- **Procedimiento N.º: PS/00027/2021**

Recurso de reposición N.º RR/00774/2021

Examinado el recurso de reposición interpuesto por ***XFERA MÓVILES, S.A.*** (en adelante, la parte recurrente o XFERA) contra la resolución dictada por la directora de la Agencia Española de Protección de Datos (en lo sucesivo, AEPD), en el procedimiento sancionador PS/00027/2021, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 10 de noviembre de 2021, se dictó resolución por la directora de la AEPD en el procedimiento sancionador PS/00027/2021, en virtud de la cual se imponía a una sanción de 200.000'00 euros (doscientos mil euros), por la vulneración de lo dispuesto en artículo 5.1.f) 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 y por el que se deroga la Directiva 95/46/CE (en lo sucesivo RGPD), tipificada en el artículo 83.5.a) del RGPD y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Dicha resolución, que fue notificada a la parte recurrente en fecha 12 de noviembre de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la LOPDGDD, y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00027/2021, quedó constancia de los siguientes:

> PRIMERO: XFERA es la responsable de los tratamientos de datos referidos en esta Resolución, toda vez que conforme a la definición del artículo 4.7 del RGPD es quién determina la finalidad y medios de los tratamientos realizados, tal y como informa su Política de Privacidad: "*El responsable será la sociedad **XFERA MÓVILES, S.A.U,** con NIF: **A-82528548** y dirección social situada en Avenida de Bruselas, 38, 28108, Alcobendas (Madrid), España. Esta sociedad ofrece servicios de telecomunicaciones a través de diferentes marcas como MÁSMÓVIL, Yoigo, LlamaYa y HappyMóvil."*
>
> SEGUNDO: XFERA presta sus servicios de telefonía móvil a través de cuatro marcas comerciales aquí analizadas que son: YOIGO, MÁSMÓVIL, LLAMAYA y LEBARA. Cada una de ellas dispone de distintas operativas de funcionamiento.
>
> TERCERO: Con fecha 8 de octubre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte RECLAMANTE UNO (expediente con núm. de referencia ***E/11270/2019***), dirigida contra XFERA, tras expedirse en fecha 25 de septiembre de 2019, un duplicado de la tarjeta SIM de la línea ******TELEFONO.1***, a favor

de una tercera persona distinta a la titular de la línea -la parte RECLAMANTE UNO-.

Estos hechos fueron denunciados ante Dirección General de la Policía Nacional en las dependencias de Granada Centro, en fecha 26 de septiembre de 2019, con número de atestado ***XXXX/XX,*** en la que la parte RECLAMANTE UNO manifestó lo siguiente:

"(…) Que el compareciente en el día de ayer sobre las 18:30 horas se percató que su teléfono móvil de la compañía Yoigo y con numero de terminal ******TELEFONO.1*** *se encontraba fuera de servicio, por lo que se puso en contacto con Atención al Cliente de dicha compañía, la cual le informó que posiblemente hubiera tenido un problema con la tarjeta SIM.*

--Que en el día de hoy se ha personado en su entidad bancaria Bankia para realizar unos pagos, indicándole el empleado que en la cuenta corriente de su hija, llamada ***A.A.A.*** *con mismo domicilio y teléfono de contacto que el compareciente se hallaba con tal solo 5,60 euros.*

--Que como quiera que el denunciante estaba seguro que en dicha cuenta había más dinero, es por lo que los empleados de Bankia han comprobado que persona/s desconocidas han accedido a la banca online del teléfono móvil del compareciente y han sacado 1300 euros de la tarjeta del denunciante la han traspasado a su cuenta corriente de la entidad Bankia y a continuación le han efectuado un reintegro de 1000 euros por el procedimiento Carg.Pag amigos a la persona de ***B.B.B.*** *y un reintegro de 150 euros de un cajero automático, del cual no puede aportar datos.*

--Que han intentado realizar otro reintegro en cajero si bien se ha bloqueado la operación.

--Que el denunciante es persona autorizada en la cuenta corriente de su hija ***A.A.A.****, por lo que a través de su teléfono móvil han accedido a la cuenta de su hija y han realizado tres transferencias inmediatas por un importe de 2000 euros, 800 euros y 100 euros, siendo la destinataria* ***C.C.C.***

--Que toda ésta información se la ha indicado el empleado de Bankia, ya que tanto el denunciante como su hija en ningún momento han tenido conocimiento de lo ocurrido y menos aún han autorizado las operaciones indicadas. (…)"

En la segunda de las denuncias con número de atestado ***YYYY/YY,*** de fecha 26 de septiembre de 2019, manifiesta:

"(…) *EI día veintiséis de los corrientes, el dicente formuló denuncia en estas dependencias con número* ***XXXX/XX****, en la que daba cuenta de la extracción fraudulenta en su cuenta bancaria y en la cuenta bancaria de su hija, (****A.A.A.****), por la cantidad total de 4050 euros, hecho ocurrido en la fecha y lugar indicado.*

--Compareciendo nuevamente para comunicar, que tras realizar gestiones

con la compañía telefó nica de Yoigo, ha sido informado que los presuntos autores de los hechos narrados realizaron un duplicado de tarjeta SIM, con el número de teléfono del denunciante, en la oficina de Yoigo, sito en Castellón de la Plana, avenida de la Virgen del Lidón, número 19, con número de duplicidad: (ICC) ******NÚMERO.1.***

--Queriendo hacer constar el compareciente, que entiende que la empresa Yoigo ha facilitado sus datos personales, en este caso a la persona denunciada, así como, ha facilitado una duplicidad de su tarjeta telefónica, por lo que está completamente convencido que también ha sido víctima de un ilícito penal por parte de dicha compañía telefónica, al facilitar sus datos personales libremente. (…)"

Asimismo aporta justificantes bancarios en las que figuran las siguientes transacciones realizadas:

- Transferencia inmediata desde la cuenta ******CUENTA.1***, de fecha 25 de septiembre de 2019 las 19:24 hs, por importe de 2000'00 euros a favor de ***C.C.C.***

- Transferencia inmediata desde la cuenta ******CUENTA.1***, de fecha 25 de septiembre de 2019 las 19:32 hs, por importe de 800'00 euros a favor de ***C.C.C.***

- Transferencia inmediata desde la cuenta ******CUENTA.1***, de fecha 25 de septiembre de 2019 las 21:29 hs, por importe de 100'00 euros a favor de ***C.C.C.***

- Transferencia desde la cuenta ******CUENTA.2***, de fecha 25 de septiembre de 2019 las 19:07 hs, por importe de 1000'00 euros a favor de ***B.B.B.***

- Reintegro en cajero automático desde la cuenta ******CUENTA.2***, de fecha 25 de septiembre de 2019 las 19:19 hs, por importe de 150'00 euros.

En relación con esta reclamación, XFERA afirmó en su respuesta de fecha 3 de julio 2020, a requerimiento de esta Agencia, que su departamento de fraude veía indicios de que la documentación presentada (denuncia y DNI adjunto) junto con la solicitud de duplicado de tarjeta SIM de fecha 25 de septiembre de 2019 estaba falsificado.

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA afirma que los delincuentes lograron engañar al personal de una tienda de la marca Yoigo mediante la entrega de documentación falsa, y en concreto, de un DNI y una denuncia de hurto manipulados mediante programas informáticos de tratamiento de imágenes.

CUARTO: Con fecha 5 de noviembre de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte RECLAMANTE DOS (expediente con núm. de referencia ***E/11591/2019***), dirigida contra XFERA, tras expedirse en fecha 10 de julio de 2019, un duplicado de la tarjeta SIM de la línea ******TELEFONO.2***, a favor de una tercera persona distinta a la titular de la línea -la parte RECLAMANTE DOS-.

Estos hechos fueron denunciados ante Dirección General de la Policía Nacional en las dependencias de Móstoles, en fecha 11 de julio de 2019, con número de atestado ***SSSSS/SS,*** en la que la parte RECLAMANTE DOS manifestó lo siguiente:

"Que el denunciante manifiesta que ha observado en su número de cuenta ******CUENTA.3*** *de la entidad ING dos cargos que él no ha realizado ni autorizado.*

Que los movimientos han sido realizados con la tarjeta con número ******CUENTA.4***

la cual está asociada a la cuenta arriba referida, siendo los movimientos los siguientes:

El día 10/07/2019, disposición en cajero número ******NÚMERO.2****, por un valor de 1700 euros.*

El día 10/07/2019, disposición en cajero número ******NÚMERO.2****, por un valor de 2000 euros.*

Que asimismo se ha personado en la entidad bancaria con el fin de recoger el justificante bancario, el cual aporta a esta instrucción y es adjuntado a las presentes.

Que el dicente refiere que nunca ha perdido su tarjeta bancaria, manifestando que nunca ha realizado compras en este establecimiento."

En la segunda de las denuncias con número de atestado ***RRRRR/RR,*** de fecha 29 de julio de 2019, manifiesta:

"Que las presentes son ampliatorias del atestado número ***SSSSS/SS*** *de estas dependencias.*

Que el diciente manifiesta que recibió una llamada el día 26/07/2019 a lo 'largo de este día sin concretar exactamente la hora. (…)

Que la llamada supuestamente la realizó el caporal número ******NÚMERO.3*** *de los Mossos d'Esquadra, responsable de hurtos y estafas.(…)*

Que dicho interlocutor le preguntó al denunciante que le confirmarse la titularidad del número de teléfono del que él era abonado dado que figuraba tras una serie de investigaciones que sobre estafas con tarjetas bancarias estaba realizando, que el suyo aparecía en un listado de morosos. (…)

Que su interlocutor seguidamente le solicitó la remisión de la denuncia que interpuso, para poder incluirla a las investigaciones que estaban llevando a cabo por su unidad policial (…)

Que en dicha conversación telefónica aquel agente policial le aseguró que su teléfono móvil a través de las tiendas de la compañía "MASMOVIL" habría sido el lugar desde el cual en algún momento dado se habría producido el duplicado de su tarjeta, hecho este que al respecto el denunciante recordaría que días previos a la materialización de los cargos fraudulentos en su cuenta y por lo que interpuso con posterioridad denuncia, se percató que por breve espacio de tiempo su teléfono móvil se quedó sin línea e inutilizable, debiendo por ello cambiar su tarjeta SIM. (…)"

Asimismo aporta justificantes bancarios en las que figuran las siguientes transacciones realizadas:

- Habilitar puesto para la elección de clave de seguridad para el cliente ***D.D.D.***, con NIF ******NIF.1***, de fecha 11 de julio de 2019 las 10:08:37 hs, en la Oficina de Móstoles del Banco ***ING***.

- Reintegro en cajero automático desde la cuenta ******CUENTA.3***, de fecha 10 de julio de 2019, por importe de 1700 euros.

- Reintegro en cajero automático desde la cuenta ******CUENTA.3***, de fecha 10 de julio de 2019, por importe de 2000 euros.

En relación con esta reclamación, XFERA afirmó en su respuesta de fecha 9 de octubre de 2020, a requerimiento de esta Agencia, que el canal por el que se activó esta SIM fue el telefónico y aporta la oportuna grabación como Documento nº 19. Escuchada la grabación, se verifica que el operador pregunta el número de línea y el propio operador le dice el nombre y le pregunta si es él. No le pide el número de DNI tampoco.

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA afirma que todo indica que el suplantador se hizo con una tarjeta SIM "en blanco", probablemente tras obtenerla ilícitamente de una tienda o de un técnico instalador de Masmóvil. Así se desprende del contenido de la llamada, en la que se comprueba que el solicitante contaba con el ICCID completo de la tarjeta SIM que únicamente figura impreso en el dorso de la propia tarjeta.

QUINTO: para la marca Yoigo, en su respuesta de fecha 30 de enero de 2020, XFERA indica que su procedimiento de solicitud de duplicado SIM era el siguiente:

- Canal presencial: (…)

- Canal no presencial: (…)

En el documento nº 6 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta el procedimiento de YOIGO para solicitar un duplicado de Tarjeta SIM, en el que consta lo siguiente:

(…)

En el documento nº 4 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta los casos en que debe pasarse la política de seguridad de todas las empresas del Grupo MASMOVIL para el duplicado de las Tarjetas SIM, en el que consta que ésta debe pasarse, entre otros supuestos, (…)".

En el documento nº 1 que acompaña su escrito de respuesta de fecha 3 de julio de 2020, XFERA adjunta la política de seguridad de YOIGO, en el que consta que (…), entre otros. En este documento, consta que esta política consiste en solicitar del titular de la línea: *(…).*

En el documento nº2 que acompaña su escrito de respuesta de fecha 3 de julio de 2020, XFERA adjunta las instrucciones para solicitar un duplicado de tarjeta SIM, en las que se indica que (…). Y que para pedir un duplicado de Sim (…).

SEXTO: para la marca MásMóvil, en su respuesta de fecha 30 de enero de 2020, XFERA indica que su procedimiento de solicitud de duplicado SIM era el siguiente:

- Canal presencial: (…)

- Canal no presencial: (…) En el caso de que la solicitud tuviera como origen el robo del terminal o de la tarjeta SIM, (…).

En el documento nº 5 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta el procedimiento de MásMóvil para solicitar un duplicado de Tarjeta SIM, en el que consta lo siguiente: *"En primer lugar, recuerda que tendrás que pasar política de seguridad".* Y a continuación se describen los pasos a seguir: (…).

En el documento nº 4 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta los casos en que debe pasarse la política de seguridad de todas las empresas del Grupo MASMOVIL para el duplicado de las Tarjetas SIM, en

el que consta que ésta debe pasarse, entre otros supuestos, (…).

En el documento nº 5 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta el procedimiento para duplicado SIM de la marca MasMóvil, en el que se indica que (…).

En el documento nº 6 que acompaña su escrito de respuesta de fecha 3 de julio de 2020, XFERA adjunta el procedimiento de MásMóvil para la solicitud de duplicados de tarjetas SIM. En este documento se indica que desde el 22 de junio de 2020 se reactiva la (…). Y que "el procedimiento para solicitarlo no cambia: pasa política de seguridad y haz la petición por MYSIM como siempre". Para solicitar la SIM, se indica que "se puede solicitar en una tienda o por llamada". Y que "para solicitar el duplicado debemos pasar la Política de seguridad".

En el documento nº 7 que acompaña su escrito de respuesta de fecha 3 de julio de 2020, XFERA adjunta copia de la política de seguridad de MásMóvil. En este documento se indica que "La política de seguridad son las preguntas que haremos al titular o usuario de una línea para hacer cualquier gestión:

(…)

Entre los casos en los que se debe pasar política de seguridad, se menciona (…).

En el documento nº 8 que acompaña su escrito de respuesta de fecha 3 de julio 2020, XFERA adjunta el procedimiento de activación de ICC para MásMóvil (en pruebas en ese momento). En este documento se indica (…). Y consta como política de seguridad:

(…)

SÉPTIMO: para la marca Llamaya, en su respuesta de fecha 30 de enero de 2020, XFERA indica que su procedimiento de solicitud de duplicado SIM era el siguiente:

- Canal presencial: (…)

- Canal no presencial: (…)

En el documento nº 4 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta los casos en que debe pasarse la política de seguridad de todas las empresas del Grupo MASMOVIL para el duplicado de las Tarjetas SIM, en el que consta que (…).

En su escrito de fecha 3 de julio de 2020, XFERA manifestó que (…).

En el documento nº 4 que acompaña su escrito de respuesta de fecha 3 de julio 2020, XFERA adjunta la política de seguridad para la marca Llamaya. En este documento se indica que

(…)

Entre los casos en los que se debe pasar política de seguridad, se menciona (…).

En el documento nº 5 que acompaña su escrito de respuesta de fecha 3 de julio 2020, XFERA adjunta el procedimiento de activación y solicitud de duplicados de tarjeta SIM de Llamaya, en el que consta que (…).

OCTAVO: para la marca Lebara, en su respuesta de fecha 30 de enero de 2020, XFERA indica que su procedimiento de solicitud de duplicado SIM era el siguiente:

- Canal presencial: (…)

- Canal no presencial: (…)

Igual que ocurre con el resto de las marcas (…).

En el documento nº 4 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta los casos en que debe pasarse la política de seguridad de todas las empresas del Grupo MASMOVIL para el duplicado de las Tarjetas SIM, en el que consta que ésta debe pasarse, entre otros supuestos (…).

En el documento nº 3 que acompaña su escrito de respuesta de fecha 3 de julio 2020, XFERA adjunta el procedimiento de solicitud de duplicado de la tarjeta SIM para la marca Lebara- canal no presencial. En este documento se indica (…).

En cuanto a la política de seguridad, el documento en cuestión indica que (…) cuando ya tiene la tarjeta.

Debe pasar la política de seguridad en dos niveles.

(…)

NOVENO: En el documento nº 3 que acompaña su escrito de respuesta de fecha 30 de enero de 2020, XFERA adjunta captura de pantalla de una comunicación interna MASMOVIL desde Atención al cliente en la que se indica "Recientemente se están detectando prácticas incorrectas por parte de los agentes a la hora de identificar clientes y aplicar la política de seguridad. Se ha publicado en ***HERRAMIENTA.1 un recordatorio del proceso y he enviado a todas las agencias para que sean conscientes de la importancia del tema. (…)".

También se adjunta capturas de pantalla desde Atención al Cliente (…) en las que se indica "Ayer publicamos una información de absoluta relevancia en ***HERRAMIENTA.1 acerca del proceso que deben seguir los agentes para hacer una correcta identificación de los clientes. Seguir este proceso es crucial para detectar fraude y garantizar un uso adecuado de los datos privados (como por ejemplo usuarios y contraseñas para acceso a sus áreas privadas), quedando terminantemente prohibido solicitar estos datos directamente al cliente. (…)".

DÉCIMO: En cuanto al envío de tarjeta SIM por correo, en su escrito de respuesta de fecha 30 de enero, a requerimiento de esta Agencia, XFERA manifestó que, con carácter general, en el momento de la solicitud de un duplicado de Tarjeta SIM y que se proceda al envío de la misma mediante un sistema de mensajería a través del Servicio de Atención al cliente, el cliente debe aceptar la política de seguridad.

La entrega del duplicado de la tarjeta SIM se realiza a través del servicio ***SERVICIO.1", (…). Se adjunta como documento 2 de este escrito dos ejemplos de albaranes de entrega en los que se refleja que "El/la que suscribe declara que el envío reseñado ha sido debidamente: Entregado" y debajo figura nombre y apellidos de una persona (que coincide con el destinatario del envío) y un DNI/PASAPORTE/NIE, junto con una firma.

(…)

En su escrito de respuesta de 3 de julio de 2020, a requerimiento de esta Agencia, XFERA manifestó que la casuística por la que un cliente puede solicitar el envío de un duplicado de la SIM a una dirección distinta es variada: (…).

En el documento nº 9 que acompaña este escrito se adjunta copia del contrato de colaboración mercantil entre XFERA y la ***EMPRESA.1, de fecha 5 de octubre de

2018, cuyo objeto es designar a ***EMPRESA.1 como “colaborador para la entrega, en nombre y por cuenta de Masmovil, de tarjetas SIM sin activar a clientes de Masmovil”.

En la cláusula séptima de este contrato se indica que “En el caso de que con el fin de poder prestar a MASMOVIL los Servicios, ***EMPRESA.1 deba tratar datos de carácter personal cuyo responsable sea MASMOVIL, ***EMPRESA.1 actuará en nombre y por cuenta de éste, asumiendo la consideración de encargado del tratamiento, todo ello en cumplimiento del artículo 28 del RGPD y demás normativa que resulte aplicable, así como de conformidad con lo dispuesto en el Contrato de Encargo de Tratamiento que se adjunta al presente Contrato, como Anexo 1, como parte inseparable del mismo”.

En la documentación aportada no se proporciona detalle alguno sobre el servicio que presta ***EMPRESA.1 respecto a la debida identificación de los titulares de las líneas objeto de duplicado SIM para la entrega de las tarjetas en cuestión.

UNDÉCIMO: Respecto a si la realización de los controles para la verificación de la identidad del solicitante del duplicado de la tarjeta SIM queda reflejada, para cada solicitud atendida, en el Sistema de Información de la entidad, en su escrito de respuesta de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA manifestó que las actuaciones más relevantes durante el año 2019 para asegurar los derechos de los clientes han sido por cada marca:

-.Yoigo: en julio 2019, se comienza a custodiar además de copia física del contrato de duplicado de SIM, copia digital del contrato más copia de DNI en su gestor documental.

-. Masmovil/Llamaya: desde principios de 2019 se comienza a generar un contrato de cambio de SIM, junto con dicho contrato se establece como necesario la recogida de una copia del DNI o documento acreditativo de la personalidad.

-. Pepephone: en julio 2019 se comienza a generar y custodiar la documentación que acredite el cambio de SIM.

Se adjunta como Documento 3 un ejemplo de grabación de solicitud de duplicado de SIM de MASMOVIL. En esta grabación el agente solicita el número de teléfono de la línea en cuestión y para confirmar que se trata del titular se pide nombre completo y DNI. A continuación se pregunta si fue a ***EMPRESA.1 a buscar la nueva tarjeta SIM o a una tienda. Y le pregunta los cuatro últimos números “de un número super largo” que figura en la tarjeta debajo del código de barra. Los datos no coinciden en un primer momento, pero el agente finalmente encuentra la tarjeta asociada a ese número y, para confirmar los datos, le dice el número completo del código ICC a la persona que llama por teléfono.

DUODÉCIMO: En cuanto a los motivos por los cuales ha sido posible en algunos casos la suplantación de la identidad de clientes para la emisión de duplicados de SIM, en su escrito de respuesta de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA ha manifestado que:

- para el canal presencial: se ha podido producir por presentación de documentación falsificada (DNI y/o denuncia por pérdida o robo de documentación y teléfono) y por error humano; y

- para el canal telefónico: se ha podido producir por error humano del teleoperador o del personal del servicio de entrega, por uso de documentación falsificada en la

entrega y por conocimiento de todos los datos personales de cliente.

DÉCIMO TERCERO: Respecto a las acciones emprendidas cuando se detecta uno de estos casos, en su escrito de respuesta de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA ha manifestado que se sigue el siguiente procedimiento que ha sido distribuido entre los equipos de Atención al Cliente:

- "Desde riesgo, cuando localicen un fraude, informarán al cliente de que tiene que ir a un distribuidor a por una nueva tarjeta SIM. Ellos dejarán la línea con un bloqueo y además abrirán un ticket en ***APLICACION.1 de suplantación de identidad para vosotros podáis hacer el seguimiento.

- Vosotros tendréis que ir haciendo filtros a lo largo del día (No deberían entrar más de 2-3 casos al día) e intentar poneros en contacto con el titular, para confirmar que ha adquirido la nueva tarjeta SIM (…)

- (…)

DÉCIMO CUARTO: En cuanto a las acciones emprendidas para evitar que casos de este tipo se vuelvan a producir, en su escrito de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA ha manifestado que en septiembre 2019 se comenzó a diseñar unas nuevas reglas en la herramienta de monitorización de tráfico fraudulento para la detección de posibles duplicados fraudulentos, en dichas reglas se analizan (…).

Durante el mes de noviembre de 2019 la herramienta fue configurada y se estuvo validando el funcionamiento además de realizar una vigilancia activa en horario de oficina.

El 28 de noviembre de 2019 se abrió el servicio (…). Se adjunta como documento 10 el manual de procedimiento correspondiente. En el apartado "Cambio SIM MasMóvil", se indica que (…). En caso de no identificar coherencia en el uso de la línea se procederá a contactar con el cliente para indicarle que por motivos de seguridad se necesita confirmar si ha realizado un cambio de SIM (…) en las últimas horas. Si el análisis de los eventos o el contacto con el cliente confirman el cambio de SIM correcto se vuelve a activar la recepción de SMS en Mysim y se cierra el ticket de posible fraude.

Se destacan una serie de rasgos identificativos que podrán ayudar a identificar aquellos casos donde hay un posible cambio de SIM fraudulento:

- (…)

En el apartado "Cambio SIM Yoigo", se indica que cuando se active un alerta de posible fraude (…).

(…) "se procederá a contactar con el cliente para indicarle que por motivos de seguridad se necesita confirmar si ha realizado un cambio de SIM en tienda en las últimas horas".

Si el análisis de los eventos es correcto y no existen indicios de fraude, se anotarán el análisis realizado y se cierra la alerta.

Si se identifican indicios de posible fraude, se abre ***APLICACION.1 con el caso identificado.

Se destaca que existen una serie de rasgos identificativos que podrán ayudar a identificar aquellos casos donde hay un posible cambio de SIM fraudulento y se de-

tallan los mismos supuestos enumerados en el apartado de Yoigo, reseñado anteriormente.

En cuanto a la gestión de la llamada de confirmación de duplicado de SIM, se detalla el siguiente guion:

(…)

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA manifiesta que no tenía conocimiento de la operativa criminal conocida como “SIM swapping” hasta que recibe un requerimiento de la Subdirección General de Atención al Usuario de Telecomunicaciones, de la Secretaría de Estado para el Avance Digital (SEAD), de fecha 25 de septiembre de 2019, que se aporta como Documento 2 y que comienza:

“En esta Subdirección General se han recibido consultas y reclamaciones acerca de un fraude con la siguiente operativa: con carácter previo se obtienen ciertos datos personales de un usuario (como el DNI, o número de cuenta corriente). Partiendo de esos datos, quien tiene la intención de cometer el fraude solicita al operador, con los datos personales previamente obtenidos, un duplicado de la tarjeta SIM. A partir de ahí, una vez conseguido, se pueden realizar transacciones financieras accediendo a los servicios financieros por Internet, dado que estos incluyen como mecanismo de seguridad, la consecución de una clave que es enviada al teléfono móvil (a la que se accedería mediante el duplicado de la tarjeta SIM)”.

También en su escrito de alegaciones de fecha 3 de marzo de 2021, XFERA proporcionó más detalles respecto al sistema automático de detección de fraude que ha implantado, que consiste en una herramienta informática denominada “***HERRAMIENTA.2” y que se trata de un sistema de filtrado que se aplica (…). En caso de que una solicitud sea detectada como potencialmente fraudulenta, el sistema lanza una alarma, a efectos de que un técnico pueda revisar si el caso es efectivamente fraudulento y aplicar el protocolo pertinente. El sistema se activa en función de factores como los siguientes:

(…)

También se explica que se ha implantado una revisión aleatoria de aquellas solicitudes de duplicado de tarjeta no detectadas como sospechosas por el sistema “***HERRAMIENTA.2”. Esta revisión se realiza por las noches, por parte del departamento de control de servicio, y tiene en cuenta factores como los siguientes:

(…)

La principal acción, en caso de sospecha, es el inmediato bloqueo en el envío y recepción de mensajes SMS; además de tratar de contactar con el titular de la línea para verificar que, efectivamente, ha solicitado un duplicado de su tarjeta SIM.

En cuanto a la eficacia de las medidas, se aportan las estadísticas de 2020:

Concepto	**Cantidad**	**Porcentaje**
Duplicados de tarjeta SIM realizados	***CANTIDAD.1	***PORCENTAJE.1
Intentos de activación potencialmente fraudulentos detectados	***CANTIDAD.2	***PORCENTAJE.2

Intentos fraudulentos que superaron la política de seguridad (1ª capa)	***CANTIDAD.3	***PORCENTAJE.3
Intentos fraudulentos que superaron la ***HERRAMIENTA.2 (2ª capa)	***CANTIDAD.4	***PORCENTAJE.4
Intentos fraudulentos que superaron la revisión aleatoria (3ª capa)	***CANTIDAD.5	***PORCENTAJE.5

XFERA manifiesta que la implementación de estas medidas sumó una eficacia acumulada del ***PORCENTAJE.9; y supuso una reducción efectiva del ***PORCENTAJE.10 en los casos en los que los delincuentes lograron sus ilícitos objetivos. Se aporta, como Documento 6, una tabla con los ***CANTIDAD.3 casos que superaron la primera barrera.

DÉCIMO QUINTO: En cuanto al número de casos de solicitudes fraudulentas de duplicados de SIM detectados durante todo el año 2019, en su respuesta de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA manifestó que se detectaron ***CANTIDAD.7 casos en total, (…).

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA manifestó que (…) casos detectados anualmente en 2019 fueron test de intrusión realizados por el personal de seguridad de la empresa, con datos ficticios, a efectos de evaluar la robustez de los procedimientos entonces existentes. Por lo que dicha cifra debe reducirse en (…) casos menos.

También se indica en este escrito de alegaciones que en 2020 la cifra de casos se redujo a ***CANTIDAD.5.

DÉCIMO SEXTO: En cuanto al número de clientes de telefonía móvil total, en su respuesta de fecha 30 de enero de 2020, a requerimiento de esta Agencia, XFERA manifestó que tenía 4.739.191 clientes postpago y 1.758.708 cliente prepago.

DÉCIMO SÉPTIMO: En su escrito de fecha 3 de julio de 2020, a requerimiento de esta Agencia, XFERA aporta un listado con “los 20 primeros casos de solicitud de duplicado de SIM de forma fraudulenta confirmados” desde el 1 de enero de 2020. De esta lista, solo dos de los casos han sido reclamados o denunciados directamente por el cliente. El resto de casos se iniciaron a consecuencia de un alerta generada por la herramienta de XFERA para detectar, entre otras cosas, solicitudes de duplicados de tarjeta SIM fraudulentos mediante la detección de patrones (herramienta descrita en el hecho probado décimo catorce). La tabla facilitada era la siguiente:

FECHA	MSISDN	MARCA	CANAL
05/01/2020	***TELEFONO.3***	MásMóvil	Telefónico
14/01/2020	***TELEFONO.4***	Yoigo	Tienda
15/01/2020	***TELEFONO.5***	MásMovil	Telefónico
20/01/2020	***TELEFONO.6***	MásMóvil	Telefónico
25/01/2020	***TELEFONO.7***	Yoigo	Telefónico
27/01/2020	***TELEFONO.8***	MásMóvil	Telefónico
27/01/2020	***TELEFONO.9***	Yoigo	Tienda
28/01/2020	***TELEFONO.10***	Yoigo	Tienda

04/02/2020	***TELEFONO.11***	Yoigo	Telefónico
25/02/2020	***TELEFONO.12***	Yoigo	Telefónico
27/02/2020	***TELEFONO.13***	Yoigo	Telefónico
29/02/2020	***TELEFONO.14***	Yoigo	Telefónico
03/03/2020	***TELEFONO.14***	Yoigo	Telefónico
05/03/2020	***TELEFONO.15***	Yoigo	Telefónico
05/03/2020	***TELEFONO.11***	Yoigo	Telefónico
11/03/2020	***TELEFONO.16***	Yoigo	Tienda
13/03/2020	***TELEFONO.17***	Yoigo	Telefónico
03/04/2020	***TELEFONO.18***	MásMóvil	Telefónico
04/04/2020	***TELEFONO.19***	MásMóvil	Telefónico
08/04/2020	***TELEFONO.20***	Yoigo	Tienda
12/04/2020	***TELEFONO.21***	Yoigo	Telefónico

En su escrito de fecha 9 de octubre de 2020, a requerimiento de esta Agencia, XFERA aporta como Documentos 1 a 8 duplicados y copias del DNI aportados en las solicitudes realizadas en tienda de la lista en cuestión. Se aclara que en relación con el ***TELEFONO.20*** no ha sido posible localizar la documentación debido a que está relacionado con un posible robo de credenciales. En este caso, la tienda en la que consta que se ha solicitado el duplicado afirma que el mismo no se ha tramitado en su tienda.

Esta suplantación se realizó durante el estado de alarma, lo cual dificulta su investigación y no se tiene certeza sobre la afirmación de la tienda.

De la documentación aportada, se verifica que:

- De tres de los casos se aporta copia del DNI del solicitante y documento de cambio de SIM.

- De un caso aportan copia de un documento de identidad de la República Italiana. En el documento de cambio de SIM consta que se ha aportado un NIF y como número de DNI/NIF el número de documento identificativo italiano, lo cual no es correcto.

- Se observa que en dos de los casos los DNI tienen algunos datos iguales, cambiando los nombres (mismo CAN (Card Identity Number), fecha de expedición, nombres de padres y la misma firma manuscrita).

En este mismo escrito, XFERA aporta, para los casos de solicitud telefónica, como Documentos nº 9 a 18 copia de las grabaciones de las conversaciones donde el solicitante del SIM supera la política de seguridad y copia de las grabaciones de las conversaciones donde el solicitante de la activación del SIM supera la política de seguridad.

Se aclara que no ha sido posible localizar algunas de las llamadas, posiblemente por errores en la codificación (nomenclatura) de las mismas, lo cual dificulta su localización, dado que cuando las llamadas a control de servicio o atención al cliente se realizan desde la línea de referencia se guardan automáticamente en los sistemas, pero cuando se realizan desde una numeración distinta, como en los casos de activación de duplicados, los agentes deben introducir la nomenclatura manualmente, lo cual es susceptible de errores en la codificación.

De las escuchas de las diez llamadas aportadas, todas referidas a la activación de la tarjeta, ya en poder del solicitante, que suele mencionar que la ha recibido por mensajería, se verifica lo siguiente:

- Caso 1: (…). El operador pregunta número de línea. El solicitante pregunta también por número de cuenta bancaria, menciona que empieza por cuatro determinados dígitos y la operadora contesta afirmativamente.

- Caso 2: (…) pregunta número de línea. La operadora menciona que la tarjeta se suele mandar activada.

- Caso 3: El operador pregunta (…).

- Caso 4: El operador pregunta (…).

- Caso 5: El operador pregunta (…).

- Caso 6: El solicitante dice (…).

- Caso 7: Pregunta número de línea. En ningún momento le pide DNI ni nombre. El operador llama por su nombre de pila al solicitante. El operador le dice el PIN nuevo de la tarjeta sin preguntarlo el solicitante.

- Caso 8: Pregunta (…).

- Caso 9: Pregunta (…). El solicitante pregunta por importe de factura de 51,33 euros y dirección postal a la que fue enviada. El operador le indica la dirección de envío de la factura.

- Caso 10: Pregunta (…).

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA indica que uno de los casos de este listado, el relativo a la línea ******TELEFONO.4***, está siendo investigado por la vía pena por el Juzgado de Instrucción nº. 9 de Alicante, en el marco de las diligencias previas ÑÑÑÑÑ/ÑÑÑÑ. Se acompaña, como Documento 1, oficio del citado juzgado de fecha 23 de enero de 2021, dirigido a XFERA, en el que se le solicita que facilite "el número de IMEI de los terminales móviles donde se ha utilizado la tarjeta SIM asociada al número ******TELEFONO.4***".

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA aporta como Documentos 7, 8, 9, 10 las grabaciones de las cinco llamadas que no habían sido localizadas anteriormente debido a un error en la codificación (esto es cuando la llamada es realizada desde una línea diferente a aquella sobre la que versa la consulta, y el operador no hace constar esta circunstancia manualmente en los sistemas de atención al cliente de la empresa).

En el Documento 7, se aporta grabación correspondiente a la línea ******TELEFONO.3*** de fecha 5 de enero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona (…), pero sólo recuerda de memoria los tres últimos dígitos del número de línea. El agente le indica el número completo de la línea de teléfono. Y el solicitante le dicta el número que aparece en la tarjeta SIM nueva.

En el Documento 8, se aporta grabación correspondiente a la línea ******TELEFONO.6*** de fecha 20 de enero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona (…). También el solicitante le indica el número ICC de la tarjeta SIM.

En el Documento 9, se aporta grabación correspondiente a la línea ******TELEFONO.22*** de fecha 27 de enero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona (…). La operadora duda porque el envío del duplicado de la tarjeta no consta en el sistema y consulta con una compañera. Ésta le dice que le pida el ICC de la tarjeta SIM antigua. La operadora le pide el ICC

de la tarjeta SIM antigua, pero el solicitante dice que perdió la tarjeta anterior. Y la operadora le indica que debe acudir a una tienda. El solicitante afirma que no puede acudir a una tienda. La operadora consulta a su coordinador y este le indica que puede activar la tarjeta si ha pasado la política de seguridad y tiene el número ICC de la tarjeta nueva.

En el Documento 10, se aporta grabación correspondiente a la línea ******TELEFONO.12*** de fecha 25 de febrero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona (…). La operadora duda porque el envío del duplicado de la tarjeta no consta en el sistema. Es ella la que le facilita el número completo de la línea. Tras ser preguntado, el solicitante facilita también el código ICC de la tarjeta que supuestamente recibió de ***EMPRESA.1, que no coincide con lo que figura en el sistema. Luego de realizar unas consultas, la operadora le pide confirmar los apellidos del titular, que el solicitante facilita correctamente. Y le pide nuevamente el código ICC, tras lo cual se le tramita la activación de la SIM.

En el Documento 11, se aporta grabación correspondiente a la línea ******TELEFONO.18*** de fecha 3 de abril de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona (…).

En su escrito de alegaciones de fecha 8 de marzo de 2021, XFERA reproduce una tabla donde figuran nuevamente las veinte reclamaciones aportadas en su momento a la Agencia, pero incorporando la fecha y hora en que se recibió la solicitud ilícita y el momento de bloqueo de la tarjeta SIM. Se destaca que tres de los números están repetidos porque la operativa fraudulenta fue interceptada en dos ocasiones por el sistema de seguridad.

MSISDN	MARCA	CANAL	Solicitud	Bloqueo
******TELEFONO.3***	MásMóvil	Telefónico	05/01/2020 22:12	05/01/2020 22:24
******TELEFONO.4***	Yoigo	Tienda	14/01/2020 20:18	15/01/2020 21:43
******TELEFONO.5***	MásMovil	Telefónico	15/01/2020 12:43	15/01/2020 13:20
******TELEFONO.6***	MásMóvil	Telefónico	20/01/2020 21:01	20/01/2020 22:51
******TELEFONO.7***	Yoigo	Telefónico	25/01/2020 16:48	25/01/2020 17:50
******TELEFONO.8***	MásMóvil	Telefónico	27/01/2020 14:20	27/01/2020 17:50
******TELEFONO.9***	Yoigo	Tienda	27/01/2020 17:07	27/01/2020 17:28
******TELEFONO.9***	Yoigo	Tienda	27/01/2020 19:56	27/01/2020 21:50
******TELEFONO.10***	Yoigo	Tienda	28/01/2020 12:29	28/01/2020 12:59
******TELEFONO.11***	Yoigo	Telefónico	04/02/2020 16:08	04/02/2020 16:26
******TELEFONO.12***	Yoigo	Telefónico	25/02/2020 23:05	25/02/2020 23:12
******TELEFONO.13***	Yoigo	Telefónico	27/02/2020 18:31	27/02/2020 19:19
******TELEFONO.14***	Yoigo	Telefónico	29/02/2020 21:38	29/02/2020 21:51
******TELEFONO.14***	Yoigo	Telefónico	03/03/2020 7:37	03/03/2020 7:48

TELE-FONO.15	Yoigo	Telefó-nico	05/03/2020 17:07	05/03/2020 22:23
TELE-FONO.11	Yoigo	Telefó-nico	05/03/2020 21:07	05/03/2020 21:37
TELE-FONO.16	Yoigo	Tienda	11/03/2020 13:59	11/03/2020 14:42
TELE-FONO.17	Yoigo	Telefó-nico	13/03/2020 12:51	13/03/2020 13:24
TELE-FONO.18	MásMóvil	Telefó-nico	03/04/2020 15:11	03/04/2020 15:22
TELE-FONO.19	MásMóvil	Telefó-nico	04/04/2020 13:45	04/04/2020 14:04
TELE-FONO.20	Yoigo	Tienda	08/04/2020 21:03	08/04/2020 22:04
TELE-FONO.21	Yoigo	Telefó-nico	12/04/2020 15:39	12/04/2020 15:54

En 10 sobre los 22 listados anteriormente, el sistema ***HERRAMIENTA.2 detectó el posible fraude y el personal de XFERA logró contactar con el titular de la línea, bloqueando la tarjeta duplicada antes de que los delincuentes lograsen su objetivo, hasta donde se sabe: ***TELEFONO.3, ***TELEFONO.7, ***TELEFONO.9** (en dos ocasiones), ***TELEFONO.10, ***TELEFONO.13, ***TELEFONO.17, ***TELEFONO.18, ***TELEFONO.20, ***TELEFONO.21**. El tiempo medio de bloqueo, en los casos listados, fue de 40 minutos; y su mediana, de 31 minutos.

En un total de 9 sobre los 22 listados anteriormente, el sistema ***HERRAMIENTA.2 detectó el posible fraude y, a pesar de que el personal de XFERA no consiguió contactar con el titular de la línea, se bloqueó la posibilidad de recibir SMS en la tarjeta duplicada antes de que los delincuentes lograsen su objetivo, hasta donde se sabe: ***TELEFONO.5, ***TELEFONO.22, ***TELEFONO.11** (en dos ocasiones), ***TELEFONO.12, ***TELEFONO.14** (en dos ocasiones), ***TELEFONO.16, ***TELEFONO.19**. El tiempo promedio de bloqueo, en los casos listados, fue de 43 minutos; y su mediana, de 19 minutos.

En el caso del número ***TELEFONO.15**, el sistema de ***HERRAMIENTA.2 no detectó el posible fraude, pero sí lo hizo la auditoría de control de servicio de XFERA (tercera capa de seguridad), bloqueando la tarjeta duplicada. Resultó ser un "falso positivo": el cliente contactó con la empresa días más tarde, para solicitar su desbloqueo.

En dos casos, el sistema ***HERRAMIENTA.2 no detectó el fraude, y fueron los propios clientes los que contactaron con XFERA, tras detectar que su línea no funcionaba correctamente: ***TELEFONO.4, ***TELEFONO.6**.

De estos dos casos, es importante señalar que, en lo tocante al número de teléfono ***TELEFONO.4**, la suplantación de identidad se produjo en (…), y que el solicitante exhibió un DNI falso, cuya copia fue aportada al expediente.

DECIMO OCTAVO: En cuanto a la posibilidad de conseguir una SIM sin asociarla a una línea telefónica, en su escrito de fecha 9 de octubre de 2020, a requerimiento de esta Agencia, XFERA manifestó que sólo conoce dos casos:

1. Envío de tarjetas de reemplazo, que van sin activar y sin asociar a ninguna línea. Para evitar que se produzca fraude en la activación de estas SIMs se ha instaurado el procedimiento de (…).

2. Lotes de SIMs de (…). Estas SIMS no tienen por finalidad sustituir una SIM de un cliente activo, sino proporcionárselas a clientes que hayan solicitado una portabili-

dad en el momento de instalación.

El departamento de fraude de XFERA ha detectado que las SIMs cuya activación se ha solicitado de forma telefónica y han resultado ser suplantaciones, (…). Se desconoce las circunstancias en las que los "usurpadores" se hacen con estas SIMs.

DÉCIMO NOVENO: En cuanto a si se han detectado casos de duplicación de SIM fraudulentos en los que de forma previa se produzca un cambio de titularidad suplantando la identidad del antiguo titular, para, posteriormente realizar el nuevo titular el cambio de SIM, en su escrito de fecha 9 de octubre de 2020, XFERA manifestó que no les constaba ningún caso hasta el momento. Como documento nº 20 se adjunta la política de seguridad que se pasa al solicitante en los cambios de titularidad vía telefónica. En este documento se indica que :

"La política de seguridad son las preguntas que haremos al titular o usuario de una línea para hacer cualquier gestión:

(…)

También se indica que debe pasarse la política de seguridad, entre otros casos, en un "Cambio de titular".

En este documento también figura que para el cambio de titular para sólo móvil y convergencia, "El cliente debe enviar por mail a cambiotitular@masmovil.com, la siguiente documentación:

(…)

Se indica que (…).

Como documento nº 21 se adjunta el procedimiento de cambio de titularidad. En este documento se indica que "Para cambiar el titular de una línea, el titular actual y el nuevo tienen que ir juntos a una tienda (Yoigo o The Phone House dependiendo donde se diera de alta) y presentar la siguiente documentación (…)". En este documento se incluye también la política de seguridad en la que se indica que debe solicitarse (…).

VIGÉSIMO: En cuanto a si se proporcionaba información a los trabajadores sobre la comprobación de los elementos de seguridad de DNI y pasaporte, en su escrito de respuesta a la Propuesta de Resolución del presente procedimiento sancionador, XFERA aporta como Documento 1 una presentación con la marca "Yoigo", de fecha julio 2013, que lleva por título "Procedimiento de Identificación de documentación falsificada", en la que se da información sobre las herramientas utilizadas para la detección de documentación (…).

TERCERO: La parte recurrente ha presentado, en fecha 14 de diciembre de 2021, ante el Registro General de la AEPD, recurso potestativo de reposición en el que muestra su disconformidad con la resolución impugnada.

El recurso potestativo de reposición se considera interpuesto en plazo debido a una incidencia técnica producida en fecha 13 de diciembre de 2021, que imposibilitó el funcionamiento ordinario de la plataforma común del Sector Público Administrativo Estatal para la identificación y autenticación electrónicas, Clave.

XFERA invoca una serie de argumentos expuestos a continuación, a través de los cuales discrepa del contenido de la resolución y de las conclusiones alcanzadas:

PRIMERA. Vulneración del artículo 89.3 de la LPACAP: se alega, incumplimiento

del deber de motivación de las resoluciones previsto en el artículo 89.3 de la Ley 39/2015, y por extensión, del artículo 9.3 de la Constitución Española.

SEGUNDA. Vulneración del artículo 77 de la LPACAP: la Agencia insiste, en afirmar que se ha producido una quiebra en el principio de confidencialidad del dato, cuando no ha sido así; y no ha logrado incorporar al procedimiento ningún tipo de prueba para sostener esta afirmación, más allá de sus propias palabras.

TERCERA. Vulneración del artículo 8 de la Ley 40/2015: la competencia para sancionar ese tipo de conductas recae, exclusivamente, en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. Así lo recoge el artículo 84.1 de la LGTEL.

CUARTA. Vulneración del artículo 28 de la Ley 40/2015.

QUINTA. Vulneración del artículo 29 de la Ley 40/2015: XFERA ya había adoptado medidas, antes incluso de la apertura del procedimiento sancionador: bastó un requerimiento de la Secretaría de Estado para el Avance Digital para que realizase un nuevo análisis de riesgos e incrementase sus medidas de seguridad.

SEXTA. Subsidiariamente, solicitud de aplicación del artículo 29.4 de la Ley 40/2015: se solicita la aplicación del citado artículo reduciendo la sanción a una cuantía no superior a 100.000€.

SÉPTIMA. Se solicita la suspensión de la ejecución del acto recurrido.

Por último, SOLICITA:

a. Tenga por realizadas las alegaciones;

b. Se resuelva revocar y dejar sin efecto la resolución recurrida;

c. En cualquier caso, se acuerde la suspensión de la ejecución del acto recurrido, en tanto en cuanto, no se resuelva el presente recurso potestativo de reposición.

d. Proceda a considerar como confidenciales, y por tanto, no publicar los párrafos señalados en amarillo en la resolución que adjunta.

FUNDAMENTOS DE DERECHO

PRIMERO: Competencia.

Es competente para resolver el presente recurso la directora de la AEPD de conformidad con lo dispuesto en el artículo 48.1 de la LOPDGDD.

SEGUNDO: Sobre el recurso potestativo de reposición interpuesto.

En relación con las manifestaciones efectuadas por la parte recurrente, se reiteran básicamente las alegaciones ya presentadas a lo largo del procedimiento sancionador. Debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho (en lo sucesivo, FD) de la resolución recurrida, cuyo contenido se da por íntegramente reproducido.

TERCERO: Sobre la vulneración del artículo 89.3 de la LPACAP.

Aduce incumplimiento del deber de motivación de las resoluciones previsto en el artículo 89.3 de la LPACAP, y por extensión, del artículo 9.3 de la Constitución Española (en lo sucesivo, CE).

Alega el "principio de especialidad", asentado por el Tribunal Supremo. Aduce que aportó, no solo referencias jurisprudenciales y doctrinales, sino antecedentes en los que la Agencia calificó supuestos similares como vulneración del artículo 32 y no del artículo 5. Sin embargo, la resolución desestimó sus argumentos por estos motivos:

> 1.1. La conducta infractora halla encaje en el artículo 5.1.f: XFERA considera que puede ser subsumida en el artículo 32 del RGPD y así lo manifestó la Agencia en el acuerdo de inicio. Sin embargo, y pese a las reiteradas alegaciones de esta parte, la Agencia ignora en su resolución la posibilidad de aplicar al caso el citado artículo 32, hasta el punto de no dedicarle ni una sola línea en los fundamentos de derecho.
>
> 1.2. Los hechos son, en opinión de la Agencia, muy graves: la gravedad de la conducta es el único argumento esgrimido por la Agencia por el que cabría entender que los hechos merecerían ser considerados como vulneradores del artículo 5.1.f) del RGPD, en lugar del artículo 32. Afirmar que *"los perjuicios económicos no se hubieran producido si XFERA hubiera asegurado la identidad y autenticación correcta de sus clientes"* es una mera suposición que, no aporta nada al caso que nos ocupa y debería haber sido omitida en la resolución. Conforme a la lógica expresada por la Agencia, prácticamente cualquier conducta infractora podría ser subsumida como vulneración del artículo 5 del RGPD, siempre que sea lo suficientemente grave a juicio del regulador.
>
> 1.3. El artículo 5.1.f) no es "vago o abstracto", según la Agencia: lo que solicitaba XFERA es que se realizase una comparación entre los dos artículos (5 y 32), para concluir cuál de los dos es "más ajustado", "más complejo", "más concreto", "más preciso"; todo ello, en línea con lo asentado por el Alto Tribunal, y conforme al "principio de especialidad" aplicable al derecho administrativo sancionador. Es el artículo 32 el que define con más exactitud las obligaciones del responsable en relación con la seguridad en el tratamiento de los datos; y es algo natural, en la medida en que el artículo 5 define "principios", y el 32 "aterriza" o concreta uno de dichos principios. Alude a uno de los párrafos de la resolución (pág. 131) y al considerando 83 mencionado en la Resolución.
>
> 1.4. Conclusión: hay que determinar sobre cuál de los dos artículos supuestamente infringidos (el 5.1.f) o el 32) se debe fundamentar la sanción, y por qué. La Agencia se posiciona por el primero de los dos, pero no explica por qué.

En cuanto a la falta de motivación, debemos partir del artículo 89.3 de la LPACAP que dice:

> *3. En la propuesta de resolución se fijarán de forma motivada los hechos que se consideren probados y su exacta calificación jurídica, se determinará la infracción que, en su caso, aquéllos constituyan, la persona o personas responsables y la sanción que se proponga, la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión, así como las medidas provisionales que, en su caso, se hubieran adoptado. Cuando la instrucción concluya la inexistencia de infracción o responsabilidad y no se haga uso de la facultad prevista en el apartado primero, la propuesta declarará esa circunstancia.*

Asimismo, el artículo 88.1 de la LPACAP dice:

> *1. La resolución que ponga fin al procedimiento decidirá todas las cuestiones*

planteadas por los interesados y aquellas otras derivadas del mismo.

Cuando se trate de cuestiones conexas que no hubieran sido planteadas por los interesados, el órgano competente podrá pronunciarse sobre las mismas, poniéndolo antes de manifiesto a aquéllos por un plazo no superior a quince días, para que formulen las alegaciones que estimen pertinentes y aporten, en su caso, los medios de prueba.

(…)

3. Las resoluciones contendrán la decisión, que será motivada en los casos a que se refiere el artículo 35. (…)

Además, la exigencia de motivación de ciertos actos administrativos viene impuesta con carácter general por el artículo 35 de la LPACAP, entre ellos:

"1. Serán motivados, con sucinta referencia de hechos y fundamentos de derecho:

(…)

h) Las propuestas de resolución en los procedimientos de carácter sancionador, así como los actos que resuelvan procedimientos de carácter sancionador o de responsabilidad patrimonial (…)."

Esta exigencia de motivación responde a una triple necesidad, por cuanto, en primer lugar, expresa la racionalidad de la actuación administrativa al realizar la interpretación de la voluntad de la norma; en segundo lugar, permite que los destinatarios del acto pueden conocer esas razones y eventualmente someterlas a crítica; y, por último, abre las puertas a la fiscalización por los Tribunales de lo contencioso- administrativo de los actos o disposiciones impugnados, con el alcance previsto en el CE, satisfaciendo así adecuadamente el derecho a la tutela judicial proclamado en el artículo 24.1 de la CE.

En relación con la motivación de los actos administrativos el Tribunal Supremo ha declarado, como en la Sentencia de 4 de abril de 2012, que:

"(…) el deber de la Administración de motivar sus actos, como señala el Tribunal Supremo, entre otras, en la Sentencia de 19 de noviembre de 2001 , tiene su engarce constitucional en el principio de legalidad proclamado en el artículo 103 de la Constitución, así como en la efectividad del control jurisdiccional de la actuación de la Administración reconocido en el artículo 106 de la misma Constitución, siendo, en el plano legal, el artículo 54 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, el precepto que concreta con amplitud los actos que han de ser motivados, con suscita (sic) referencia a los hechos y fundamentos de derecho.

La exigencia de la motivación de los actos administrativos responde, según reiterada doctrina jurisprudencial, de la que es exponente la Sentencia del Tribunal Supremo de 16 de julio de 2001 , a la finalidad de que el interesado pueda conocer con exactitud y precisión el cuándo, cómo y por qué de lo establecido por la Administración, con la amplitud necesaria para la defensa de sus derechos e intereses, permitiendo también, a su vez, a los órganos jurisdiccionales el conocimiento de los datos fácticos y normativos que les permitan resolver la impugnación judicial del acto, en el juicio de su facultad de revisión y control de la actividad administrativa; de tal modo que la falta de esa motivación o su in-

suficiencia notoria, en la medida que impiden impugnar ese acto con seria posibilidad de criticar las bases y criterios en que se funda, integran un vicio de anulabilidad, en cuanto dejan al interesado en situación de indefensión.

Todo ello sin perjuicio de la lógica discrepancia de quien obtiene una resolución desfavorable a sus intereses, lo que no constituye falta de motivación, porque su derecho no alcanza a la concesión de lo pedido, ya que nadie tiene derecho a que le den la razón, sino a que la decisión que se le brinda ofrezca la explicación necesaria para que el administrado pueda conocer con exactitud y precisión el contenido del acto".

En el FD Quinto de la Resolución de fecha 10 de noviembre de 2021 (en adelante, la Resolución), bajo el epígrafe "Alegaciones aducidas a la Propuesta de resolución", dimos respuesta a las alegaciones formuladas por XFERA, en concreto, a las que planteaban la "Disconformidad con la calificación de la supuesta infracción", y se indicó lo siguiente:

En el presente caso, el principio de confidencialidad del dato se ha visto comprometido dado que se facilitó el acceso a unos duplicados de tarjetas SIM solicitados de forma fraudulenta. Y este acceso se produjo debido a que XFERA no contaba con medidas suficientemente apropiadas en los términos del reseñado artículo 5.1.f) del RGPD a fin de evitar que estos hechos se produjeran. Al respecto, se remite a lo expuesto en el FD Tercero de la presente Resolución.

Los hechos controvertidos, se consideran de la suficiente relevancia y gravedad, como para subsumirlos en una vulneración del artículo 5.1.f) del RGPD, precisamente, porque no se ha garantizado la seguridad de los datos de los clientes -de forma adecuada-, y en consecuencia, se ha producido un tratamiento no autorizado e ilícito que afecta a la confidencialidad de dato y que ha devenido en otras consecuencias, nada triviales, como son los perjuicios económicos, que no se hubieran producido, si XFERA, hubiera asegurado la identidad y autentificación correcta de sus clientes.

Las medidas de seguridad deben garantizar que en nuestra organización los datos de carácter personal sólo se usen con el fin legítimo para el que se recabaron, salvo posibles excepciones legales. Hay que realizar las comprobaciones periódicas que verifiquen y valoren la eficacia de las medidas de seguridad que hemos implantado.

Y por supuesto que existe un coste de aplicación, que requieren un tiempo, que a su vez deben ser conforme a la normativa y el estado de la técnica, pero es que, para seleccionar las medidas de seguridad adecuadas, el responsable debe basarse en los riesgos para las personas físicas, así como en lo que es razonable y técnicamente posible. El artículo 28.2.a) de LOPDGDD establece algunos supuestos en los que ya avisa que es necesario contemplar mayores riesgos que los que el responsable pudiera estimar si sólo tuviera en cuenta sus propios intereses (usurpación de identidad, perjuicios económicos…).

Por todo ello, la alegación que formula XFERA respecto de la inadecuada interpretación del principio de especialidad decae, puesto que los Hechos Probados se incardinan perfectamente en el vulnerado artículo 5.1.f) del RGPD. Este precepto, que no es vago o abstracto, establece obligaciones claras de cumplimiento -impedir tratamientos no autorizados o ilícitos implementando medidas

de seguridad apropiadas- cuya infracción determina una conducta típica, por cuya comisión ahora se sanciona a la operadora.

A mayor abundamiento, hemos de significar que XFERA confunde la tipificación de las infracciones prevista en el RGPD, apartados 4 y 5 del artículo 83 del RGPD, con la tipificación a los meros efectos de la prescripción prevista en los artículos 72, 73 y 74 de la LOPDGDD, a los efectos de su derecho de defensa. Así, la operadora considera que la LOPDGDD tipifica otra conducta que se ajusta de forma mucho más exacta al supuesto de hecho, cual es la prevista en el artículo 73.f) de la LOPDGDD.

Pues bien, la propia exposición de motivos de la LOPDGDD aclara que "La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea".

La conducta típica se encuentra enmarcada, tal y como se ha motivado, en el artículo 5.1.f) del RGPD constituyendo una infracción tipificada en el artículo 83.5.a) del RGPD; consecuencia de lo anterior, se tipifica de manera directa e inmediata como una infracción muy grave a los meros efectos de la prescripción en el artículo 72.1.a) de la LOPDGDD. Este es el camino que marca el RGPD para tipificar las infracciones y no otro.

Como sostiene el Auto del Tribunal Constitucional (ATC) 951/1986, de 12 de noviembre, *"una cosa es la carencia de motivación y otra la motivación concentrada, aunque precisa y suficiente".*

Por consiguiente*:*

> *"no es exigible una pormenorizada respuesta a todas las alegaciones de las partes, sino que basta que la motivación cumpla la doble finalidad de exteriorizar el fundamento de la decisión adoptada y permitir su eventual control jurisdiccional"* [SSTC 36/1989, de 14 de febrero, 70/1990, de 5 de abril; vid. Igualmente SSTC 14/1991, de 28 de enero, 116/1991, de 23 de mayo, 109/1992, de 14 de septiembre].

Incluso el Tribunal Constitucional ha admitido la motivación de aquellas resoluciones que, pese a mostrar lagunas en su argumentación, permitan inferir sin dudas el sentido y fundamento de la decisión. Declara en tal sentido la Sentencia del Tribunal Constitucional (en lo sucesivo, STC) 2/1992, de 13 de enero, que:

> *"Las exigencias de motivación que el art. 24.1 C.E. impone a las resoluciones judiciales no implican necesariamente una contestación expresa a todas y cada una de las alegaciones vertidas por las partes a lo largo del proceso. Por el contrario, según doctrina de este Tribunal (por todas, STC 175/1990), el silencio del órgano judicial respecto a alguna de las cuestiones suscitadas por las partes puede resultar ajustado a las exigencias del art. 24.1 C.E. cuando, atendidas las circunstancias del caso, pueda ser razonablemente interpretado como desestimación tácita de la argumentación esgrimida por el litigante"* (Vid. También STC 175/1990, de 12 de noviembre).

En el presente supuesto, la resolución recurrida especifica la infracción por la que se acuerda la sanción impuesta, en este caso, por "*la vulneración de lo dispuesto en ar-*

tículo 5.1.f) del Reglamento".

Sobre dicha infracción, ha podido alegar y probar lo que ha estimado pertinente. No existe, por lo tanto, un derecho a una determinada extensión de la motivación, puesto que su función se limita a comprobar si existe fundamentación jurídica y, en su caso, si el razonamiento que contiene constituye, lógica y jurídicamente, suficiente motivación de la decisión adoptada, cualquiera que sea su brevedad y concisión, incluso en supuestos de motivación por remisión (por todas, SSTC 184/1998, de 28 de septiembre, FJ 2; 187/1998, de 28 de septiembre, FJ 9; 215/1998, de 11 de noviembre, FJ 3; 206/1999, de 8 de noviembre, FJ 3, 187/2000, FJ 2).

El Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, Sentencia de 5 Mar. 2012, Rec. 6515/2010, indica: "*El contenido mínimo de la motivación depende del «juicio de suficiencia» exigido por el caso concreto en el que se integre. Ello implica, que bastará cualquier motivación, por sucinta que sea, que explicite los elementos fácticos y jurídicos que constituyan las premisas del acto a motivar; de tal manera que éste aparezca como la conclusión razonada y razonable de aquéllos."*

En cuanto al principio de especialidad invocado y la comparación entre los dos artículos del RGPD y la fundamentación de porqué imputamos el tipo infractor del artículo 5.1.f) y no el artículo 32, se aclara lo siguiente.

El principio de legalidad sancionadora previsto en el artículo 25 de la CE y desarrollado en el artículo 25 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en lo sucesivo, LRJSP) en relación con el artículo 27 LRJSP, supone que la norma de rango legal definirá la infracción y la sanción que corresponda y las garantías del procedimiento que recogen los artículos 63, 64, 85 y 89 en relación con el 90 de la LPACAP exigen esa existencia y correspondencia entre el hecho que se imputa y la sanción correspondiente. La jurisprudencia del Tribunal Supremo ha sido reiterada, por todas las de 21 de febrero y 4 de abril de 2006, al señalar que la individualización de una sanción es una operación de carácter reglado y ciertamente sometida a la regulación de las normas de rango legal que disciplinan una operación. Cada tipo infractor se corresponde con la imposición de una sanción, y en consecuencia la Administración Pública titular de la potestad sancionadora que en cada caso se actúa deberá de conducirse aplicando la técnica jurídica descrita.

Por otra parte, el artículo 29.5 de la LRJSP, dice: *Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida.*

Pues bien, la AEPD, conforme al artículo 64.2.b) de la LPACAP, acordó iniciar expediente sancionador contra XFERA por presunta infracción del artículo 5.1.f) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1.a) de la LOPDGDD a los efectos de la preinscripción, sin perjuicio de lo que resultase de la instrucción del procedimiento. En este sentido, el artículo 75 de la LPACAP, se refiere a los "Actos de instrucción" como aquellos necesarios para la determinación, conocimiento y comprobación de los hechos en virtud de los cuales deba pronunciarse la resolución. Tras el análisis de las pruebas practicadas y de las alegaciones aducidas conforme a lo previsto en los artículos 76 y 77 de la LPACAP, se constataron los hechos probados y se concluyó, que no podía colegirse una infracción del artículo 5.2 del RGPD, pero sí del artículo 5.1.f) del RGPD. Esta decisión, repercutió directamente en la sanción propuesta que pasó de 500.000'00 a 250.000'00 en la propuesta de resolución y que finalmente se fijó en 200.000'00 euros.

Por otra parte, es perfectamente admisible que la AEPD considere la vulneración de un determinado precepto en el convencimiento de que se ajusta más a los hechos que acontecen, sin que esta actuación pueda calificarse de arbitraria, máxime cuando está debidamente motivada.

El considerando 39 del RGPD señala:

> *" … Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento."*

El considerando 85 del RGPD dice:

> *"Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. (…)"*

El deber de confidencialidad surge del artículo 5.1.f) del RGPD cuando afirma que los datos deben ser *"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»)".*

Se trata, por tanto, del principio relacionado tanto con la confidencialidad de los datos personales tratados como con la seguridad del tratamiento.

Es decir, las operadoras deben estar en disposición de establecer mecanismos que impidan que se produzca la duplicación fraudulenta de las tarjetas SIM, medidas que respeten la confidencialidad de los datos y que impidan que un tercero acceda a datos que no son de su titularidad, pues precisamente compete a la operadora tratar datos de carácter personal conforme al RGPD.

Por dicha razón, este es un proceso en dónde la diligencia prestada por estas es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que el tratamiento de datos es conforme al RGPD.

Tomando como criterio la jurisprudencia dictada sobre la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se diferenciaba entonces entre la vulneración del deber de secreto, asimilable hoy al deber de confidencialidad (artículo 5.1 LOPDGDD), de estas otras infracciones relativas a medidas de seguridad, a través de afirmar que, mientras la infracción del deber de secreto exige un resultado (divulgación o comunicación de datos), la relativa a medidas de seguridad es una infracción de actividad (ausencia de medidas adecuadas), sin requerir por tanto tal divulgación. En otras palabras, mientras que la infracción del principio de confidencialidad supone que los datos se hayan revelado a un tercero, la infracción de medidas de seguridad únicamente requiere que se declare probada la ausencia de los requisitos de seguridad exigidos.

Resulta ilustrativa la Sentencia de la Audiencia Nacional (en lo sucesivo, SAN)

3059/2009, de 18 de junio, que señala:

> *"Por lo tanto, resulta que no se ha acreditado que se haya producido ninguna forma de infracción del deber de secreto pues aunque, es cierto que la documentación no estuvo correctamente custodiada y no era razonable que las historias clínicas viajaran en un camión con el resto de escombros de la demolición de un hotel, la realidad es que ninguna violación del secreto se ha producido y nadie ha llegado a tener noticia de la documentación clínica que, al parecer, sigue custodiada en las cajas en cuestión cuya fotografía ha aportado la parte recurrente.*
>
> *Esta Sala tiene establecido como la infracción del deber de secreto es una infracción de resultado en la que lo relevante es que se llegue a producir la divulgación de un secreto, no siendo relevante (a los efectos de la violación del deber de secreto) con la simple omisión de medidas de seguridad."*

Del mismo modo, en la SAN 2285/2009, de 7 de mayo, se expuso expresamente esta diferencia del siguiente modo:

> *"La infracción tipificada en el art. 44.3 .g) es una infracción de resultado que exige que los datos personales sobre los que exista un deber de secreto profesional -como aquí ocurre en relación con el número de la cuenta corriente- se hayan puesto de manifiesto a un tercero, sin que pueda presumirse que tal revelación se ha producido. Efectivamente, la Agencia Española de Protección de Datos en su resolución se limita a poner de manifiesto que el sistema de cierre, mediante ventanilla transparente, de los sobres utilizados por el Banco para realizar determinadas comunicaciones a sus clientes pudiera dar lugar a que determinados datos personales contenidos en esas comunicaciones puedan ser conocidas por terceras personas respecto de las que deba mantenerse el secreto. No prueba sin embargo que los datos fueran efectivamente conocidos por dichos terceros. Estaríamos, por tanto, como sostiene el recurrente, ante una posible infracción de medidas de seguridad -que es una infracción de actividad- pero no ante la infracción que se le imputa que exige la puesta en conocimiento de un tercero de los datos personales."*

Por tanto, integrando el tipo infractor del artículo 83.5.a) por infracción del artículo del 5.1.f) del RGPD, se encuentra el hecho de que la información o datos personales se pongan en comunicación de terceros, circunstancia que concurre en los casos analizados. Cuando se produce la emisión y entrega del duplicado a un tercero no autorizado, los afectados pierden el control de la tarjeta SIM (soporte físico que almacena datos personales) y el tercero no autorizado efectúa un tratamiento de los datos almacenados en la tarjeta SIM que corresponden al legítimo titular y lo hace, sin base legal alguna.

De ahí que, el duplicado de la tarjeta SIM impida al legítimo titular hacer uso de su terminal telefónico, al quedar anulada la anterior tarjeta, con los consecuentes problemas a la hora de hacer uso (en su caso) de las aplicaciones como también del servicio contratado. Así, el usuario de la tarjeta SIM legítima dejará de tener cobertura en su teléfono móvil, no podrá realizar llamadas ni enviar SMS. Por lo tanto, el valor de ese dato personal, integrado en un soporte físico -tarjeta SIM-, es real e incuestionable, motivo por el cual XFERA tiene el deber legal de garantizar su seguridad y confidencialidad, tal como haría con cualquier otro activo de la empresa.

En consecuencia, la alegación primera debe ser desestimada.

CUARTO: Sobre la vulneración del artículo 77 de la LPACAP.

Se alega, incumplimiento durante la instrucción del procedimiento del deber de abrir un período de prueba, conforme al citado artículo y por extensión, del artículo 24.2 de la CE.

La Agencia insiste en afirmar que se ha producido una quiebra en el principio de confidencialidad del dato, cuando no ha sido así; y no ha logrado incorporar al procedimiento ningún tipo de prueba para sostener esta afirmación.

Aduce, que la tarjeta SIM que se entrega al usuario al realizar un duplicado está en blanco, no contiene datos de carácter personal de ningún tipo. Tampoco identifica número de teléfono alguno, porque el número de teléfono del usuario no se almacena en la tarjeta SIM, sino en los servidores de XFERA.

La parte reclamante razona lo siguiente:

- Que una tarjeta SIM no es un dato personal, sino un soporte susceptible de almacenar datos personales. Por tanto, el mero duplicado de una tarjeta no constituye una vulneración de la confidencialidad de los datos, especialmente cuando en su interior no se hayan almacenado datos de esta naturaleza;
- Que una tarjeta SIM nueva, como la que se entrega a un usuario cuando solicita un duplicado, únicamente incluye claves criptográficas del operador y un número de serie, denominado IMSI, que únicamente identifica a la propia tarjeta. Lo que se conoce vulgarmente como “activar una tarjeta SIM” es un procedimiento técnico que XFERA realiza en sus propios servidores, consistente en derivar el tráfico generado o dirigido a número de un abonado (MSISDN) al IMSI de una determinada tarjeta SIM. Es indudable que la realización de este procedimiento “supone el tratamiento de los datos personales” del titular de la línea telefónica; pero este tratamiento se realiza en los servidores de XFERA, jamás en la propia tarjeta SIM. Así, cuando un delincuente logra obtener un duplicado:
    - ◦ No se añade ni se elimina dato alguno de la SIM: la tarjeta sigue almacenando exactamente la misma información que incluía antes de la activación, cuando ya obraba en poder del delincuente, por lo que no puede entenderse que contenga datos personales; y
    - ◦ En ningún momento el suplantador tiene acceso a la información almacenada en los servidores de XFERA, luego no puede atribuirse a mi representada una vulneración del principio de confidencialidad;

  ▪ Que, en relación con el IMSI incluido en la tarjeta duplicada, en ningún momento es utilizado en el teléfono móvil del titular real de la línea, por lo que tampoco es posible asociarlo con esta persona;

  ▪ Que en relación con el IMEI, se trata de un código que identifica de forma unívoca a un concreto terminal de telefonía móvil, esto es, al propio aparato, al teléfono móvil en sentido estricto; y nada tiene que ver con la tarjeta SIM ni con el IMSI. y

  ▪ Que en relación con la identidad del titular de la línea, el suplantador ya contaba con esa información, pues en caso contrario no habría podido superar los procedimientos de seguridad de XFERA.

La resolución ni siquiera dedica una línea a explicar por qué estos sólidos argumentos

deben ser desechados: se limita a afirmar que *"el principio de confidencialidad del dato se ha visto comprometido dado que se facilitó el acceso a unos duplicados de tarjetas SIM solicitados de forma fraudulenta*", sin ofrecer más explicaciones. Se vulnera así, también lo establecido en el artículo 90.1 de la LPACAP, que exige que la resolución incluya "*la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión*".

Debemos partir del artículo 77 de la LPACAP, que dice:

> *1. Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba admisible en Derecho, cuya valoración se realizará de acuerdo con los criterios establecidos en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*
>
> *2. Cuando la Administración no tenga por ciertos los hechos alegados por los interesados o la naturaleza del procedimiento lo exija, el instructor del mismo acordará la apertura de un período de prueba por un plazo no superior a treinta días ni inferior a diez, a fin de que puedan practicarse cuantas juzgue pertinentes. Asimismo, cuando lo considere necesario, el instructor, a petición de los interesados, podrá decidir la apertura de un período extraordinario de prueba por un plazo no superior a diez días.*
>
> *3. El instructor del procedimiento sólo podrá rechazar las pruebas propuestas por los interesados cuando sean manifiestamente improcedentes o innecesarias, mediante resolución motivada.*
>
> *4. En los procedimientos de carácter sancionador, los hechos declarados probados por resoluciones judiciales penales firmes vincularán a las Administraciones Públicas respecto de los procedimientos sancionadores que substancien.*
>
> *5. Los documentos formalizados por los funcionarios a los que se reconoce la condición de autoridad y en los que, observándose los requisitos legales correspondientes se recojan los hechos constatados por aquéllos harán prueba de éstos salvo que se acredite lo contrario.*
>
> *6. Cuando la prueba consista en la emisión de un informe de un órgano administrativo, organismo público o Entidad de derecho público, se entenderá que éste tiene carácter preceptivo.*
>
> *7. Cuando la valoración de las pruebas practicadas pueda constituir el fundamento básico de la decisión que se adopte en el procedimiento, por ser pieza imprescindible para la correcta evaluación de los hechos, deberá incluirse en la propuesta de resolución.*

El principio de presunción de inocencia, recogido en el artículo 24.2 de la CE y 28.1 de la LRJSP, y que la doctrina del Tribunal Constitucional ha considerado aplicable al derecho administrativo sancionador (SSTC 13/1981, 76/1990) implica, efectivamente, que la carga de la prueba de los hechos constitutivos de la infracción recaiga sobre la Administración (SSTC 76/1990, 120/1994, 154/1994, 23/1995, 97/1995, 147/1995 y 45/1997).

Asimismo, la jurisprudencia ha declarado que la presunción de inocencia *"(...) comporta que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponde a quien acusa, sin que nadie esté obligado a probar su propia inocencia, y que cualquier insuficiencia*

en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, deba traducirse en un pronunciamiento absolutorio" (STS de 20 de septiembre de 2012, Rec. 371/2011).

Pues bien, con fecha 5 de mayo de 2021, se notificó a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, el acuerdo de apertura de un periodo de prueba, por un plazo de 10 días hábiles, con el fin de que pudieran llevarse a cabo las pruebas que por su relevancia se declararon pertinentes.

En esta línea y a modo de ejemplo, obra en el expediente lo siguiente:

- Denuncias ante Dirección General de la Policía Nacional en las dependencias de Granada Centro, en fecha 26 de septiembre de 2019, con número de atestado ***XXXX/XX*** y ***YYYY/YY***.
- Denuncias ante Dirección General de la Policía Nacional en las dependencias de Móstoles, en fecha 11 de julio de 2019, con número de atestado ***SSSSS/SS*** y ***RRRRR/RR.***
- Justificantes bancarios en las que figuran las transacciones realizadas.
- Archivos de audio sobre las grabaciones realizadas.
- Documentación aportada por XFERA, por ejemplo, el protocolo de cambio de SIM .
- Afirmaciones de la parte recurrente:
    - Respecto a la parte reclamante uno informó en su respuesta de fecha 3 de julio 2020, que su departamento de fraude veía indicios de que la documentación presentada (…) junto con la solicitud de duplicado de tarjeta SIM de fecha 25 de septiembre de 2019 estaba falsificado. En escrito de alegaciones, de fecha 8 de marzo de 2021, afirmó que los delincuentes lograron engañar al personal de una tienda de la marca Yoigo mediante la entrega de documentación falsa, y en concreto, de un (…).
    - En el caso de la parte reclamante dos indicó que, en fecha 9 de octubre de 2020, que el canal por el que se activó la SIM fue el telefónico y aportó la oportuna grabación como Documento nº 19. Escuchada la grabación, se verificó que el operador preguntó (…). No le pide el número de DNI tampoco. En alegaciones de fecha 8 de marzo de 2021, afirma que todo indica que el suplantador se hizo con una tarjeta SIM “en blanco”, probablemente tras obtenerla ilícitamente de (…). Así se desprende del contenido de la llamada, en la que se comprueba que el solicitante contaba con el ICCID completo de la tarjeta SIM que únicamente figura impreso en el dorso de la propia tarjeta.

A la vista de lo expuesto, no cabe sino concluir en la correcta valoración de la prueba por parte de la Agencia, prueba que tiene entidad para ser considerada de cargo y desvirtuar el derecho fundamental a la presunción de inocencia garantizado en el artículo 24.2 de la CE.

Respecto a los razonamientos aducidos sobre la tarjeta SIM, IMSI e IMEI, el Informe de la Fiscalía General del Estado sobre “Identificación de terminales o dispositivos de conectividad al amparo del art. 588 Ter de la Ley Orgánica 13/2015” elaborado en el mes de julio de 2016 indica que: Según los estándares europeos relativos a sistemas

de telecomunicaciones celulares digitales establecidos por el Instituto Europeo de Estándares de Telecomunicaciones, un dispositivo de comunicaciones móviles celulares plenamente operativo, denominado en el lenguaje coloquial “Teléfono Móvil” y en el técnico “Estación Móvil”, se compone materialmente de dos elementos esenciales:

- En primer lugar, el terminal o equipo electrónico móvil dotado de pantalla, procesador, memoria, módem de comunicaciones y batería.

- En segundo lugar, el módulo de identificación de usuario, más conocido como “tarjeta SIM” (Subscriber Identity Module). Esta tarjeta SIM es intercambiable entre los diferentes terminales móviles existentes en el mercado y contiene en su chip digital la información necesaria para identificar y autenticar al abonado, incluido el International Mobile Subscriber Identity (IMSI), el cuál identifica de forma inequívoca al abonado en la red celular. Sin un IMSI válido los servicios de telefonía móvil no serán accesibles, salvo en el caso de llamadas de emergencia.

La Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, concretamente en su artículo 3.1.e.2º, establece como datos necesarios para la identificación del equipo de comunicación empleado en el ámbito de la telefonía móvil el IMSI y el IMEI, entre otros.

Así, mientras que un terminal móvil puede ser suministrado a un usuario en cualquier comercio del sector electrónico o por su proveedor de servicios de telecomunicaciones, una tarjeta SIM operativa siempre habrá de ser suministrada al abonado por su compañía proveedora de servicios de telecomunicaciones, conteniendo la ya citada información que le identificará en la red, IMSI incluido, y que le dará acceso a los servicios contratados. Por este motivo, un proveedor de servicios de telecomunicaciones contará en sus bases de datos de clientes y de facturación con los datos personales del abonado, de la SIM y el IMSI suministrado y, en caso de haber suministrado también un terminal móvil, el IMEI del mismo (International Mobile Estation Equipment Identity).

El IMSI es, por tanto, el código de identificación por excelencia en la red de comunicaciones móviles celulares, que da acceso al abonado a los servicios contratados y que permite la facturación correspondiente por parte del proveedor. Es por tanto fundamental para identificar al usuario del teléfono y aparece en todas las conexiones entre el terminal y la red. Esa interacción y el consiguiente trasvase de datos se produce, por supuesto, cuando se está produciendo una conversación telefónica, pero no debemos olvidar que también hay conexión desde el momento en que se enciende el terminal, y por lo tanto en situaciones ajenas a un proceso comunicativo concreto.

Asimismo, el Informe 0030/2021 del Gabinete Jurídico de la AEPD indica:

> *Conviene aclarar, en primer lugar, que el IMSI se integra en la tarjeta SIM, y sirve para identificar internacionalmente al abonado, y a partir del cual se asigna un MSISDN que se conoce como número comercial, conocido coloquialmente como el número de teléfono. Y, en segundo lugar, debe tenerse en cuenta que la tarjeta SIM contiene una programación que, una vez introducido el PIN permite la búsqueda de redes GSM y UMTS y trata de conectarse en una de ellas. Cuando se ha conectado a la red, el teléfono (IMSI y IMEI) queda registrado y estará disponible para usar los servicios contratados.*

Por lo tanto, si el IMSI está almacenado en la tarjeta SIM, quien tenga la tarjeta SIM (el

suplantador) tiene el IMSI almacenado (almacenar un dato personal implica tratarlo). Además, en cuanto el suplantador introduzca la SIM en un terminal y lo encienda, el IMSI va a ser accedido e intercambiado con la red.

Respecto al IMEI, consideramos que se trata de un dato personal y también puede haber tratamiento. Cuando el suplantador utiliza la SIM en un equipo propio, el operador puede asociar el IMEI del equipo del suplantador al usuario, registrando toda la actividad asociada a dicho usuario con un IMEI incorrecto, en cuyo caso, se produciría un problema de "exactitud" (artículo 5.1.d) RGPD).

Hay que destacar la Sentencia de la Audiencia Provincial (SAP) de Barcelona núm. 390/2019 de 30 de mayo, que dispone: "*Sin embargo, la identidad del titular de la tarjeta SIM, o lo que es lo mismo, la identidad del titular del número de teléfono asociado a dicha tarjeta, no constituye un dato de tráfico derivado de las comunicaciones telefónicas ni un dato que afecte a la comunicación misma. No cabe duda de que constituye un dato personal relativo a la intimidad de la persona amparada en el art. 18.1 CE."*

De manera que, cuando el suplantador consigue que se active la tarjeta SIM se hace con el control del número de teléfono del abonado con el fin de realizar una serie de acciones asociadas a ese número, y desde ese instante, se produce un tratamiento de datos (artículo 4.2 RGPD) no autorizado e ilícito.

Según el Informe denominado "Contrarrestar el intercambio de SIM" publicado en diciembre de 2021 por ENISA (Agencia de la Unión Europea para la Ciberseguridad):

> *"Los atacantes abusan de la capacidad de los proveedores para portar rápidamente y sin problemas un número de teléfono a un dispositivo que contiene un módulo de identidad de suscriptor diferente (SIM). Como resultado, el atacante se hace cargo de la cuenta y puede recibir todos los SMS y llamadas de voz destinados al suscriptor legítimo. Los estafadores pueden realizar fraudes bancarios en línea, pero también eludir la autenticación de dos factores (2FA) utilizada para proteger las redes sociales y otras cuentas en línea." (…)*
>
> *"Los operadores de redes móviles deben reforzar los mecanismos fraudulentos de detección y bloqueo de la SIM mediante la mejora de los procesos internos para proporcionar al cliente una experiencia preferentemente sin fisuras." (…)*
>
> *"Del mismo modo, a muchos otros ataques contra la confidencialidad, integridad y autenticidad de las comunicaciones electrónicas de los suscriptores individuales, en los ataques de intercambio de SIM, el objetivo del atacante es obtener el control de la cuenta móvil del abonado objetivo con el fin de realizar una serie de acciones asociadas con su número de móvil. Este tipo de ataque aprovecha la capacidad del ORM -operador de red móvil- para transferir un número de teléfono móvil a una SIM diferente, un procedimiento denominado «portabilidad de número». Por lo tanto, el objetivo del atacante es hacerse cargo de la cuenta de un abonado móvil cambiando la afiliación de dicha cuenta de la tarjeta SIM original a una tarjeta SIM bajo el control del atacante.*
>
> *El atacante normalmente comienza un ataque de intercambio de SIM mediante la recopilación de detalles personales sobre el suscriptor objetivo, por ejemplo a través de ingeniería social, phishing, malware, la explotación de información de violaciones de datos o haciendo investigaciones en las*

redes sociales. Una vez que el atacante ha obtenido suficientes detalles para hacerse pasar por el suscriptor objetivo, puede ser capaz de convencer al ORM de que porte el número móvil del abonado a una nueva tarjeta SIM bajo el control del atacante.

Si esta parte inicial del ataque tiene éxito, la tarjeta SIM del suscriptor genuino perderá la conexión a la red. Esto permitirá al atacante recibir todo el tráfico SMS y de voz destinado al suscriptor objetivo, como contraseñas únicas (OTP) enviadas mediante llamadas de texto o telefónicas, por ejemplo para iniciar sesión en la banca en línea."

"(…) interceptar el SMS, incluyendo OTP (One Time Password) para transacciones financieras, es uno de los objetivos básicos de los atacantes. Mientras que los atacantes también pueden interceptar el SMS OTP utilizando métodos de ataque más elaborados (como explotar vulnerabilidades de protocolo SS7), el intercambio de SIM parece ser la forma más fácil de interceptar SMS para realizar fraudes bancarios, ya que no requiere herramientas técnicas complejas o costosas." (La traducción es nuestra)

Por todo lo cual, el acceso a una copia de tarjeta SIM no autorizada por el legítimo titular, sí supone la pérdida de disposición o control sobre dicho soporte, y en consecuencia, se ve afectada tanto la confidencialidad como la seguridad del tratamiento.

En consecuencia, la alegación segunda debe ser desestimada.

QUINTO: Sobre la vulneración del artículo 8 de la LRJSP.

Aduce XFERA que existe una normativa específica y especial sobre el RGPD, cual es el artículo 39.1 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (LGTEL), que dice lo siguiente:

"1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias."

Podría discutirse, alega, si procede atribuir la comisión de una infracción, tipificada en el artículo 78.10 de dicho cuerpo legal, cuando la competencia para sancionar ese tipo de conductas recae, exclusivamente, en la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales. Así lo recoge el artículo 84.1 de la LGTEL, que debe ser puesto en relación, a los efectos que nos ocupan, con el artículo 8 de la Ley 40/2015, que esta representación entiende vulnerado.

Cuando el Tribunal Constitucional reconoció el derecho fundamental a la protección de datos como una realidad autónoma, a través de las sentencias 94/1998 y 292/2000, citadas por la Agencia en su resolución, lo hizo con una finalidad clara: dotar a las personas físicas de un poder de disposición y de control sobre los datos personales, no sobre una línea telefónica y una tarjeta SIM.

Sin embargo, la Agencia retuerce las categorías jurídicas para intentar convertir una acción, tipificada desde la perspectiva del secreto de las comunicaciones, en una vulneración de la normativa de protección de datos personales, arrogándose un papel (el de defensora del usuario de los servicios de comunicaciones electrónicas) que no le corresponde, mediante el artificio de reconducir los hechos hacia una supuesta infracción del principio de confidencialidad de los datos personales que no se acredita en

ningún momento.

Pues bien, alude la parte recurrente al artículo 39 incluido en el Capítulo III bajo el epígrafe “Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas” y omite, sin embargo, lo dispuesto en el artículo 41 también incluido en el mismo Capítulo.

> *Artículo 41. Protección de los datos de carácter personal.*
>
> *1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal. Dichas medidas incluirán, como mínimo:*
>
> *a) La garantía de que sólo el personal autorizado tenga acceso a los datos personales para fines autorizados por la Ley.*
>
> *b) La protección de los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos.*
>
> *c) La garantía de la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales.*
>
> *La Agencia Española de Protección de Datos, en el ejercicio de su competencia de garantía de la seguridad en el tratamiento de datos de carácter personal, podrá examinar las medidas adoptadas por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público y podrá formular recomendaciones sobre las mejores prácticas con respecto al nivel de seguridad que debería conseguirse con estas medidas.*
>
> *(…)*
>
> *4. Lo dispuesto en el presente artículo será sin perjuicio de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.*

La SAN 1695/2011, de 1 de abril de 2011, dice:

> *La seriedad que conlleva el ejercicio de la potestad sancionadora aconseja que se pongan en marcha los mecanismos administrativos y jurisdiccionales correspondientes solo cuando se suponga que se ha producido una verdadera violación del derecho fundamental a la protección de datos.*

El artículo 39 de la LGTEL y la correlativa infracción del artículo 78.10 se refieren a los procedimientos de interceptación legal de las comunicaciones. Es decir, a la obligación de los operadores de telecomunicaciones de colaborar con los Jueces y Tribunales cuando estos le dirijan una orden de interceptación para la escucha de comunicaciones privadas. Esta cuestión, nada tiene que ver con el procedimiento sancionador resuelto por la directora de la AEPD, que trata sobre la seguridad y confidencialidad de los datos personales. En el primer caso, se regula la excepción al derecho del secreto

de comunicaciones que se prevé en el artículo 18.3 CE, mediante intervención judicial, y que requiere la colaboración del operador. En el segundo, se trata del derecho fundamental a la protección de datos (artículo 18.4 CE), que es un derecho fundamental diferente.

Por lo tanto, cabe concluir la desestimación de la alegación aducida.

SEXTO: Sobre la vulneración del artículo 28 de la LRJSP.

Entiende XFERA que el citado artículo ha sido vulnerado por esta Agencia, desde dos puntos de vista: el llamado "principio de culpabilidad" y el llamado "principio de responsabilidad personal".

4.1. Sobre el principio de culpabilidad:

Alega que no tuvo conocimiento de las consecuencias de la aplicación de la Directiva hasta el 26 de septiembre de 2019, cuando recibe un requerimiento de la Subdirección General de Atención al Usuario de Telecomunicaciones, de la Secretaría de Estado para el Avance Digital (SEAD) en el que se le informa de que "se han recibido consultas y reclamaciones" en relación con el tipo de fraude que conocemos como SIM Swapping. XFERA no es un sujeto obligado por esta Directiva, por lo que desconocía su alcance y la forma en la que las entidades bancarias optarían por implementarla; y estas últimas implementaron el envío a sus clientes de códigos de autenticación por SMS sin informar en ningún momento a las empresas del sector de las telecomunicaciones ni contar con su opinión, aun a sabiendas de que este método era vulnerable y estaba desaconsejado por los principales organismos especializados en ciberseguridad.

Que, en cuanto tuvo conocimiento de esta problemática, actuó con diligencia: en un plazo de dos meses ya había actualizado sus medidas de seguridad, que se comenzaron a aplicar el 28 de noviembre de ese mismo año y que lograron una drástica reducción (superior al 95%) de los casos de duplicado ilícito de tarjetas SIM.

Sin embargo, la consideración de estas circunstancias como atenuante es insuficiente, pues deberían haber sido consideradas eximentes, siquiera parciales; y trae a colación la doctrina del error invencible, íntimamente relacionada con el principio de culpabilidad recogido en el artículo 28 de la LRJSP.

Como explica la Agencia en su "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD":

"Garantizar una adecuada gestión de riesgos requiere la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas para reducir el nivel de exposición al riesgo.

Se recomienda revisar el análisis de riesgos realizado ante cualquier cambio significativo en las actividades de tratamiento que pueda derivar en la aparición de nuevos riesgos".

Eso fue, exactamente, lo que hizo XFERA; y a pesar de cumplir con lo recomendado por esta Agencia, es considerada administrativamente responsable, y sancionada con la nada despreciable cantidad de 200.000€.

Conforme al RGPD, las medidas no tienen que ser adecuadas para evitar las suplantaciones de identidad, pues nos encontraríamos ante una obligación de

resultado, ajena al ordenamiento. Antes al contrario, la obligación del Responsable es “evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos”, y XFERA cumplió con esta obligación, como se ha demostrado al aportar al expediente los distintos análisis de riesgos realizados.

Es evidente que las medidas resultaron ser insuficientes, pero ello no se debió a la falta de cuidado de XFERA, sino a una modificación en las circunstancias del tratamiento de la que no tenía conocimiento, motivada por causas ajenas a su actividad empresarial.

Por último, alude a que la Agencia fundamenta su resolución en el resultado. Aplica un criterio de responsabilidad objetiva: se la considera negligente, no por carecer de unas medidas de seguridad adecuadas al riesgo, sino por el resultado socialmente dañoso producido.

4.2. Sobre el principio de responsabilidad personal: a la hora de analizar la gravedad de la infracción deben tenerse en cuenta únicamente los hechos de los que es directamente responsable XFERA y no a la posterior realización de “operaciones bancarias fraudulentas”. Por tanto, y aunque sea en forma de agravante, se atribuye a XFERA responsabilidad por unos hechos (las operaciones bancarias fraudulentas) que le son ajenos, vulnerando así el principio de personalidad aplicable al derecho administrativo sancionador.

XFERA no es “responsable” ni “encargada” de ninguno de los tratamientos a los que logra acceder el delincuente de forma indebida a través de dichos SMS: es un mero “tercero”, conforme al artículo 4 del RGPD; y los terceros no están sujetos al régimen sancionador previsto en el propio Reglamento ni en la LOPDGDD.

Pues bien, el artículo 28.1 de la LRJSP, dispone que:

> *Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa.*

Ya se analizó en el FD Quinto de la Resolución, bajo la rúbrica “CUARTA. Vulneración del principio de culpabilidad”, que, en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas. Según la STC 246/1991:

> *"(...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma*" (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

Alude a un desconocimiento de la Directiva, cuando el artículo 6.1 del Código Civil, in-

dica: La ignorancia de las leyes no excusa de su cumplimiento. (…)

Invoca la doctrina del error invencible. En este sentido, la Sentencia del Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia 602/2015 de 13 Oct. 2015, Rec. 191/2015, indica: "El error ha de demostrarse indubitada y palpablemente (STS 123/2001, 5 de febrero), pues la jurisprudencia tiene declarado que el concepto de error o el de creencia errónea (art. 14 CP 1995) excluye por su significación gramatical, la idea de duda; y en este sentido error o creencia errónea equivale a desconocimiento o conocimiento equivocado, pero en todo caso firme. En cualquier caso -recuerda la STS 687/1996, 11 de octubre -, el error o la creencia equivocada no sólo ha de probarse por quien la alega, aunque esto en algún aspecto sea discutible, sino que además, y esto es lo importante, no es permisible su invocación en aquellas infracciones que sean de ilicitud notoriamente evidente, de tal modo que de manera natural o elemental se conozca y sepa la intrínseca ilicitud". En definitiva, el error invencible conlleva la carga de su prueba por quien lo alega.

El artículo 5.2 del RGPD establece que *"El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)"*. Así, en este precepto, se destaca la figura que debe asumir la responsabilidad última (el responsable del tratamiento) por cualquier tratamiento de datos personales que realice él mismo o por su cuenta (considerando 74 del RGPD).

Implica, que no sólo existe responsabilidad por una infracción, sino que la no adopción del conjunto de medidas requeridas para el perfecto cumplimiento normativo, o la falta de diligencia al hacerlo, supone también una responsabilidad punible para las organizaciones o empresas.

La SAN, Sala de lo Contencioso-administrativo, Sección 1ª, de 5 Mayo 2021, Rec. 1437/2020, indica:

> *Por otro lado, en cuanto al hecho de que nos encontramos ante el fraude de un tercero, como dijimos en la SAN de 3 de octubre de 2013 (Rec. 54/2012): "Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento...".*

Resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica que:

> "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

En cuanto a la responsabilidad objetiva, que dice, exige la Agencia, tal y como razona la SAN de 21 de enero de 2010 (JUR 2010, 60135), rec. 719/2008 , en su FJ 3º:

> *"...No basta con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto,*

no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados (...) la observancia de aquellas instrucciones.

Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros . Y ello porque toda responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos personales han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues también es responsable de que las mismas se cumplan y se ejecuten con rigor. En definitiva, toda responsable de un fichero debe asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios, o cualesquiera otros datos de carácter personal, puedan llegar a manos de terceras personas."

La Sentencia del Tribunal Supremo (STS) 5298/1994, de 9 de julio de 1994, indica:

"…la potestad sancionadora de la Administración goza de la misma naturaleza que la potestad penal, por lo que en consecuencia, las directrices estructurales del ilícito administrativo tienden también, como en el ilícito penal, a conseguir la individualización de la responsabilidad, vedando cualquier intento de construir una responsabilidad objetiva o basada en la simple relación con una cosa, por consiguiente en el ámbito de la responsabilidad administrativa no basta con que la conducta sea antijurídica y típica, sino que también es necesario que sea culpable, esto es, consecuencia de una acción u omisión imputable a su autor por malicia o imprudencia, negligencia o ignorancia inexcusable (STC, Sala del artículo 61 de la Ley Orgánica del Poder Judicial, de 6 de noviembre de 1990)"

No nos encontramos con una responsabilidad objetiva, tal y como asevera la parte recurrente, sino con un resultado objetivo producido de suplantación de identidad al no haberse garantizado una seguridad adecuada en el tratamiento de los datos personales.

Por lo tanto, cabe apreciar falta de diligencia en la actuación de XFERA, sin que quepa apreciar falta de culpabilidad.

En cuanto al principio de responsabilidad personal invocado, no es que la Agencia contradiga sus propias afirmaciones o que no se haya ceñido a la responsabilidad que corresponde a XFERA, sino que, en los casos analizados, la falta de diligencia de la parte recurrente ha sido clara, existiendo una falta de diligencia en el tratamiento de los datos de los clientes como ya se ha expuesto anteriormente.

SÉPTIMO: Sobre la vulneración del artículo 29 de la LRJSP.

XFERA ya había adoptado dichas medidas, antes incluso de la apertura del procedimiento sancionador: bastó un requerimiento de la SEAD para que realizase un nuevo análisis de riesgos e incrementase sus medidas de seguridad, reduciendo la incidencia de esta práctica de forma extraordinaria.

Por tanto, no se acredita por la Agencia que una sanción, de un importe tan relevante como 200.000'00 euros, sea "necesaria". Máxime, cuando dicho concepto ha sido interpretado por nuestro Tribunal Constitucional como la inexistencia de otra medida más moderada para la consecución del tal propósito con igual eficacia.

XFERA sigue mejorando sus medidas de forma proactiva habiéndose adoptado (entre otras) las siguientes decisiones:

> 1. Se ha añadido un nuevo elemento de seguridad en la solicitud de información a los clientes, reforzando así el procedimiento de autenticación:
>
> *"Importe de la última factura o recarga (en caso de no disponer de ella, remitirle a su área personal)"*
>
> Aporta las nuevas políticas de seguridad a efectos de identificación y autenticación de clientes de las marcas Yoigo, Másmóvil y Llamaya.
>
> 2. En el caso de la marca Yoigo, se ha impuesto un paso intermedio en la tramitación de duplicados de tarjeta SIM: solo se realizará una activación cuando exista un pedido incorporado a la plataforma de servicio postventa "Order Box", que utilizan para realizar sus gestiones las plataformas de atención al cliente, bien presenciales (tiendas) o telefónicas. A este respecto, se ha difundido un vídeo de concienciación sobre la problemática del SIM swapping, dirigido a todo el personal de atención al cliente de la marca.
>
> 3. También, en caso de detección de vulneración de los procedimientos previstos para la activación, solicitud o gestión de duplicados de SIM para cualquier marca estamos procediendo a penalizar a las plataformas de atención al cliente y tiendas que ascienden hasta 500 euros por cada duplicado de SIM gestionado incorrectamente.

Debe destacarse que la puesta en marcha de estos cambios en las políticas de seguridad ha dado como resultado un cambio en el comportamiento por parte de los delincuentes, que buscan otras vías de llevar a cabo el fraude evitando las políticas de seguridad. Pone como ejemplo, el incidente que afectó a uno de sus encargados del tratamiento, la empresa finlandesa de servicios en la nube QVANTEL FINLAND OY, que les notificó la pasada semana un ataque de fuerza bruta contra sus servidores que se vio acompañado de un envío masivo de ***EMPRESA.1 electrónicos de phishing contra muchas de las tiendas, así como llamadas desde números ocultos suplantando al soporte del canal, con la intención de obtener credenciales del aplicativo de servicio postventa y del TPV de la marca Yoigo. A pesar de que no hay constancia de exfiltración de datos, el incidente afectó a la disponibilidad del sistema durante unas horas, y fue notificado a la Agencia el pasado día 10; habiendo recibido el número de registro de entrada ***NÚMERO.4***. Actualmente, una vez contenido el ataque, siguen analizando lo acontecido en la última semana para entender el nuevo modus operandi.

Considera que la acción de la Agencia debería ir encaminada a instar a las entidades bancarias a avanzar en otra línea, sin hacer recaer la responsabilidad exclusivamente sobre unos operadores de telecomunicaciones que son víctimas de este tipo de delitos. Mientras las entidades financieras no refuercen sus sistemas de autenticación, los operadores de telecomunicaciones, afirma, van a seguir recibiendo ataques para conseguir ilícitos objetivos por parte de delincuentes que no se amilanan ante una política de seguridad reforzada.

El artículo 29.3 de la LRJSP, que invoca, dice:

3. En la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá observar la debida idoneidad y necesidad de la sanción a imponer y su adecuación a la gravedad del hecho constitutivo de la infracción. La graduación de la sanción considerará especialmente los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza de los perjuicios causados.

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

Debe traerse a colación lo dispuesto en el considerando 11 del RGPD:

La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

En el considerando 148 del RGPD:

A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

Y el considerando 150 del RGPD que señala:

A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de

> *la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. (…).*

A mayor abundamiento, el artículo 29.2 de la LRJSP también configura la función desalentadora o disuasoria de las multas al indicar que "*El establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el cumplimiento de las normas infringidas".*

Hay que destacar el artículo 83.1 del RGPD donde se establece el ejercicio de la potestad sancionadora al señalar que:

> *Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.*

En similar sentido se pronuncia el artículo 58.2.i) del RGPD, cuando dice que la autoridad de control tiene el poder de:

> *i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;*

También el artículo 83.5 del RGPD dice:

> *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*: (…)

El denominado Grupo del artículo 29, sustituido por el Comité Europeo de Protección de Datos-, en las "Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679" WP 253, dice:

> *(…) las multas administrativas deben responder adecuadamente a la naturaleza, la gravedad y las consecuencias de la violación, y las autoridades de control deben evaluar todos los hechos del caso de una manera coherente y objetivamente justificada. La evaluación de lo que es efectivo, proporcionado y disuasorio en cada caso también deberá reflejar el objetivo perseguido por la medida correctiva seleccionada, ya sea restablecer el cumplimiento de la normativa o castigar un comportamiento ilícito (o ambos).*

También aclara que para lograr tal disuasión se debe utilizar la definición del concepto de empresa:

> *Para imponer multas efectivas, proporcionadas y disuasorias, la autoridad de control debe utilizar la definición del concepto de empresa prevista por el TJUE a los efectos de la aplicación de los artículos 101 y 102 del TFUE, a saber, que el concepto de empresa debe entenderse como una unidad económica que puede estar formada por la sociedad matriz y todas las filiales participantes. De acuerdo con el Derecho y la jurisprudencia de la UE4 , una empresa debe ser entendida como una unidad económica que lleva a cabo actividades co-*

merciales/económicas, con independencia de la persona jurídica de que se trate (considerando 150).

XFERA, en cuanto a "Tipo de empresa" está catalogada como "Matriz de grupo" y en cuanto al "Tamaño UE" se cataloga como "Corporate" ("Corporativa" -la traducción es nuestra-) y cuenta con 473 empleados, según los datos declarados en el ejercicio 2019.

Así, el establecimiento de la multa se ha basado en una evaluación de todas las circunstancias pertinentes del caso y se considera que es eficaz, proporcionada y disuasoria respecto a los Hechos Probados, teniendo en cuenta los elementos de graduación aplicados conforme al artículo 83.2 del RGPD.

A este respecto, la Sentencia del TJUE, de 13 de junio de 2013, Versalis Spa/Comisión, C-511/11, ECLI:EU:C:2013:386, dice:

"94. Respecto, en primer lugar, a la referencia a la sentencia Showa Denko/Comisión, antes citada, es preciso señalar que Versalis la interpreta incorrectamente. En efecto, el Tribunal de Justicia, al señalar en el apartado 23 de dicha sentencia que el factor disuasorio se valora tomando en consideración una multitud de elementos y no sólo la situación particular de la empresa de que se trata, se refería a los puntos 53 a 55 de las conclusiones presentadas en aquel asunto por el Abogado General Geelhoed, que había señalado, en esencia, que el coeficiente multiplicador de carácter disuasorio puede tener por objeto no sólo una «disuasión general», definida como una acción para desincentivar a todas las empresas, en general, de que cometan la infracción de que se trate, sino también una «disuasión específica», consistente en disuadir al demandado concreto para que no vuelva a infringir las normas en el futuro. Por lo tanto, el Tribunal de Justicia sólo confirmó, en esa sentencia, que la Comisión no estaba obligada a limitar su valoración a los factores relacionados únicamente con la situación particular de la empresa en cuestión."

"102. Según reiterada jurisprudencia, el objetivo del factor multiplicador disuasorio y de la consideración, en este contexto, del tamaño y de los recursos globales de la empresa en cuestión reside en el impacto deseado sobre la citada empresa, ya que la sanción no debe ser insignificante, especialmente en relación con la capacidad financiera de la empresa (en este sentido, véanse, en particular, la sentencia de 17 de junio de 2010, Lafarge/Comisión, C-413/08 P, Rec. p. I-5361, apartado 104, y el auto de 7 de febrero de 2012, Total y Elf Aquitaine/Comisión, C-421/11 P, apartado 82)."

En este sentido, el volumen de ventas declarado durante el año 2019 fue de 1.598.873.000'00 euros.

Efectivamente, se ha registrado en la Agencia una brecha de seguridad, con fecha 10 de enero de 2021, que ha afectado a (…) usuarios y corresponde a duplicados de SIM fraudulentos de eSIM, es decir, servicio en el que no existe una tarjeta SIM física, sino que se utiliza una tarjeta virtual en el móvil que se activa a través de un código QR que Yoigo envía al cliente.

Estos hechos, no hacen más que confirmar la importancia de la gestión del riesgo por parte del responsable del tratamiento.

El considerando 75 desarrolla el concepto de riesgo para los derechos y libertades como cualquier efecto o consecuencia no deseados sobre los interesados o no previsto en el propio tratamiento de datos personales, capaz de generar daños o perjuicios sobre sus derechos y libertades, particularizando, entre otros: los daños y perjuicios físicos, materiales o inmateriales, problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización, perjuicios económicos o sociales, privación a los interesados de sus derechos y libertades, que se les impida ejercer el control sobre sus datos personales, etc.

En conclusión, el foco de la gestión de riesgos en el RGPD es la protección de la persona, en su dimensión individual y social, como sujeto de los datos o afectado por el tratamiento.

Respecto a las decisiones adoptadas (1, 2 y 3), ya en la Resolución reconocimos que: *Amén de las medidas de seguridad implementadas con posterioridad a la comisión de los hechos probados y que son valoradas positivamente por esta Agencia, lo cierto es que la infracción se ha cometido.*

Asimismo, el artículo 118.1 de la LPACAP, dispone:

> *1. (…)*
>
> *No se tendrán en cuenta en la resolución de los recursos, hechos, documentos o alegaciones del recurrente, cuando habiendo podido aportarlos en el trámite de alegaciones no lo haya hecho. Tampoco podrá solicitarse la práctica de pruebas cuando su falta de realización en el procedimiento en el que se dictó la resolución recurrida fuera imputable al interesado.*

De modo que, siguiendo este precepto, la información referida ni afecta a la tipificación de los hechos ni a los factores atenuantes, ya valorados.

Por añadidura, la estafa SIM Swapping sigue presente y va en aumento. Muestra de ello son los datos recogidos en la Memoria 2021 de la Fiscalía General del Estado dedicado a la “Criminalidad informática” que dedica en su punto 8 una mención a las actuaciones fraudulentas online:

> *“En este breve repaso de las actuaciones fraudulentas online, es obligada la mención de las conductas que afectan al sector de las telecomunicaciones en sus distintas variantes, y muy relacionadas con ellas, aunque el perjuicio se genera en la banca online, el conocido vulgarmente como fraude de SIM Swapping, que está siendo utilizado con alarmante frecuencia en los últimos años. La técnica consiste en burlar las medidas de seguridad de las entidades bancarias accediendo a los códigos alfanuméricos de confirmación, de uso único, generados con ocasión de las transacciones electrónicas y que ordinariamente se comunican a los/as clientes a través de mensajes SMS. Para ello, los/as delincuentes obtienen previamente un duplicado o una nueva tarjeta SIM a nombre de su víctima, ya sea solicitándola del operador correspondiente, simulando la identidad de aquella, ya sea valiéndose de una metodología más elaborada, como en el supuesto objeto de instrucción judicial en Zamora, en el que se aprovechaba con esa finalidad un establecimiento de reparación de móviles. Una vez tienen la tarjeta SIM a su disposición, los delincuentes se garantizan la recepción en su propio dispositivo del código de confirmación de la transacción fraudulenta y, en definitiva, la posibilidad de hacer efectiva la misma en su be-*

neficio, evitando que en ese momento sea conocida por el perjudicado o perjudicada. Esta forma de defraudación ha generado en los últimos años múltiples investigaciones policiales y la incoación de procedimientos judiciales en distintos territorios como A Coruña y Valencia. Su efectividad y la facilidad con que los/as delincuentes logran sus ilícitos propósitos ha determinado la adopción por los operadores de telefonía de medidas específicas de prevención y fortalecimiento de las garantías para la emisión de estas tarjetas o de sus duplicados."

También otras Memorias de las Fiscalías Territoriales, por ejemplo:

- La Memoria de la Fiscalía de la Comunitat Valenciana -2021 (Ejercicio 2020)- informa:

  Se ha comenzado a incoar procedimientos judiciales por formas novedosas de fraudes como el SIM Swapping.

- Especial mención se hace en la Memoria de la Fiscalía de la Comunidad Autónoma del País Vasco -2021 (Ejercicio 2020)- que dice:

  Igualmente se ha constatado la existencia de cada vez más procedimiento de SIM Swapping, inexistentes hasta el momento, y que requieren cada vez más mayores medidas de control por parte de las compañías de telefonía móvil para la emisión de duplicados de tarjetas SIM.

- La Memoria de la Fiscalía de la Comunidad Autónoma de Andalucía -2021 (Ejercicio 2020)- informa:

  Destaca la Guardia civil en su informe anual, que se está produciendo una nueva variedad de estafa llamada sim swapping, en el que los autores doblan la tarjeta sim del perjudicado, siendo esta la llave para conseguir suplantar la identidad del perjudicado.

Para finalizar, el Informe 0030/2021 del Gabinete Jurídico de la AEPD dice:

Y por último debe indicase que corresponde a las operadoras de telecomunicaciones y a las entidades bancarias cumplir lo dispuesto en el RGPD en tanto responsables del tratamiento de los datos de sus clientes, y en especial establecer medidas para que el tratamiento sea leal, confidencial y se impida el acceso no autorizado por terceros a información personal, de acuerdo con lo indicado en los artículos 5.1f), 24 y 32 del RGPD, y 28.2 de la LOPDGDD, sin perjuicio de lo que corresponda a las entidades bancarias como proveedores de servicios de pago derivado del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

Por lo tanto, cabe concluir que, el principio de proporcionalidad de las sanciones, como señalan las SSTS, Sala 3ª, de 3 de diciembre de 2008 (Rec. 6602/2004) y 12 de abril de 2012 (Rec. 5149/2009) es el fundamental que late y preside el proceso de graduación de las sanciones e implica, en términos legales, "*su adecuación a la gravedad del hecho constitutivo de la infracción*" como dispone el artículo 29.3 de la LRJSP, dado que toda sanción debe determinarse en congruencia con la entidad de la infracción cometida y según un criterio de proporcionalidad en relación con las circunstancias del hecho.

Pues bien, de conformidad con las consideraciones expuestas, estima la Agencia que

la resolución sancionadora no ha infringido el principio de proporcionalidad en la determinación de la sanción impuesta, que resulta ponderada y proporcionada a la gravedad de la infracción cometida y la entidad de los hechos, sin que se aprecien razones que justifiquen su minoración.

Por todo lo expuesto, la alegación relativa a la vulneración del artículo 29 de la LRJSP debe ser desestimada.

OCTAVO: Sobre la solicitud de aplicación del artículo 29.4 de la LRJSP.

De forma subsidiaria a lo expuesto, y habida cuenta de las circunstancias concurrentes en el caso y de los esfuerzos realizados por XFERA para poner solución a los hechos supuestamente constitutivos de infracción, se solicita la aplicación del citado artículo al caso que nos ocupa, reduciendo la sanción a una cuantía no superior a 100.000'00 euros (esto es, la mitad de la impuesta, toda vez que las cuantías de las sanciones previstas en el artículo 83.4.a), inferior en grado al 83.5.a) aplicado, son inferiores en un 50%.

El artículo 29.4 de la LRJSP, dispone:

> *4. Cuando lo justifique la debida adecuación entre la sanción que deba aplicarse con la gravedad del hecho constitutivo de la infracción y las circunstancias concurrentes, el órgano competente para resolver podrá imponer la sanción en el grado inferior.*

En este sentido, no ha lugar a la petición deducida por cuanto la resolución sancionadora resulta conforme con el principio de proporcionalidad en la determinación de la sanción impuesta, que resulta ponderada y proporcionada a la gravedad de la infracción cometida y la entidad de los hechos, y debidamente motivada, teniendo en cuenta la cuantía a la que puede ascender dicha sanción de conformidad con el artículo 83.5.a) del RGDP, que prevé para la infracción del artículo 5 del RGDP, "*multas administrativas de 20.000.000 € 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*".

NOVENO: Sobre la solicitud de suspensión de la ejecución del acto recurrido.

Alude la parte recurrente al artículo 117.2.b) de la LPACAP, sin embargo, es el artículo 90.3 de la LPACAP, bajo el epígrafe "Especialidades de la resolución en los procedimientos sancionadores", el que dispone la ejecutividad de la resolución y posibilita la suspensión cautelar de la ejecución de la resolución:

> *3. La resolución que ponga fin al procedimiento será ejecutiva cuando no quepa contra ella ningún recurso ordinario en vía administrativa, pudiendo adoptarse en la misma las disposiciones cautelares precisas para garantizar su eficacia en tanto no sea ejecutiva y que podrán consistir en el mantenimiento de las medidas provisionales que en su caso se hubieran adoptado.*
>
> *Cuando la resolución sea ejecutiva, se podrá suspender cautelarmente, si el interesado manifiesta a la Administración su intención de interponer recurso contencioso-administrativo contra la resolución firme en vía administrativa. Dicha suspensión cautelar finalizará cuando:*
>
> *a) Haya transcurrido el plazo legalmente previsto sin que el interesado haya interpuesto recurso contencioso administrativo.*
>
> *b) Habiendo el interesado interpuesto recurso contencioso-administrativo:*

1.º No se haya solicitado en el mismo trámite la suspensión cautelar de la resolución impugnada.

2.º El órgano judicial se pronuncie sobre la suspensión cautelar solicitada, en los términos previstos en ella.

Según lo expuesto, la sanción será ejecutiva desde el momento en que no quepa recurso ordinario en vía administrativa. En concreto, en el caso analizado, dado que se ha interpuesto el recurso potestativo de reposición, la resolución sancionadora carece de ejecutividad mientras no se resuelva el recurso administrativo dirigido contra ella.

Cuando la resolución sea ejecutiva, se podrá suspender cautelarmente, si XFERA manifiesta a la Agencia su intención de interponer recurso contencioso-administrativo contra la resolución firme en vía administrativa, circunstancia no manifestada en el presente caso.

DÉCIMO: Sobre la publicidad de la resolución.

Alega XFERA respecto a la información que consta en la Resolución, la necesidad de evaluar su publicidad dada la existencia de información clasificada como “Confidencial” y que podría ser utilizada con fines delictivos.

Según lo establecido en el artículo 50 de la LOPDGDD bajo el epígrafe ”Publicidad”:

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Así, la publicación de determinadas resoluciones de la AEPD viene impuesta por la LOPDGDD.

El artículo 50 de la LOPDGDD no dispone la publicidad de la resolución como una sanción.

La finalidad de esta publicidad no es sancionar públicamente al infractor, sino aplicar el principio de transparencia y facilitar el conocimiento a la ciudadanía de la actividad desarrollada por la AEPD.

En este sentido, el artículo 11 del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos establece, bajo el epígrafe “Transparencia y publicidad”, que:

1. La Agencia Española de Protección de Datos publicará en su página web las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y las que impongan medidas cautelares.

2. Sin perjuicio de lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, será igualmente obje-

to de publicación en la página web toda aquella información que la Presidencia considere relevante y que contribuya al mejor cumplimiento de sus funciones.

Además, se comprueba con facilidad cuál es la finalidad de la publicación de las resoluciones de la AEPD si se tiene en cuenta que las que se publican no son únicamente aquellas en las que se puede llegar a sancionar, sino que se incluyen las tutelas de derechos, cualquier otra que ponga fin a los procedimientos de reclamación (que pueden terminar o no, en la imposición de una sanción), las que archiven actuaciones previas de investigación, impongan medidas cautelares o las que fije el Estatuto.

Así, es una garantía para la ciudadanía en los términos del artículo 45.1 de la LPACAP que dice:

1. Los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente.

Es obligada, por tanto, la publicación de la resolución administrativa, tal y como impone la Ley al señalar literalmente que "*publicará*" (artículo 50 LOPDGDD).

Al publicar la resolución en los términos del citado artículo se consuma el interés general encomendado a la AEPD. Eso sí, previa anonimización y detracción de las cuestiones confidenciales o de secreto intelectual e industrial.

En cuanto a la jurisprudencia sobre solicitud de medidas cautelares y publicación de resoluciones sancionadoras, por todas, cabe citar el Auto del Tribunal Supremo de 31 de marzo de 2015, Secc. 2ª, Recurso: 73/2015, y las diversas resoluciones que en dicho auto se citan.

PRIMERO.- Por la entidad mercantil "Western Union Payment Servicies Ireland Limited (WUPSIL)" se solicita en este incidente la adopción de la medida cautelar <<consistente en la suspensión de la ejecutividad de las sanciones de amonestación pública>> impuestas en la Orden del Ministerio de Economía y Competitividad de 2 de diciembre de 2014 por la comisión de una infracción grave, y en el Acuerdo del Consejo de Ministros de 12 de diciembre de 2014 por la comisión de una infracción muy grave, en materia de prevención de blanqueo de capitales. Dicha entidad recurrente constriñe su solicitud de suspensión a las sanciones de amonestación, sin que extienda su petición ni formule alegaciones respecto de la suspensión de las sanciones económicas, sobre las que nada se interesa en vía cautelar.

*SEGUNDO.- Limitado pues nuestro análisis a la suspensión de la publicidad de las sanciones de amonestación pública**,** impuestas por el Consejo de Ministros por la comisión de una infracción muy grave, afirma la entidad recurrente que procede la medida cautelar por cuanto la ejecución de la sanción haría perder su finalidad al recurso, dado el daño reputacional que sufriría la entidad -se afirma- que afectaría a sus relaciones de servicio de pago con entidades de crédito y a las relaciones con sus actuales clientes y agentes, dada la gravedad de la conductas imputadas, cuya sanción se tacha de <desproporcionada>, a lo que añade la inexistencia de perturbación de los intereses generales y de tercero, el transcurso de varios años desde las conductas sancionadas y el refuerzo del control interno para evitar situaciones similares de futuro.*

Pues bien, el planteamiento de la pretensión cautelar no puede ser acogida. Como hemos sostenido de modo reiterado a este respecto (entre otras, en la

Sentencia de 14 de noviembre de 2002 -RC 8351/1999 - y en las que en ella se citan, y en los Autos de 17 de febrero de 2010 PMC 613/2009 con cita del Auto de 4 de mayo de 2005), la Administración Pública actúa en un régimen de publicidad de sus actos con carácter general y, de modo específico, tanto más cuanto así lo establezcan las normas reguladoras de cada sector del ordenamiento. En concreto, el Legislador ha querido mediante la Ley 19/1993, sobre medidas de prevención del blanqueo de capitales (artículo 12.2), que la publicidad de las sanciones impuestas a las entidades financieras en esta materia se atenga a lo dispuesto en la Ley 26/1988, de 29 de julio, de Disciplina e Intervención de las Entidades de Crédito. Ley cuyo artículo 27.5 dispone que las sanciones por infracciones muy graves serán publicadas en el Boletín Oficial del Estado una vez que sean firmes. La firmeza a la que se refiere el precepto legal es aquella que se produce cuando se ha agotado la vía administrativa, como en este caso ocurre. Semejante decisión legislativa corrobora que existe un indudable interés público en la citada publicación, que por lo demás no viene a descubrir ningún dato que deba mantenerse oculto, pues las sanciones impuestas a las entidades de crédito o a quienes ejerzan cargos de administración o dirección en ellas han de ser, además, objeto de comunicación a la inmediata Junta o Asamblea General que se celebre, lo que implica asimismo la publicidad general de aquéllas. La publicación de la resolución sancionadora atiende, pues, al interés público y resulta preceptiva por mandato legal. Hemos descartado en sentencias anteriores sobre esta misma cuestión que la mera publicación de los acuerdos sancionadores tenga, de suyo, el carácter irreversible que propiciaría la adopción de la medida cautelar para no privar de sentido al proceso mismo: la publicación de un eventual fallo estimatorio en el fondo, o la mención de que la sanción impuesta es susceptible aún de recurso jurisdiccional, bastan para impedir esos pretendidos efectos irreversibles. (…)

La tesis no puede ser acogida pues, como ya hemos indicado en diversas ocasiones, (por todos, ATS de 17 de febrero de 2010, R. 613/2009) la transparencia en los mercados financieros y aún los intereses de los clientes actuales y potenciales no se compadecen con el ocultamiento de un hecho relevante cual es el que las autoridades supervisoras han sancionado, tras un procedimiento contradictorio, una determinada conducta en la actividad bancaria como la que se realiza. Concurre un evidente interés público en que tales hechos se pongan en conocimiento del mercado, una vez que responden a decisiones administrativas firmes en la vía administrativa precedida de un análisis de la conducta por parte de los organismos supervisores, con intervención de la entidad sancionada. De acoger la tesis de la recurrente, supondría que toda publicidad de la sanción impuesta a una entidad financiera por infracciones relacionadas con la prevención del blanqueo de capitales puede eventualmente surtir aquellos efectos. La índole de la infracción imputada y la naturaleza de la amonestación no tienen por qué afectar de forma irreversible a los intereses de la entidad amonestada. Por lo demás, y como hemos indicado en el Auto de 13 de marzo de 2009 (PMC 21/2009) a las razones expuestas puede añadirse que, en evitación de las consecuencias que teme que se produzcan, siempre podrá argüir que la sanción impuesta no es firme judicialmente, en la medida en que está sometida al presente recurso contencioso administrativo ante esta Sala, que en su momento deberá pronunciarse sobre su conformidad a derecho mediante la correspondiente sentencia definitiva.

TERCERO. - Procede, en consecuencia, rechazar la petición cautelar interesada, (…)

En consecuencia, la publicación de la resolución en la web de la AEPD deviene obligatoria por imposición legal.

De lo hasta aquí expuesto, debe concluirse que la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación, la directora de la AEPD RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ***XFERA MÓVILES, S.A.*** contra la resolución de esta AEPD dictada con fecha 10 de noviembre de 2021, en el procedimiento sancionador PS/00027/2021.

SEGUNDO: DESESTIMAR la solicitud de suspensión sobre la ejecución de la Resolución, de fecha 10 de noviembre de 2021, por la que se acuerda imponer a XFERA, por una infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD, una multa de 200.000’00 euros (doscientos mil euros).

TERCERO: NOTIFICAR la presente resolución a XFERA.

CUARTO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la LPACAP, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el artículo 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la AEPD en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDPGDD, la presente resolución se hará pública una vez haya sido notificada al interesado.

Contra esta resolución, que pone fin a la vía administrativa conforme al artículo 48.6 de la LOPDPGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer 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.

Finalmente, se señala que conforme a lo previsto en el artículo 90.3 a) LPACAP, se

podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la AEPD, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el artículo 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo y aquella donde conste la solicitud de la suspensión cautelar de la resolución impugnada. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-100519

Mar España Martí
Directora de la AEPD