ante el orden jurisdiccional correspondiente habida cuenta que el reclamante manifiesta y así lo denunció ante la Policía que alguien suplantó su identidad utilizando sus datos personales para contratar con la citada operadora de telecomunicación utilizando copias de documentos identificativos de su personalidad tales como su DNI.

De la documentación obrante en el expediente se desprende ausencia del elemento subjetivo de culpabilidad necesario en la actuación de la parte reclamada para ejercer la potestad sancionadora.

A este respecto, la Sentencia de la Audiencia Nacional de 22 de marzo de 2012 SAN 1465/2023 se pronuncia sobre un supuesto similar, en los siguientes términos "(...) es *decir, conforme a lo pactado, se exigió por el establecimiento la documentación correspondiente para cotejar si el titular de la tarjeta coincidía con el que figuraba en el DNI y con la fotografía que constaba en el documento de identidad, anotándose en el citado documento de venta el número de DNI exhibido por el cliente, que coincidía con*

el número del denunciante, por lo que si se verificó la identidad del comprador. (...)

Por todo lo cual y a la vista de las especiales circunstancias concurrentes en el caso de autos, no cabe apreciar culpabilidad alguna (ni siquiera a título de culpa o falta de diligencia) en la actuación de la entidad recurrente, que actuó en la creencia de que la persona con la que contrataba era quien decía ser y se identificaba como tal con una documentación en apariencia auténtica y a ella correspondiente, por lo que estaba legitimada para el tratamiento de sus datos de carácter personal. En consecuencia, al faltar uno de los requisitos exigidos para la imposición de sanción por vulneración del principio del consentimiento consagrado en el artículo 6.1 de la LOPD, procede dejar sin efecto la sanción impuesta por la comisión de dicha infracción."
(…)
"Por todo lo cual, conforme a lo argumentado respecto de la infracción de vulneración del principio del consentimiento, no cabe tampoco respecto de esta infracción apreciar culpabilidad en la actuación de la entidad recurrente, que actuó en la creencia errónea de que la deuda que trató en sus ficheros y comunicó a los ficheros de solvencia patrimonial y crédito, era atribuible a la persona que efectuó la compra y obligada al pago aplazado, que se identificó documentalmente con el nombre, apellidos y DNI del denunciante, cuya identidad suplantó."

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

Por otra parte, la posible actuación infractora de la reclamada se encontraría prescrita por el transcurso de los tres años de prescripción de las infracciones muy graves, tal y como señala el artículo 72.1 de la LOPDGDD, a contar desde el momento del tratamiento por la parte reclamada.

Así pues, al no haber sido posible atribuir la responsabilidad por el tratamiento y además al estar prescrita la posible infracción de acuerdo con lo señalado, por la Directora 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. con NIF A82528548 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 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.

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