Expediente N.º: PS/00027/2021

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos (en lo sucesivo, AEPD) y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte RECLAMANTE UNO), en fecha 3 de octubre de 2019, presenta un escrito en la Oficina de ***EMPRESA.1 de Granada, que es registrado en la AEPD en fecha 8 de octubre de 2019, mediante el cual interpone una reclamación dirigida contra ***XFERA MÓVILES, S.A. (MÁSMÓVIL)***, con NIF ***A82528548*** (en adelante, XFERA), por los siguientes motivos:

*"(…) Primero. En fecha 25 de septiembre 2019 YOIGO generó un duplicado de tarjeta de mi teléfono *****TELEFONO.1** siendo que esta parte no lo había solicitado y siendo que se han cedido ilícitamente mis datos personales, incluidos los bancarios.*

Segundo. La actuación anterior es contraria a los principios reguladores del tratamiento de los datos personales previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: a este efecto constan cometidas al menos, las siguientes infracciones:

El irregular tratamiento de los datos personales con conculcación de los principios de consentimiento e información del artículo 6, de la Ley Orgánica 3/2018, de 5 de diciembre.

El incumplimiento doloso del deber de secreto del artículo 5 de la misma norma orgánica.

La vulneración de los principios básicos del tratamiento según previsión de la letra a) del número 5 del art. 83 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. (…)"

Junto a la reclamación aporta dos denuncias presentadas ante la Dirección General de la Policía Nacional en las dependencias de Granada Centro, denunciando estos hechos.
En la primera de las denuncias con número de atestado ***XXXX/XX,*** de fecha 26 de septiembre de 2019, manifiesta:

*"(…) 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 **B.B.B.** 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 **C.C.C.** 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 **B.B.B.**, 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 **D.D.D..***

--Que toda esta 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, (**B.B.B.**), 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 telefónica 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 de las transacciones realizadas no

autorizadas.

De acuerdo con lo previsto en el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD), que consiste en dar traslado de las mismas a los Delegados de Protección de Datos designados por los responsables o encargados del tratamiento, o a éstos cuando no los hubieren designado, y con la finalidad señalada en el referido artículo, en fecha 26 de noviembre de 2019, se dio traslado de la reclamación a XFERA para que procedieran a su análisis y dieran respuesta en el plazo de un mes.

XFERA, no dio respuesta a este requerimiento, notificado en fecha 26 de noviembre de 2019, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 11 de febrero de 2020, en el expediente con núm. de referencia ***E/11270/2019***.

SEGUNDO: ***E.E.E.*** (en adelante, la parte RECLAMANTE DOS), en fecha 5 de noviembre de 2019, interpuso una reclamación ante la AEPD dirigida contra XFERA, por los siguientes motivos:

*"Se reclama a la empresa MÁSMÓVIL con CIF **A20609459**, que en el día 10/07/2019 se le hizo sin su consentimiento en alguna Tienda de móviles un duplicado de la tarjeta SIM llevando esto a un fraude bancario en el banco (ING) por lo que considero que la empresa MÁSMÓVIL ha infringido la ley de protección de datos.*

Por lo que aporto la documentación pertinente de los hechos ocurridos.

1) denuncia y ampliación de la denuncia.

2) importes de lo sustraído

3) email de MÁSMÓVIL como que se hizo un duplicado de la tarjeta SIM el día 10/07/2019 a la 16:46h

4) denuncia en el ministerio de economía y empresa (consumo)

5) reclamación desestimada por parte de MÁSMÓVIL de los hechos ocurridos (como que no quieren saber nada)

*Los importes han sido abonados (devueltos) por la entidad ING gracias a lo ocurrido en la ampliación de la denuncia. Si no llega a ser por el Mosso d'Escuadra nº *****NÚMERO.2** que se puso en contacto conmigo para explicarme como se me hizo el fraude, tanto ING como MÁSMÓVIL no me hubieran devuelto los importes sustraídos, (…)*

Por lo que reclamo una indemnización por vulnerar la ley de protección de datos y las molestias y trastornos ocasionados para solucionar todo este problema , así como las pertinentes sanciones a la compañía MÁSMÓVIL (…)"

Junto a la reclamación aporta dos denuncias presentadas ante la Dirección General de la Policía Nacional en las dependencias de Móstoles, denunciando estos hechos.

En la primera de las denuncias con número de atestado ***RRRRR/RR,*** de fecha 11 de julio de 2019, manifiesta:

> *"Que el denunciante manifiesta que ha observado en su número de cuenta* ******CUENTA.1*** *de la entidad ING dos cargos que él no ha realizado ni autorizado.*
>
> *Que los movimientos han sido realizados con la tarjeta con número* ******TARJETA.1*** *la cual está asociada a la cuenta arriba referida, siendo los movimientos los siguientes:*
>
> *El día 10/07/2019, disposición en cajero número* ******CAJERO.1****, por un valor de 1700 euros.*
>
> *El día 10/07/2019, disposición en cajero número* ******CAJERO.1****, 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 ***SSSSS/SS,*** de fecha 29 de julio de 2019, manifiesta:

> *"Que las presentes son ampliatorias del atestado número* ***RRRRR/RR*** *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.2*** *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 "MÁSMÓVIL" 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. (…)"

En fecha 10 de diciembre de 2020, se dio traslado de la reclamación a XFERA, para que procediera a su análisis y diera respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, XFERA manifestó -como único argumento- lo siguiente:

"Único.- Insuficiente información.

La reclamación recibida hace referencia a presuntos hechos delictivos consistentes en duplicar una tarjeta SIM como medio para llevar a cabo un fraude bancario y que se habrían producido en "(…)".

Naturalmente este tipo de conductas caen completamente fuera de la actividad propia y de ningún modo se pueden producir desde la actuación ordinaria de los protocolos de atención y gestión establecidos en la compañía.

No obstante, ante la gravedad de los hechos se ha intentado procurar alguna información al respecto, pero debido a la falta de indicaciones en la reclamación recibida no es posible aportar ninguna información complementaria fuera de manifestar el deseo de plena colaboración para el caso de que fuera posible concretar con mayor precisión lo que se solicite."

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 23 de febrero de 2020, en el expediente con núm. de referencia ***E/11591/2019.***

Dicha resolución fue objeto de una rectificación de errores en fecha 5 de marzo de 2020.

TERCERO: Con fecha 27 de noviembre de 2019, la directora de la AEPD, ante las noticias aparecidas en medios de comunicación relativas a la utilización de prácticas fraudulentas basadas en la generación de duplicados de tarjetas SIM sin el consentimiento de sus legítimos titulares con objeto de acceder a información confidencial con fines delictivos (conocidas como "SIM Swapping"), insta a la Subdirección General de Inspección de Datos (en lo sucesivo, SGID) a iniciar de oficio las Actuaciones Previas de Investigación tendentes a analizar estas prácticas y las medidas de seguridad existentes para su prevención.

A saber:

El timo de la SIM duplicada: si su teléfono hace cosas raras, revise la cuenta bancaria | Economía | EL PAÍS (elpais.com)
https://elpais.com/economia/2019/05/21/actualidad/1558455806_935422.html

La peligrosa estafa de moda: Duplicar tu número de móvil para vaciarte la cuenta del banco | Tecnología (elmundo.es)
https://www.elmundo.es/tecnologia/2020/10/15/5f8700b321efa0c9118b462c.html

CUARTO: A la vista de los hechos denunciados por las partes RECLAMANTES UNO y DOS, de los documentos aportados y de la Nota Interior acordada por la directora de la Agencia, la SGID procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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 (Reglamento general de protección de datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

En el marco de las actuaciones previas de investigación se practicaron tres requerimientos de información dirigidos a XFERA, en distintas fechas:

Requerimiento	Código Seguro de Verificación	Fecha requerimiento	Fecha notificación requerimiento
Primero	***CSV.1**	13/01/2020	16/01/2020
Segundo	***CSV.2**	18/06/2020	19/06/2020
Tercero	***CSV.3**	18/09/2020	18/09/2020

En el primero de los requerimientos, de fecha 13 de enero de 2020, se solicitaba la siguiente información:

1. Información sobre las vías de que disponen los clientes para solicitar un duplicado de tarjeta SIM. (Teléfono, Internet, tiendas, etc.).

2. Para cada una de las vías de que se disponga, se pide información detallada del procedimiento establecido para la atención de las solicitudes, incluyendo los controles para la verificación de la identidad del solicitante incluyendo los datos y documentos que se requieren al solicitante, así como el detalle de las verificaciones que se realizan sobre los mismos. En caso de envío de tarjeta SIM por correo, detalle de los controles y exigencias establecidas sobre la dirección de envío.

3. Instrucciones giradas al respecto al personal que atiende las solicitudes para la atención de las mismas. Documentación que acredite su difusión entre los empleados dedicados a dichas tareas, internos o externos a la entidad.

4. Información sobre si la realización de los controles para la verificación de la identidad queda reflejada, para cada solicitud atendida, en el Sistema de Información de la entidad. Documentación que lo acredite en su caso, tal como impresión de pantalla de los botones (check-box) u otra documentación según el método utilizado.

5. Motivos por los cuales ha sido posible en algunos casos la suplantación de la identidad de clientes para la emisión de duplicados de SIM. Razones por las cuales las medidas y controles de seguridad implementados no han surgido efecto.

6. Acciones emprendidas por la entidad cuando se detecta uno de estos casos. Información sobre la existencia de un procedimiento escrito y copia del mismo en

caso afirmativo. Acciones emprendidas para evitar que casos de este tipo se vuelvan a producir, en concreto, cambios que se hayan podido realizar sobre el procedimiento para mejorar la seguridad.

7. Número de casos de solicitudes fraudulentas de duplicados de SIM detectados durante todo el año 2019.

8. Número de clientes de telefonía móvil total de la entidad.

En el segundo de los requerimientos, de fecha 18 de junio de 2020, se solicitaba la siguiente información:

PUNTO 1

Se solicita aclaración sobre los siguientes aspectos con relación a la contestación de nuestro requerimiento de fecha 16 de enero de 2020, en el marco de este mismo expediente:

A) En el caso de la marca YOIGO se indica que (…).

Se pide copia del procedimiento por escrito donde consten todos los casos que se tramitan (…), incluyendo todos los supuestos o circunstancias aludidas.

Se pide copia de las instrucciones concretas dadas a los operadores con información detallada de cómo valora el operador todos los supuestos, incluyendo cómo debe valorar las circunstancias del cliente para acceder a la tramitación telefónica.

B) En los casos de las marcas LLAMAYA y LEBARA se indica que (…).

Se pide igualmente copia del procedimiento por escrito donde consten todos los casos que se tramitan (…), incluyendo todos los supuestos, y copia de las instrucciones concretas dadas a los operadores con información detallada de cómo valora el operador que el cliente no pueda acudir a un punto de venta.

C) En el caso de la marca MÁSMÓVIL confirmación de (…).

D) En su escrito de contestación se alude a la política de seguridad que debe pasar el cliente en las solicitudes telefónicas. Se pide copia de las políticas de seguridad de todas las marcas, donde consten claramente los datos que se solicitan según los diferentes casos, incluyendo todos los supuestos.

Se pide copia de las instrucciones concretas dadas a los operadores para ello con información detallada de los datos que deben pedir en cada caso.

C^2) Sobre el proceso de solicitud (…) de LLAMAYA:

Se pide información sobre si se remite a (…).

Información sobre si el cliente puede fijar una dirección de entrega distinta de la habitual, como parece desprenderse de la información facilitada.

Para todas las marcas, en las tramitaciones (…), se pide información sobre si es posible cambiar la dirección de entrega de la SIM y bajo qué circunstancias.

D^2) Comprobaciones que se realizan en la entrega a domicilio de la tarjeta SIM para la identificación del destinatario. Copia de la documentación contractual con las empresas de logística/mensajería que realizan el reparto, donde consten las comprobaciones de identidad que debe realizar el repartidor.

PUNTO 2

Listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes. El listado incluirá los duplicados de SIM solicitados desde el 1 de enero de 2020, es decir, todos los reclamados que sucedieron a partir del 1 de enero, desde el primero, consecutivos hasta llegar a 20.

Se pide indicar en el listado la fecha, el número de línea y el canal de la solicitud.

PUNTO 3

Sobre casos presentados ante esta Agencia que se resumen en la tabla:

Ref. EXPEDIENTE	FECHA HECHOS	HECHOS	DATOS CLIENTE
E/11270/2019 y ***E/1422/2020***	25/09/2019	Duplicado SIM En oficina YOIGO	- ***A.A.A.*** - DNI ******NIF.1*** - Tel. ******TELEFONO.2***
E/*11591*/2019	10/07/2019	Duplicado SIM Oficina MÁSMÓVIL	- ***E.E.E.*** - DNI ******NIF.2*** - Tel. ******TELEFONO.3***

Se pide:

A) Copias de los DNI recabados en la solicitud de duplicado de SIM. En caso de que no exista copia recabada, reflejo que conste en los sistemas de la solicitud y comprobación de la identidad del solicitante mediante exhibición de su DNI.

B) Información sobre si se tiene como requisito para la entrega que la ciudad donde se solicita la SIM sea la ciudad de residencia del cliente. Información sobre si existe algún control adicional en caso de ciudades distintas.

C) Acciones emprendidas por XFERA en cada caso, incluyendo acreditación documental de los siguientes aspectos:

- Si se ha marcado como víctima de fraude al cliente para evitar posibles intentos de suplantación de identidad futuros.
- Si se han realizado investigaciones internas para esclarecer los hechos con el punto de venta.
- Si se ha contactado con el cliente para alertarle de lo sucedido y sobre la resolución de su caso.

En el tercero y último de los requerimientos, de fecha 18 de septiembre de 2020, se solicitaba la siguiente información:

PUNTO 1

Sobre el listado de 20 casos de duplicados de SIM denunciados/reclamados facilitados en la contestación anterior:

FECHA	MSISDN	MARCA	CANAL
05/01/2020	******TELEFONO.4***	MásMóvil	Telefónico

14/01/2020	***TELEFONO.5**	Yoigo	Tienda
15/01/2020	***TELEFONO.6**	MásMovil	Telefónico
20/01/2020	***TELEFONO.7**	MásMóvil	Telefónico
25/01/2020	***TELEFONO.8**	Yoigo	Telefónico
27/01/2020	***TELEFONO.9**	MásMóvil	Telefónico
27/01/2020	***TELEFONO.10**	Yoigo	Tienda
28/01/2020	***TELEFONO.11**	Yoigo	Tienda
04/02/2020	***TELEFONO.12**	Yoigo	Telefónico
25/02/2020	***TELEFONO.13**	Yoigo	Telefónico
27/02/2020	***TELEFONO.14**	Yoigo	Telefónico
29/02/2020	***TELEFONO.15**	Yoigo	Telefónico
03/03/2020	***TELEFONO.15**	Yoigo	Telefónico
05/03/2020	***TELEFONO.16**	Yoigo	Telefónico
05/03/2020	***TELEFONO.12**	Yoigo	Telefónico
11/03/2020	***TELEFONO.17**	Yoigo	Tienda
13/03/2020	***TELEFONO.18**	Yoigo	Telefónico
03/04/2020	***TELEFONO.19**	MásMóvil	Telefónico
04/04/2020	***TELEFONO.20**	MásMóvil	Telefónico
08/04/2020	***TELEFONO.21**	Yoigo	Tienda
12/04/2020	***TELEFONO.22**	Yoigo	Telefónico

A. Se pide, en los casos de (…):

- Copia de los DNI o documentos identificativos aportados por los solicitantes del cambio de SIM.

- Para los clientes de YOIGO, copia del documento firmado por el solicitante para el nuevo SIM.

B. Para los casos de (…):

- Copia de la grabación de la conversación donde el solicitante del SIM supera la política de seguridad.

- Copia de la grabación de la conversación donde el solicitante de la activación del SIM supera la política de seguridad.

- Detalle de las circunstancias que concurrieron para para acceder a la tramitación de la solicitud telefónica.

PUNTO 2

Sobre el caso ref ***E/11591/2019***, relativo a ***E.E.E.***, DNI ***NIF.2***, línea ***TELEFONO.3***, se pide:

- Canal por el que se solicitó y se tramito el 10/07/2019 un cambio de SIM.

- Si el canal fue (…) aportar misma documentación que la que se requiere en el PUNTO 1. A del presente escrito, si fue (…), documentación requerida en el PUNTO 2. B.

PUNTO 3

A. Información sobre si es posible adquirir SIM sin asociarlos a ninguna línea o cliente. Información sobre si se permite que un cliente obtenga un SIM sin activar y sin asociar a una línea determinada, que posteriormente pueda activar telefónicamente y asociar a una línea.

Información si existe esta posibilidad, sin fraude de *SIM swapping*, consistente en la activación de un SIM que esté en posesión de un cliente, sin haber sido asociado previamente en los sistemas de la entidad a una línea de su titularidad.

B. Política de seguridad que se pasa al solicitante en la recogida del SIM cuando no se asocia a una línea o cliente durante su recogida (en caso de que sea posible).

PUNTO 4

Información sobre 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.

Se pide aportar:

A. Política de seguridad que se pasa al solicitante en los cambios de titularidad vía (…).

B. Copia de las instrucciones concretas que al respecto disponen los operadores.

C. Procedimiento de cambio de titularidad y requisitos pedidos a los solicitantes para ello.

QUINTO: Con fecha 29 de enero de 2020, XFERA solicita la ampliación del plazo para aducir alegaciones y aportar documentos u otros elementos de juicio.

Con fecha 31 de enero de 2020, por el inspector se acuerda la ampliación de plazo instada.

SEXTO: En respuesta a los tres requerimientos formulados, XFERA aportó la siguiente información que fue objeto de análisis por esta Agencia:

Respecto al primero de los requerimientos se especifica la información conforme a los apartados requeridos según el orden de numeración:

1.- Información sobre las vías de que disponen los clientes:

"(…)"

2.- Información detallada del procedimiento:

Procedimiento de solicitud de duplicado SIM para la marca YOIGO

CANAL PRESENCIAL

(…)

CANAL NO PRESENCIAL

(…)

Procedimiento de solicitud de duplicado SIM para la marca MÁSMÓVIL

CANAL PRESENCIAL

(…)

CANAL NO PRESENCIAL

(…)

Procedimiento de solicitud de duplicado SIM para la marca LLAMAYA

CANAL PRESENCIAL

(…)

CANAL NO PRESENCIAL

(…)

Procedimiento de solicitud de duplicado de la tarjeta SIM para la marca LEBARA

CANAL PRESENCIAL

(…)

CANAL NO PRESENCIAL

(…)

3.- Información sobre las instrucciones giradas a los operadores: consiste en pasar la política de seguridad tanto para solicitud como activación de SIM. Se verifica que dicha

política es:

(…)

Los representantes de XFERA manifiestan que a través de la herramienta ***HERRAMIENTA.1 se ha remitido a todos los agentes internos y externos los nuevos protocolos a seguir en el caso de que se solicite el duplicado de una tarjeta SIM.

Aportan los siguientes documentos:

- Captura de pantalla de la comunicación remitida a todos los agentes internos y externos sobre la existencia de estas políticas, indicando que esta comunicación se remitió a todos los proveedores externos con la finalidad de que lo transmitieran a sus empleados.

- Casos en que debe solicitarse por parte de los operadores telefónicos o a través de los canales presenciales la aprobación de la política de seguridad de todas las empresas del Grupo MÁSMÓVIL para el duplicado de las Tarjetas SIM.

- Procedimiento de MÁSMÓVIL para solicitar un duplicado de Tarjeta SIM.

- Procedimiento de YOIGO para solicitar un duplicado de Tarjeta SIM.

Todos estos procedimientos tienen en común la necesidad de que el usuario facilite la misma información que se dio a XFERA en el momento de la contratación o de la venta de la Tarjeta SIM prepago.

En ningún caso se facilita al cliente información, limitándose los operadores de XFERA a realizar dicha comprobación.

Aportan copia de dos recordatorios remitidos sobre la política y procedimientos a seguir.

4.- Información sobre la realización de los controles:

Controles y exigencias establecidas sobre la dirección de envío para la remisión de tarjetas SIM por correo.

Al margen de las especialidades que ya se han detallado para cada marca, con carácter general se cumplen los siguientes aspectos:

(…)

Aportan copia de ejemplos de los Albaranes de Entrega.

(…)

Durante el año 2019 se ha reforzado en diferentes momentos el protocolo a seguir en el caso de Duplicado de SIM en el canal presencial para las distintas marcas.

Las actuaciones, tendentes a asegurar los derechos de los clientes, más relevantes durante el año 2019 han sido las siguientes realizadas por cada una de las marcas:

(…)

Aportan grabación "(…)" como un ejemplo de grabación de solicitud de duplicado de SIM de MÁSMÓVIL para acreditar los controles que se han implantado.

5.- Motivos por los cuales ha sido posible en algunos casos la suplantación de la identidad de clientes:

Los casos en que se ha podido producir este tipo de actuaciones pese a los controles establecidos son los siguientes:

(…)

6.- Acciones emprendidas por la entidad:

Aportan impresión de procedimiento distribuido entre los equipos de Atención al cliente. En él se especifica el seguimiento que se realiza cuando el departamento de fraude detecta una posible suplantación de identidad. (…).

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, (…).

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.

Indican que el 28 de noviembre de 2019 se abrió el servicio en 24x7 en la plataforma Control de Servicio. Aportan el manual de procedimiento actual. En él se aprecian diversas actuaciones, (…). También se analizan los últimos (…), y si no la hay se contacta con el cliente para confirmar.

Manifiestan que con la finalidad de demostrar el establecimiento de los controles, aportan tres grabaciones de las conversaciones telefónicas con el cliente durante el proceso de monitorización para verificación:

- Llamada de verificación tras alarma: con el resultado de falso positivo.

- Llamada de verificación tras alarma: con el resultado positivo y fraude confirmado.

- Llamada recibida para restablecimiento de servicio tras bloqueo preventivo, motivado por análisis de alerta sin haber podido verificar con el cliente.

También se exponen en el procedimiento algunos rasgos identificativos de un posible cambio de SIM fraudulento, tales como el cambio a formato electrónico de la factura, cambio de cuenta de correo electrónico, eventos previos al cambio de SIM con llamadas entrantes a la línea de lugares sospechosos, y llamadas posteriores al cambio de SIM a servicios de atención al cliente de entidades financieras.

7.- Sobre el número de casos de solicitudes fraudulentas de duplicados de SIM detectados durante todo el año 2019, la entidad ha manifestado: Casos totales (…).

(…)

Sobre el número de clientes de telefonía móvil total de la entidad han manifestado:

POSTPAGO: 4.739.191 Clientes.

PREPAGO: 1.758.708 Clientes

Respecto a los casos presentados ante la agencia:

PARTE RECLAMANTE UNO:

Aportan copia denuncia de robo de DNI ante la policía así como copia de DNI (el solicitante del duplicado de SIM aportaría una fotocopia del DNI y no el original ya que declara que le había sido robado). Los representantes de XFERA indican que su departamento de fraude ve indicios de que la denuncia y su documento adjunto (DNI) están falsificados.

PARTE RECLAMANTE DOS:

Los representantes de XFERA indican que la solicitud fue por canal telefónico, no presencial como el reclamante ha manifestado. Aportan grabación de la llamada.

Escuchada la grabación se verifica que el operador pregunta (…).

Sobre otros casos no presentados ante la agencia:

Aportado el listado requerido se verifica que constan 20 casos (…).

Los representantes de XFERA indican que de los 20 casos solo 2 han sido reclamados, manifestando que el grupo cuenta con una herramienta de detección de fraude y la mayoría de los casos de *SIM swapping* son detectados por esta vía no por reclamación.

Se verifica lo siguiente:

(…)

Se ha requerido también a XFERA para que, de los quince casos de (…), aporte copia de la grabación de la llamada donde el solicitante pase la política de seguridad, (…).

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

CASO 1. (…). El solicitante pregunta también por núm. cuenta bancaria, men-

ciona que empieza por cuatro determinados dígitos y la operadora contesta afirmativamente.

CASO 2. El operador pregunta el nombre y el solicitante lo dice sin apellidos. (…). 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 DNI, nombre y apellidos y número de línea.

CASO 7. Pregunta núm. Línea. En ningún momento le pide (…). 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 (…).

De los cinco casos restantes no se aportan grabaciones.

De los diez casos aportados, en tres ocasiones el operador no pasa la política de seguridad completa (…). Todos los casos son de las marcas MÁSMÓVIL y YOIGO. En dos casos los agentes facilitan datos.

Se observa que los operadores en ocasiones facilitan datos al interlocutor a pesar de constar en la política de seguridad que no se debe de facilitar datos personales en ningún caso, incluso superada la política.

Se observa que los operadores en ocasiones (…), refiriendo el solicitante de la activación que estaba con otro operador activando la SIM y se cortó la llamada, o que le han enviado por mensajería la SIM y le dijeron que tenía que llamar para dar el ICC, u otras circunstancias. En ningún caso el operador dice que la SIM no valga o sea incorrecta al no tener la numeración ICC o no estar registrada para ese cliente o línea, simplemente asocia en el sistema el nuevo número de ICC a la línea del cliente.

Se ha preguntado a XFERA por la posibilidad de adquirir SIM sin asociar a ninguna línea o cliente, e información sobre si se permite que un cliente obtenga un SIM sin activar y sin asociar a una línea determinada, que posteriormente pueda activar telefónicamente y asociar a una línea, así como si existe la posibilidad, sin fraude de *SIM swapping*, de la activación de un SIM que esté en posesión de un cliente, sin haber sido asociado previamente en los sistemas de la entidad a una línea de su titularidad.

Los representantes de XFERA han manifestado al respecto que:

(…)

SÉPTIMO: Con fecha 27 de agosto de 2020, se obtiene información de la Comisión Nacional de los Mercados y la Competencia sobre las líneas de telefonía móvil de voz por tipo de contrato y por segmento siendo los resultados:

OPERADOR	PREPAGO		POSPAGO	
	Residencial	Negocios	Residencial	Negocios
Grupo MÁSMÓVIL	1.761.276	0	5.565.794	19.416

OCTAVO: Con fecha 27 de enero de 2021, se obtiene información comercial sobre el volumen de ventas de XFERA durante el año 2019 siendo los resultados de 1.598.873.000 euros. El capital social asciende a 1.000.000 euros.

NOVENO: Con fecha 11 de febrero de 2021**,** la directora de la AEPD acuerda iniciar un procedimiento 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 como muy grave, pudiendo ser sancionada con una multa administrativa de 500.000,00 de euros (quinientos mil euros), sin perjuicio de lo que resultase de la instrucción.

DÉCIMO: Con fecha 12 de febrero de 2021, la AEPD, en cumplimiento de lo establecido en el artículo 77.2 del RGPD comunica a las partes RECLAMANTES UNO y DOS la incoación del expediente sancionador ***PS/00027/2021***.

UNDÉCIMO: El Acuerdo de Inicio se notifica a XFERA, en fecha 15 de febrero de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

DUODÉCIMO: Con fecha 22 de febrero de 2021, XFERA solicita la ampliación del plazo para aducir alegaciones.

DÉCIMO TERCERO: Con fecha 1 de marzo de 2021, la instructora del procedimiento acuerda la ampliación de plazo instada hasta un máximo de cinco días, de acuerdo con lo dispuesto en el artículo 32.1 de la LPACAP.

El Acuerdo de ampliación se notifica a XFERA en fecha 1 de marzo de 2021.

DÉCIMO CUARTO: Con fecha 8 de marzo de 2021, se recibe en esta Agencia, en tiempo y forma, escrito del representante de XFERA en el que aduce alegaciones y tras manifestar lo que a su derecho conviene, termina solicitando el archivo de las actuaciones, sin que sea necesaria la formulación de la Propuesta de Resolución, debido a que los Hechos Probados no constituyen, de modo manifiesto, infracción administrativa; subsidiariamente, se proponga el archivo de las actuaciones, debido a la ausencia de culpabilidad por parte de XFERA; y subsidiariamente, se proponga una sanción más leve que la incluida en el Acuerdo de Inicio.

En síntesis aduce que:

PREVIA.- ASPECTOS PRELIMINARES.

a) NECESARIA SUSPENSIÓN DEL PROCEDIMIENTO POR PREJUDICIALIDAD PENAL.

En el marco de la investigación, le fue requerida a XFERA la presentación de un "listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes". Este listado fue tenido en cuenta por la Agencia, tanto a efectos probatorios (a efectos de "verificar el cumplimiento de los procedimientos por parte de los gestores de las solicitudes", página 35 del Acuerdo) como para determinar la gravedad de la infracción y su consiguiente sanción pecuniaria (se considera que los hechos acontecen "hasta el 12 de abril de 2020 [último de los casos presentados ante la agencia]", página 45 del Acuerdo). Entre los casos que integran este listado se encuentra el relativo al número de línea ******TELEFONO.5***, ocurrido el 14 de enero de 2020 y relacionado con el DNI ******NIF.3***. Este caso está siendo investigado por la vía penal, y en concreto, por el Juzgado de Instrucción n.º 9 de Alicante, en el marco de las diligencias previas ***ÑÑÑÑÑ/ÑÑÑÑ***. Se acompaña, como Documento 1, oficio del citado juzgado dirigido a nuestra empresa que acredita este hecho.

El modus operandi de este supuesto es idéntico al identificado en el caso de la parte RECLAMANTE UNO: persona que acude a una tienda de Yoigo para solicitar un duplicado de una tarjeta SIM, aportando un DNI supuestamente falsificado para identificarse. Es opinión de XFERA que resulta decisivo para resolver el expediente acreditar si efectivamente los hechos se produjeron de la forma descrita, pues de confirmarse este extremo, la ausencia de culpabilidad de XFERA sería evidente, lo que necesariamente conllevaría el archivo del expediente. Se alega que encontrándose pendiente un procedimiento penal para la averiguación de tales hechos, debe suspenderse cualquier actuación administrativa sancionadora en tanto no se determine la responsabilidad penal dilucidada. Todo ello a la espera de resolución judicial firme, cuyos hechos declarados probados vincularán a esta Agencia respecto del presente procedimiento sancionador, conforme a lo previsto en el artículo 77.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP). Por lo que se solicita la suspensión del plazo de resolución del expediente hasta que recaiga una sentencia en el indicado procedimiento penal.

b) DISCONFORMIDAD CON LA ACUMULACIÓN DE HECHOS EN EL PRESENTE EXPEDIENTE.

XFERA manifiesta su disconformidad con la acumulación de los hechos de los que trae causa este expediente en un único procedimiento administrativo, toda vez que considera que no se cumplen los requisitos previstos en el artículo 57 de la LPACAP. Dicho artículo reza lo siguiente: "El órgano administrativo que inicie o tramite un procedimiento, cualquiera que haya sido la forma de su iniciación, podrá disponer, de oficio o a instancia de parte, su acumulación a otros con los que guarde identidad sustancial o íntima conexión, siempre que sea el mismo órgano quien deba tramitar y resolver el procedimiento. Contra el acuerdo de acumulación no procederá recurso alguno". XFERA considera que los hechos aquí analizados no guardan "identidad sustancial", porque traen causa de dos situaciones muy diferentes que, se pueden resumir en que, en uno de

los casos, XFERA fue víctima de presuntos delitos de falsedad en documento oficial y usurpación de identidad, toda vez que los empleados de una de sus tiendas fueron engañados por una persona que exhibió una denuncia y un Documento Nacional de Identidad manipulados, lo que incide decisivamente sobre la antijuridicidad y la culpabilidad de XFERA en relación con la infracción que se le atribuye, mientras que, en el otro caso, el engaño se produjo por teléfono, debido a que el solicitante contaba con una tarjeta SIM no activada y recitó correctamente todos los dígitos de su ICCID, por lo que no hubo una desviación del procedimiento establecido en cuanto al cambio de SIM telefónico en ese momento. El artículo 85 de la LPAC reconoce al infractor el derecho a reconocer su responsabilidad y a proceder al pago voluntario de la sanción pecuniaria propuesta, con las reducciones legalmente previstas. Al respecto, XFERA no puede ni debe reconocer su responsabilidad en el primero de los casos expuestos, porque es evidente que carece de toda culpabilidad en relación con la infracción a ella atribuida. Sin embargo, al acumular las actuaciones, se ha conculcado su derecho a reconocer la responsabilidad y proceder al pago voluntario sobre el segundo de los hechos expuestos. Toda vez que contra la acumulación de hechos infractores en un único procedimiento no cabe recurso, se deja constancia de esta disconformidad desde el momento inicial del procedimiento administrativo, así como de la indefensión y conculcación de derechos que causa a XFERA, a efectos de poder utilizar este argumento en la posible impugnación de la resolución que dicte esta digna Agencia para poner fin a su tramitación.

PRIMERA.- ¿QUÉ ES EL SIM SWAPPING?

La expresión inglesa “SIM swapping” se utiliza en nuestro país para designar un tipo de

ciberestafa, que es descrito por la Policía Nacional como sigue: “El método utilizado para la estafa consta de varias fases; en una primera fase, los investigados se apoderaban de las claves de acceso a los portales de banca online de las diferentes entidades mediante técnicas de “phishing”, “malware” o “pharming”. Conseguidas las claves, los autores solicitaban un duplicado de las tarjetas SIM de las diferentes víctimas, aportando a las empresas de telefonía móvil documentación falsa -en algunos casos, incluso de personajes públicos- con intención de recibir los códigos de confirmación de las transferencias fraudulentas que posteriormente realizaban. Obtenidos esos códigos, realizaban las transferencias fraudulentas desde las cuentas de las víctimas a cuentas de terceras personas, que les servían para canalizar el dinero. En otras ocasiones, también solicitaban préstamos preconcedidos o microcréditos a las entidades bancarias, con el fin de obtener mayor beneficio económico. Todo ello se realizaba en un corto periodo de tiempo, entre una y dos horas; tiempo máximo en el que la víctima se percataba de que su teléfono había dejado de funcionar -ya que su tarjeta SIM estaba inactiva-debido a que ya se estaba operando con la nueva tarjeta duplicada” (https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=8081).

Como se ve, la comisión de este delito conlleva la realización de toda una serie de conductas delictivas, que comienzan con el acceso por el delincuente a la información personal y las claves de bancarias de las víctimas, pasan por la usurpación de la identidad de la víctima para lograr una copia de su tarjeta SIM, y terminan con la recepción en un dispositivo móvil de los códigos de confirmación necesarios para autorizar la realización de transferencias. Se trata de una modalidad de estafa que, como recoge

la memoria del año 2020 de la Fiscalía, referida al año 2019, “está generando justificada preocupación por su incremento en el último periodo anual”(https://www.fiscal.es/memorias/memoria2020/FISCALIA_SITE/recursos/pdf/capitulo_III/cap_III_8_2.pdf, pág. 1011).

XFERA considera importante clarificar que la obtención por los perpetradores del duplicado de la tarjeta SIM es un medio para la comisión del delito, que se produce únicamente tras haber obtenido las claves e información personal de la víctima. Y que la práctica se extendió en el año 2019, a raíz de la implementación precipitada por las entidades financieras de las llamadas “obligaciones de autenticación reforzada” previstas en la Directiva (UE) 2015/2366 (conocida como PSD2), que entraba en vigor el 14 de septiembre de dicho año. Esto fue así dado que el método elegido por los bancos, en contra del criterio de organismos públicos de ciberseguridad como Incibe, fue la llamada “autenticación en dos pasos” mediante el envío de claves por SMS; una técnica claramente vulnerable, como se ha demostrado en la práctica.

a) LAS TARJETAS SIM SON DUPLICADAS MEDIANTE FALSIFICACIONES.

Debe partirse de la base de que el ciberdelincuente ya tenía en su poder los datos personales del afectado necesarios para duplicar la tarjeta SIM y así lo reconoce el propio Acuerdo (página 31): “Hay que señalar que para que los suplantadores puedan efectuar operaciones bancarias fraudulentas, además de duplicar la tarjeta SIM de las personas afectadas, deben tener en su poder otros datos, en concreto los bancos con los que operan estas personas y las credenciales de acceso a la banca on-line, ya que el acceso a los mensajes SMS por sí solo no permite la ejecución de operaciones bancarias”. De este modo, para que un estafador pueda obtener un duplicado de la SIM, debe generar elementos suficientes de presunción de identidad del afectado, aportando datos como una copia de su DNI, su propio teléfono o los datos identificativos relativos a la víctima que superen las medidas de control implantadas para este proceso. Tal es así que, de no disponer previamente de estos datos, el llamado “procedimiento de seguridad” bloquearía cualquier intento de acceso. En definitiva, la confidencialidad de los datos no se ha comprometido por ninguna causa imputable a XFERA, pues ya estaba previamente comprometida.

b) LA AUTENTICACIÓN EN DOS PASOS POR SMS ES INTRÍNSECAMENTE INSEGURA.

Desde el año 2017, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) considera que el uso de las redes telefónicas públicas conmutadas para el envío de códigos de autenticación (por ejemplo, a través de SMS) debe ser restringido (ver al respecto: https://pages.nist.gov/800-63-3/sp800-63b.html#restricted).

Por las mismas fechas, el Instituto Nacional de Ciberseguridad de España (Incibe) publicaba en su blog, al hablar de la autenticación de doble factor: “Los mecanismos de dos pasos son más vulnerables y están desaconsejados, al poderse interceptar la comunicación del segundo factor pues suele ser algo que nos envían, generalmente por SMS” (https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos).

Sin embargo, y a pesar de estas alertas, las entidades financieras vienen considerando que el envío de un código de autenticación por SMS cumple con los

criterios establecidos en la Directiva PSD2 para ser considerado un mecanismo de “autenticación reforzada”. Así, comenzaron hace años por ofrecer a sus clientes la posibilidad de utilizar este método de identificación, para más recientemente imponerlo a toda su clientela.

La entrada en vigor de estas obligaciones de autenticación reforzada no se produjo hasta el 14 de septiembre de 2019; pero muchas entidades financieras se adelantaron a dicha fecha. Es en este contexto en el que se populariza el delito conocido como “SIM swapping”.

Con la adaptación a PSD2, los delincuentes necesitaban también acceder a los SMS que los bancos enviaban a los usuarios, comenzando entonces a suplantar la identidad de dichas víctimas para tratar de obtener de las operadoras duplicados de sus tarjetas SIM. Empresas como XFERA se encontraron de golpe con una nueva operativa delictiva que hasta el momento, simplemente, desconocían; y es, precisamente, en ese contexto temporal en el que se produjeron los hechos denunciados por los reclamantes, toda vez que la denuncia de la parte RECLAMANTE DOS se refiere a hechos ocurridos el 25 de septiembre de 2019, y la presentada por la parte RECLAMANTE DOS versa sobre hechos acaecidos el 10 de julio de 2019.

SEGUNDA.- XFERA GESTIONÓ ADECUADAMENTE EL RIESGO EN RELACIÓN CON EL SIM SWAPPING.

XFERA alega que los hechos de los que trae causa este procedimiento deben dividirse en dos períodos claramente diferenciados: el anterior al conocimiento por parte de XFERA de la operativa criminal conocida como “SIM swapping”, y el posterior a la identificación de dicho riesgo. La realidad es que XFERA no tiene conocimiento efectivo de esta problemática 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), que comienza como sigue (se acompaña copia del citado requerimiento como Documento 2): “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)”. Ante estas noticias, XFEA activó un procedimiento de revisión de sus medidas de seguridad, en línea con las obligaciones de gestión de riesgos y responsabilidad activa establecidas por el RGPD. De una parte, se reforzaron los procedimientos de identificación, recogidos en las páginas 16 y siguientes del Acuerdo; y de otra, se activaron dos capas de seguridad adicionales, que comenzaron a aplicarse el 28 de noviembre de 2019, pero a pesar de que son mencionadas en la página 24 del propio Acuerdo, todo apunta a que su eficacia y el esfuerzo realizado por la empresa para su desarrollo no han sido tenidos suficientemente en cuenta por esta Agencia. Para acreditar que la revisión de las medidas de seguridad se produjo, efectivamente, tras tener conocimiento de esta problemática, se aporta el documento de análisis de riesgos en relación con el tratamiento de identificación de usuarios de XFERA, en sus versiones anterior y posterior a la detección de esta operativa delictiva, como Docu-

mentos 3 y 4, respectivamente.

2.1. CAPAS DE SEGURIDAD IMPLEMENTADAS POR XFERA.

El sistema de seguridad por capas implementado por XFERA desde noviembre de 2019 sigue el llamado “modelo de queso suizo” de gestión de riesgos. En este modelo, las barreras de una organización contra las amenazas se modelan en capas, representadas como lonchas de queso. Se parte de la base de que ninguna medida de seguridad es perfecta, por lo que las debilidades inherentes a cada capa se representan como agujeros en las lonchas de queso. Si las medidas implementadas en cada una de las capas son diferentes, los agujeros variarán de una capa a otra. Para que se produzca la brecha de seguridad, los agujeros de todas las lonchas deberían alinearse, de manera que un ataque las pudiese atravesar en su totalidad; pero la probabilidad de que esto ocurra, si el sistema está bien planteado, es extraordinariamente baja.

La primera de las capas de seguridad implementadas por XFERA, y la única existente hasta noviembre de 2019 en relación con los duplicados de tarjetas SIM, es la llamada “política de seguridad”, que sirve para validar la identidad de los solicitantes. La Agencia aprecia en ella “posibles vulnerabilidades” (página 35 del Acuerdo), derivadas tanto del error humano como por la habilidad de los delincuentes para suplantar la identidad de las víctimas. Sin embargo, no evalúa las dos capas de seguridad adicionales implementadas por XFERA, lo que da lugar a un análisis incompleto de los hechos, hasta el punto de calificarla injustamente como “negligente”.

La segunda de las capas implementadas se basa en el llamado principio de “protección de datos desde el diseño”, y consiste en una herramienta informática denominada “***HERRAMIENTA.2”. (…). 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:

(…)

Este sistema se aplica aun habiéndose rebasado la primera capa de seguridad por parte de los delincuentes solicitantes (esto es, una vez superadas las políticas de identificación establecidas en tiendas y en el servicio de atención al cliente), y tiene una elevadísima eficacia. Las alertas son monitorizadas por un equipo técnico, en modo 24x7 y con SLA establecido de 5 minutos.

La tercera capa de seguridad, es la 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 (se acompaña la política en aplicación como Documento 5). En cuanto a la eficacia de las medidas, los números hablan por sí solos, y demuestran su rotundo éxito. Estas son 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

Las conclusiones que se pueden extraer de esta estadística son las siguientes:

- Si bien la cantidad total de intentos fraudulentos de duplicación de tarjetas SIM es elevada, supone un porcentaje muy pequeño del inmenso volumen de solicitudes legítimas que recibe anualmente en XFERA.
- La política de seguridad aplicada por la compañía, en líneas generales, es muy eficaz: (…). La eficacia de esta medida fue, por tanto, del ***PORCENTAJE.6.
- El sistema ***HERRAMIENTA.2 también ha demostrado su eficacia: (…) por este segundo filtro. Su concreta eficacia fue, por tanto, del ***PORCENTAJE.7.
- En cuanto a las revisiones aleatorias realizadas por parte del departamento de control de servicio, (…), con una eficacia del ***PORCENTAJE.8.

Como se aprecia, y en resumen, la implementación de la estrategia de queso suizo funcionó con 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. Evidentemente, el objetivo de XFERA es detectar el 100% de los intentos de fraude, y en esa línea seguimos trabajando... pero no puede negarse que los resultados obtenidos son verdaderamente espectaculares, y que XFERA ha volcado todos sus esfuerzos en hacer esta cifra incluso menor, con cada una de las medidas que ha venido implantando. Se aporta, como Documento 6, una tabla con los ***CANTIDAD.3 casos que superaron la primera barrera.

2.2) RELACIÓN DE ESTAS MEDIDAS Y LOS DOS CASOS DE LOS QUE TRAE CAUSA EL EXPEDIENTE.

El modelo de seguridad “queso suizo” se implementó el 28 de noviembre de 2019, tras haber tomado conocimiento XFERA de la existencia de la práctica ilícita conocida como SIM swapping. Desgraciadamente, los hechos denunciados por los reclamantes ocurrieron antes de la aplicación de estas medidas, y antes incluso de la recepción por XFERA del requerimiento de la SEAD; y si pudieron materializarse es porque XFERA desconocía esta operativa delictiva y, por tanto, no había podido tenerla en consideración a la hora de evaluar sus riesgos y

establecer medidas de seguridad acordes a los mismos. En concreto, las fechas en los que se tramitaron los duplicados de tarjeta SIM fueron los siguientes:

- En el caso de la parte RECLAMANTE UNO, el 25 de septiembre de 2019;
- En el caso de la parte RECLAMANTE DOS, el 10 de julio de 2019.

Sin embargo, se debe destacar que las circunstancias que rodean a cada uno de estos casos son bien distintas:

- En el caso de la parte RECLAMANTE UNO, 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. En ese sentido, la manipulación realizada recaía sobre elementos esenciales de los documentos facilitados al personal de la tienda, como son el nombre y apellidos del titular del DNI y del denunciante; y tuvo suficiente entidad como para engañar a estos trabajadores. Resulta, al respecto, irrelevante que el departamento de fraude de XFERA apreciase con posterioridad “indicios de que ambos habían sido falsificados” (página 40 del Acuerdo), porque no es exigible a los empleados de una tienda el conocimiento sobre falsedades documentales que concurre en un experto en detección de fraude: antes al contrario, el criterio a emplear es la idoneidad del engaño para inducir a error a una persona de capacidad media. Se resalta que la manipulación de dichos documentos no son burdas manipulaciones poco profesionales, sino manipulaciones realizadas con un grado de detalle más que suficiente para que una persona diligente y cuidadosa pueda tomar dichos documentos como verdaderos.

  En la medida en que se trata de documentos idóneos para producir un engaño, y que en la práctica lograron su objetivo, XFERA ha sido víctima de un delito de falsedad en documento oficial, previsto en el artículo 392 del Código Penal. Nótese que el bien jurídico protegido, en el caso de este delito, es la legítima confianza de los ciudadanos e instituciones fundada en la adecuación de los documentos públicos a la realidad: considerar a XFERA responsable supondría obviar el principio de culpabilidad, y generaría una evidente indefensión. De ahí que no quepa derivar responsabilidad administrativa de este supuesto.

- El caso de la parte RECLAMANTE DOS, en cambio, es algo más dudoso.

  Todo indica que el suplantador se hizo con una tarjeta SIM “en blanco”, probablemente tras obtenerla ilícitamente (…). Así se desprende del contenido de la llamada: basta escuchar la conversación para comprobar que el solicitante contaba con el ICCID completo de la tarjeta SIM, que únicamente figura impreso en el dorso de la propia tarjeta. Conviene destacar que el caso se produjo el 10 de julio de 2019, y fue el primero de esta naturaleza que afectó a XFERA: nunca antes se había detectado un duplicado de SIM en el cual el solicitante se hubiese agenciado previa e ilícitamente de una tarjeta no activada de esta marca. Có-

mo la obtuvo el delincuente, es un completo misterio para XFERA, pero probablemente fue sustraída a una tienda, o a un instalador oficial. Nótese que, en aquel momento, la empresa no efectuaba seguimientos de sus tarjetas no activadas, porque su coste económico es bajo; porque son soportes “en blanco”, que no contienen ningún tipo de información personal; y porque hasta entonces no se habían detectado fraudes similares al descrito en este procedimiento. No se había percibido, en definitiva, un riesgo relacionado con este tipo de elementos. En la práctica, en aquel entonces, solo había un método legal para obtener una SIM no activada: haberla recibido a través del servicio “***SERVICIO.1”,, tras haberla solicitado por teléfono. La forma de entrega, en sí misma, constituye una medida de seguridad, pues exige la exhibición del documento de identidad en vigor, coincidente con el número del documento de identidad del titular de la línea; y por ese motivo, hasta entonces los agentes recibían únicamente llamadas genuinas: de ahí lo laxo del trámite telefónico de activación. Fue a raíz de que se comenzasen a recibir solicitudes de este tipo cuando se modificó el procedimiento de seguridad, ampliando la necesidad de identificar adecuadamente al solicitante todo tipo de casos. Sin embargo, prever esta operativa delictiva en el momento en que se produjo esta incidencia era, sencillamente imposible para XFERA. No puede esta Agencia pretender imponer obligaciones de resultado, excluyendo de la ecuación el necesario componente subjetivo y la clara diligencia mostrada por XFERA, cuando únicamente ha sufrido un puñado de casos mientras cuenta con una base de clientes de más de 7 millones de líneas móviles. Dicho lo anterior, con el sistema implementado a finales de 2019, con total seguridad el segundo de estos dos casos no se habría producido, y muy probablemente, tampoco el primero. De ahí que se entienda que la problemática de seguridad ha sido ya corregida.

2.3) RELACIÓN ENTRE ESTAS MEDIDAS Y LOS 20 CASOS ADICIONALES, APORTADOS A LA AEPD.

En su requerimiento de 18 de junio de 2020, la AEPD solicitó a XFERA que le aportase un “listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes”. Cumpliendo con el requerimiento, remitimos a la Agencia el listado de solicitado, acompañada de una explicación de mayúscula relevancia, que se obvia en el procedimiento. La transcribimos nuevamente, para que pueda ser tenida en cuenta por la Sra. Instructora: “Con carácter previo consideramos necesario aclarar la siguiente información. Aportamos lista con los 20 primeros casos de solicitud de duplicado de SIM de forma fraudulenta confirmados. XFERA cuenta con una herramienta de detección de fraude que tiene capacidad para detectar, entre otras cosas, (…), con la finalidad de evitar el fraude .Esta alerta, se traslada al servicio de atención al cliente para que se pongan en contacto con el cliente y hagan las comprobaciones necesarias, abriendo un ticket de Reclamación en ***APLICACION.1. La gran mayoría de las reclamaciones por SIM Swapping son iniciadas por esta vía y no a través de una reclamación o denuncia realizada por el cliente, de hecho, como puede comprobarse en esta lista, solo dos de los casos que reportamos han sido reclamados o denunciados directamente por el cliente”. Como se puede apreciar, el escrito es claro al informar a la

Agencia de que se le estaban facilitando los veinte primeros casos detectados por XFERA, pero que únicamente dos de ellos se correspondían con casos denunciados o reclamados por los clientes, porque los dieciocho restantes fueron detectados de forma casi inmediata por la herramienta de detección de fraude ***HERRAMIENTA.2, que como hemos expuesto anteriormente, fue desarrollada por nuestra empresa, e implementada el 28 de noviembre de 2019.

Se reproduce, a continuación, una tabla donde figuran nuevamente las veinte reclamaciones aportadas en su momento a esta digna Agencia, pero incorporando a las mismas la fecha y hora en que se recibió la solicitud ilícita y el momento de bloqueo de la tarjeta SIM. Es digno de mención 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.4	MásMóvil	Telefónico	05/01/2020 22:12	05/01/2020 22:24
***TELEFONO.5	Yoigo	Tienda	14/01/2020 20:18	15/01/2020 21:43
***TELEFONO.6	MásMovil	Telefónico	15/01/2020 12:43	15/01/2020 13:20
***TELEFONO.7	MásMóvil	Telefónico	20/01/2020 21:01	20/01/2020 22:51
***TELEFONO.8	Yoigo	Telefónico	25/01/2020 16:48	25/01/2020 17:50
***TELEFONO.9	MásMóvil	Telefónico	27/01/2020 14:20	27/01/2020 17:50
***TELEFONO.10	Yoigo	Tienda	27/01/2020 17:07	27/01/2020 17:28
***TELEFONO.10	Yoigo	Tienda	27/01/2020 19:56	27/01/2020 21:50
***TELEFONO.11	Yoigo	Tienda	28/01/2020 12:29	28/01/2020 12:59
***TELEFONO.12	Yoigo	Telefónico	04/02/2020 16:08	04/02/2020 16:26
***TELEFONO.13	Yoigo	Telefónico	25/02/2020 23:05	25/02/2020 23:12
***TELEFONO.14	Yoigo	Telefónico	27/02/2020 18:31	27/02/2020 19:19
***TELEFONO.15	Yoigo	Telefónico	29/02/2020 21:38	29/02/2020 21:51
***TELEFONO.15	Yoigo	Telefónico	03/03/2020 7:37	03/03/2020 7:48
***TELEFONO.16	Yoigo	Telefónico	05/03/2020 17:07	05/03/2020 22:23
***TELEFONO.12	Yoigo	Telefónico	05/03/2020 21:07	05/03/2020 21:37
***TELEFONO.17	Yoigo	Tienda	11/03/2020	11/03/2020

			13:59	14:42
******TELEFONO.18***	Yoigo	Telefónico	13/03/2020 12:51	13/03/2020 13:24
******TELEFONO.19***	MásMóvil	Telefónico	03/04/2020 15:11	03/04/2020 15:22
******TELEFONO.20***	MásMóvil	Telefónico	04/04/2020 13:45	04/04/2020 14:04
******TELEFONO.21***	Yoigo	Tienda	08/04/2020 21:03	08/04/2020 22:04
******TELEFONO.22***	Yoigo	Telefónico	12/04/2020 15:39	12/04/2020 15:54

Como se puede apreciar, la eficacia de la segunda capa de seguridad es muy elevada (superior al 90%, según nuestros cálculos), y se resume a continuación:

- En los siguientes casos (un total de 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 sabemos: ******TELEFONO.4, ***TELEFONO.8, ***TELEFONO.10*** (en dos ocasiones), ******TELEFONO.11, ***TELEFONO.14, ***TELEFONO.18, ***TELEFONO.19, ***TELEFONO.21, ***TELEFONO.22***. El tiempo medio de bloqueo, en los casos listados, fue de 40 minutos; y su mediana, de 31 minutos.
- En los siguientes casos (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 sabemos: ******TELEFONO.6, ***TELEFONO.10, ***TELEFONO.12*** (en dos ocasiones), ******TELEFONO.13, ***TELEFONO.15*** (en dos ocasiones), ******TELEFONO.17, ***TELEFONO.20***. 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.16*** (1 sobre 22), 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 los siguientes casos (un total de 2 sobre 22), 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.5, ***TELEFONO.7***.

  De estos dos casos, es importante señalar que, en lo tocante al número de teléfono ******TELEFONO.5***, la suplantación de identidad se produjo en una tienda de Yoigo, y que el solicitante exhibió un DNI falso, cuya copia fue aportada al expediente. Se dan por reproducidas, al respecto, las alegaciones planteadas en relación con el caso de la parte RECLA-

MANTE UNO, en lo relativo a ausencia de antijuridicidad y culpabilidad en la conducta de XFERA.

Esta significativa mejora en los procedimientos no ha sido analizada por la Agencia Española de Protección de Datos en su Acuerdo de Inicio, a pesar de que la existencia del sistema de detección de fraude (…).

Es importante destacar que el último caso, de entre los solicitados por la Agencia, en que el solicitante logró superar las dos capas de seguridad se produjo el 20 de enero de 2020. Al respecto:

- Es evidente que la "mejora" que se reclama en el Acuerdo (página 37) ya se ha producido, y la seguridad sigue incrementándose cada día que pasa, toda vez que se utilizan los errores para calibrar proactivamente el sistema ***HERRAMIENTA.2, y hacerlo cada vez más eficaz; y
- Es incorrecto el período de duración de la supuesta infracción recogido en la página 45 del Acuerdo, toda vez que el último de los casos aportados en los que se corroboró fraude se produjo el 20 de enero de 2020, y no el 12 de abril, como indica la resolución.

2.4) INCONGRUENCIA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Llama la atención la incongruencia de la sanción propuesta en este expediente, en relación con otras resoluciones sobre casos análogos, en los que el esfuerzo de seguridad realizado por XFERA sí fue tenido en consideración por la Agencia y llevó al archivo de las actuaciones. Sirva como ejemplo la reciente resolución de fecha 15 de febrero de 2021, en el expediente ***E/09594/2020***, relativa a una supuesta "ausencia de medidas de seguridad con la consecuencia de emitirse un duplicado de tarjeta SIM sin consentimiento del reclamante", que concluyó con la inadmisión de la reclamación en base a la siguiente fundamentación: "La tramitación de la reclamación conforme a lo dispuesto en el artículo 65.4 de la LOPDGDD, ha dado lugar a la solución de las cuestiones planteadas, sin necesidad de depurar responsabilidades administrativas en el marco de un procedimiento sancionador. En este sentido, conviene hacer mención al carácter excepcional del procedimiento sancionador, del que deriva que -siempre que sea posible-deberá optarse por la prevalencia de mecanismos alternativos en el caso de que tengan amparo en la normativa vigente, tal y como ocurre en este caso. En síntesis, deben traerse a colación los principios aplicables al procedimiento sancionador. La Agencia Española de Protección de Datos ejerce la potestad sancionadora de oficio. Por tanto, es competencia exclusiva de la Agencia Española de Protección de Datos valorar si existen responsabilidades administrativas que deban ser depuradas en un procedimiento sancionador y, en consecuencia, la decisión sobre su apertura, no existiendo obligación de iniciar un procedimiento ante cualquier petición realizada por tercero. Tal decisión ha de basarse en la existencia de elementos que justifiquen dicho inicio de la actividad sancionadora, circunstancias que no concurren en el presente caso, a la vista de las actuaciones realizadas, por lo que procede el archivo de la reclamación presentada contra XFERA MÓVILES, S.A."

No parece razonable que la Agencia entienda, por una parte, que las cuestiones planteadas en relación con las medidas de seguridad estén resueltas y que no procede abrir expediente, dado el carácter excepcional del procedimiento

sancionador; y por otra, que idénticas medidas sean insuficientes y deba sancionarse a XFERA. Máxime, cuando ambas resoluciones fueron notificadas el mismo día.

2.5) LAS CINCO LLAMADAS EXTRAVIADAS HAN SIDO LOCALIZADAS, Y SE APORTAN AHORA AL EXPEDIENTE.

Afirma el Acuerdo, en su página 40, que "en cinco de los casos [adicionales aportados por Masmóvil] ni siquiera se han localizado las llamadas amparándose en posibles errores en la codificación (nomenclatura) de las mismas". Los llamados "errores en la codificación" se producen 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. No obstante, las llamadas en cuestión permanecen almacenadas en los servidores, y aunque localizarlas conlleva un arduo proceso de búsqueda, se ha logrado recuperarlas: se aportan ahora al expediente, en calidad de prueba adicional, como Documentos 7, 8, 9, 10 y 11.

Se resume su contenido:

CASO 1:Se corresponde con la línea (MSISDN) ******TELEFONO.4***, y se produjo el 5 de enero de 2020. El operador pregunta por (…). El solicitante responde correctamente a las dos primeras preguntas, pero menciona que solo se acuerda de memoria de los tres últimos dígitos del número de línea.

CASO 2:Se corresponde con la línea ******TELEFONO.7***, y se produjo el 20 de enero de 2020. El operador pregunta por (…). El solicitante responde correctamente a las tres preguntas.

CASO 3:Se corresponde con la línea ******TELEFONO.10***, y se produjo el 27 de enero de 2020. La operadora pregunta por (…). El solicitante responde correctamente a las tres preguntas. La operadora duda, porque el envío del duplicado de la tarjeta no consta en el sistema y solicita instrucciones a su coordinador. Este le confirma que, si el solicitante supera la política de seguridad, se puede activar la tarjeta.

CASO 4:Se corresponde con la línea ******TELEFONO.13***, y se produjo el 25 de febrero de 2020. El solicitante facilita el DNI y los tres últimos dígitos del número de línea. La operadora duda, porque el envío del duplicado de la tarjeta no consta en el sistema. Tras ser preguntado, el solicitante facilita también el nombre completo del titular.

CASO 5:Se corresponde con la línea ******TELEFONO.19***, y se produjo el 3 de abril de 2020. El operador pregunta por (…). El solicitante responde correctamente a las tres preguntas.

Como se puede apreciar, los solicitantes conocían, en todos los casos, los datos de DNI y nombre y apellidos de los titulares de la línea, superando así la política de seguridad inicial (primera capa) de la empresa. Ahora bien, de estos cinco supuestos, cuatro fueron interceptados por las capas adicionales de seguridad, y principalmente, por la ***HERRAMIENTA.2, lo que sin duda da una idea muy aproximada del foco puesto por XFERA en implantar medidas efectivas y del éxito de las mismas para reducir a la mínima expresión cualquier tipo de suplantación en el proceso de duplicado de SIM.

TERCERA.- LA ACTIVACIÓN DE UN DUPLICADO DE UNA TARJETA SIM NO ES

UN “TRATAMIENTO”.

Se afirma en el Acuerdo (página 32), que “con claridad meridiana resulta que los datos que se tratan para emitir un duplicado de tarjeta SIM son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos”. Sin embargo, esa “claridad meridiana” que afirma la Agencia debería aplicarse, únicamente, al proceso de verificación de identidad previo a la activación del duplicado de tarjeta SIM: la propia activación no puede ni deber ser considerada un “tratamiento”, y de hecho, el Acuerdo no justifica en ningún momento que así lo sea.

Una tarjeta SIM es un mero soporte, un dispositivo cifrado destinado a almacenar en su interior un código denominado IMSI (International Mobile Subscriber Identity) y una clave criptográfica asociada. Como explica la Comisión Nacional de los Mercados y la Competencia en su blog, el IMSI es un código de quince dígitos, consistente en lo siguiente: “Los primeros tres dígitos definen el país y se llaman MCC (Mobile Country Code) o IPM (Indicativo de País para el servicio Móvil). El MCC/IPM de cada país lo asigna la ITU y el de España es el número 214. Le sigue el número que indica el operador, que en España lo asigna la CMT. Es el MNC (Mobile Network Code) o IRM (Indicativo de la Red Móvil), de hasta tres cifras (en España es de dos). Los dígitos restantes son el MSIN (Mobile Subscription Identification Number) y se reservan para que el operador los asigne a cada una de las líneas de sus clientes.”

Un técnico del XFERA, internamente, asigna ese IMSI genérico a uno o varios MSISDN (el número de línea del usuario); pero (1) el IMSI y el MSISDN son números diferentes, y (2) este último no se almacena en la tarjeta SIM, como recoge el mismo artículo de la CNMC: “En la tarjeta SIM no se almacena nuestro número de teléfono MSISDN, pero en cambio es imprescindible que esté el IMSI (además del ICCID y otros datos). En caso de robo, si comunicamos al operador que nuestra SIM ha sido sustraída, éste nos dará una SIM nueva con un IMSI nuevo para evitar que alguien pueda realizar llamadas en nuestro nombre. Sin embargo, mantendremos nuestros MSISDN (...) Además, como antes hemos comentado, diferentes números IMSI (de diferentes abonos) pueden apuntar a un mismo número de teléfono.”

En la totalidad de las 15 llamadas telefónicas examinadas por la Agencia en el marco del procedimiento, se daba la circunstancia de que obraban en poder del solicitante tarjetas SIM no activadas, sin que XFERA pueda conocer la forma de obtención de las mismas (aunque se cree que fueron sustraídas, sea en alguna tienda, sea a algún instalador autorizado); pero dichas tarjetas están en blanco, y (1) no contienen ningún tipo de dato de carácter personal; (2) no disponen de ningún tipo de identificador asociado, directa o indirectamente, a ningún interesado; y (3) no permiten el acceso a información relativa a ninguna persona física.

En cuanto al procedimiento de activación, simplemente supone asociar el código IMSI ya incluido en la SIM con un MSISDN; y se trata de un proceso exclusivamente técnico, que no conlleva ningún tipo de operación “sobre” datos personales; algo extraordinariamente relevante, porque excluye la existencia de un “tratamiento”. Nótese que, conforme al artículo 4 del RGPD, la definición de tratamiento es la siguiente: “«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;”

El mero hecho de que el MSISDN pueda ser considerado un dato personal no conlleva que se esté ante un "tratamiento" y que, por tanto, se aplique la normativa de protección de datos: eso únicamente ocurrirá cuando se realicen operaciones sobre datos personales. La realidad es que, al activarse una tarjeta SIM, no se realiza operación alguna sobre el MSISDN, o sobre cualesquiera otros datos personales: únicamente se actúa sobre la propia tarjeta, y esta no puede ser considerada "dato de carácter personal", ni contiene información de esta naturaleza. Una tarjeta SIM no es un dato, es un soporte, y cuando se activa por vez primera, está vacío de todo contenido. No se está, por tanto, ante un tratamiento; y por ese motivo no debería aplicarse el RGPD a la concreta operación de activar la tarjeta SIM.

Evidentemente, no se puede negar que, con carácter previo a dicha activación, se produce un tratamiento de datos personales por parte de XFERA, consistente en verificar la identidad del cliente. En ese momento, efectivamente, se realizan operaciones sobre los datos personales del titular de la línea, y no hay inconveniente en admitir la aplicación del RGPD a esa fase del procedimiento objeto de análisis en el presente expediente. Pero el tratamiento en cuestión finaliza con la propia identificación del titular: la activación de la tarjeta SIM es posterior en el tiempo y, en ningún caso, debe ser considerada un "tratamiento" de datos personales. Este planteamiento, aparentemente nimio, revierte gran importancia, porque de él se deriva el riesgo que XFERA debe considerar a efectos de establecer las medidas de seguridad aplicables.

CUARTA.- APLICACIÓN AL CASO DEL PRINCIPIO DE PERSONALIDAD.

Reza el artículo 28 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en lo sucesivo, LRJSP), que "solo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas (...) que resulten responsables de los mismos a título de dolo o culpa". Este artículo consagra el llamado "principio de responsabilidad sancionadora estricta", o "principio de personalidad", previsto en el artículo 25.1 de nuestra Constitución. Se trata de uno de los pilares del derecho punitivo del Estado, que conlleva "la imposibilidad de la traslación de las consecuencias sancionadoras sobre personas o entidades distintas de los autores de los hechos punibles", en palabras de la Audiencia Nacional, que cita la doctrina de nuestro Tribunal Constitucional en la materia como sigue: "La Sentencia del Tribunal Constitucional 219/1988 , de 22 de diciembre , proclamó que el principio de personalidad de las sanciones o de responsabilidad personal por hechos propios impide un indebido traslado de la responsabilidad punitiva a persona ajena al hecho infractor, pues ello comportaría aceptar un régimen de responsabilidad objetiva que vulneraría la exigencia de dolo o culpa necesarios para la existencia de infracción administrativa".

XFERA considera que el Acuerdo, dicho sea en estrictos términos de defensa, vulnera dicho principio; y ello porque vincula la gravedad de la supuesta infracción, no al tratamiento de datos realizado por XFERA en sí mismo considerado, sino a las consecuencias de la utilización ilícita del duplicado de la tarjeta SIM por parte de terceros. Lo hace, de hecho, en múltiples ocasiones, y entre ellas:

- En las páginas 45 y 46, donde al analizar las circunstancias agravantes del caso, menciona las siguientes:
    - Naturaleza, gravedad y duración de la infracción: La Agencia considera que la naturaleza de la infracción es muy grave puesto que acarrea una pérdida de disposición y control sobre los datos personales".

      Como se ha expuesto, las tarjetas SIM que duplican los ciberdelincuen-

tes están en blanco, y carecen por tanto de cualquier dato personal en su interior. Por tanto, el acceso a una copia de la tarjeta SIM, de por sí, no supone ningún tipo de pérdida de disposición o control sobre datos personales. Nótese que los ciberestafadores únicamente pueden obtener dicha copia si previamente han logrado interceptar los datos personales del interesado por otras vías, a través de técnicas como el phishing(así lo reconoce la Agencia en la página 31 del Acuerdo). Ello demuestra que la pérdida de disposición y control sobre los datos personales ocurrió con carácter previo a los hechos sobre los que versa este expediente, y trae causa de la acción de un tercero ajeno a XFERA. Atribuir esta responsabilidad a XFERA es, simplemente, contrario a Derecho.

- Nivel de los daños y perjuicios sufridos: Alto. Deriva en operaciones bancarias fraudulentas que suceden en un corto espacio de tiempo. Mediante la duplicación de las tarjetas SIM, los supuestos suplantadores consiguen el control de la línea del abonado y en concreto la recepción de SMS dirigidos al legítimo abonado para realizar operaciones on-line con entidades bancarias suplantando su personalidad. Estos SMS los envían las entidades bancarias como parte de la verificación en dos pasos de operaciones como transferencias monetarias o pagos por Internet, y el acceso a estos SMS suele ser el motivo de la duplicación fraudulenta de las tarjetas SIM".

  Las consecuencias derivadas de los delitos cometidos por terceros no pueden ser trasladadas, en forma de agravante, a XFERA; y ello porque no cabe atribuir responsabilidad subjetiva a XFERA sobre hechos delictivos ajenos, y porque la responsabilidad objetiva está proscrita en el procedimiento sancionador.

- Categorías de datos personales afectados por la infracción: El acceso no autorizado a un duplicado de tarjeta SIM se considera particularmente grave ya que posibilita la suplantación de identidad".

  Como se ha expuesto, el acceso no autorizado a una tarjeta SIM no conlleva el acceso a dato personal alguno. Que los ciberestafadores empleen estas tarjetas como herramienta para la comisión de delitos trae causa, únicamente, de las debilidades de los sistemas de seguridad de las entidades que utilizan el SMS como medio de autenticación, aun a sabiendas de que se trata de un método intrínsecamente inseguro.

  Por tanto, se está nuevamente trasladando la responsabilidad de terceros, en forma de agravante, a XFERA, vulnerando el precepto constitucional antes citado.

- En la página 33, donde se explica la lógica en que se basa la Agencia para abrir un procedimiento contra XFERA:

  "Hemos de atender a las circunstancias singulares de las dos reclamaciones presentadas, a través de las cuales puede constatarse que, desde el momento en el que la persona suplantadora realiza la sustitución de la SIM, el teléfono de la víctima se queda sin servicio pasando el control de la línea a la persona suplantadora. En consecuencia, los reclamantes ven afectados sus poderes de disposición y control sobre sus datos personales, que constituyen parte del

contenido del derecho fundamental a la protección de datos según ha señalado el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre de 2000 (FJ 7). De manera que, al conseguir un duplicado de la tarjeta SIM, los suplantadores automáticamente tendrán acceso a los contactos y podrán acceder a todas aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder cambiar las contraseñas. En definitiva, podrán suplantar la identidad de los afectados, pudiendo acceder y controlar, por ejemplo: las cuentas de correo electrónico; cuentas bancarias; aplicaciones como WhatsApp; redes sociales, como Facebook o Twitter, y un largo etc. En resumidas cuentas, una vez modificada la clave de acceso por parte de los suplantadores pierden el control de sus cuentas, aplicaciones y servicios, lo que supone una gran amenaza."

En la medida en que una línea telefónica no es un dato de carácter personal, la afectación para los poderes de disposición y control sobre los datos personales de los reclamantes trae causa de la acción de los suplantadores, que utilizan la SIM para cambiar las contraseñas de las víctimas. Sin embargo, la responsabilidad de esta conducta es ajena, nuevamente, a XFERA, y debe ceñirse exclusivamente a los delincuentes que cometen el acto delictivo, y a las entidades que no configuran protocolos de autenticación seguros para el cambio de contraseñas por parte de sus clientes.

En resumen, la actuación de XFERA se circunscribe, en exclusiva, a la facilitación de un duplicado de una tarjeta SIM que no incluye información alguna ni sobre la víctima ni sobre sus contactos; ni tampoco da acceso a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS, puesto que esta medida requiere que los delincuentes conozcan en primer lugar qué aplicaciones utiliza la víctima y alguno de los parámetros de las credenciales de acceso, tales como correo electrónico, nombre de usuario o contraseña. Por supuesto, XFERA no puede responsabilizarse de la robustez en la autenticación de las entidades financieras o de los servicios de la sociedad de la información que entiendan como seguro el envío de credenciales a través de SMS: cada empresa ha de ser responsable de la seguridad de sus propias medidas. Hacer recaer sobre XFERA, en forma de agravante, las actuaciones u omisiones de terceros, es simplemente anticonstitucional: XFERA no puede ni debe responder de la conducta delictiva de unos estafadores, ni mucho menos de la falta de eficacia de las medidas de autenticación implementadas por las entidades financieras u otros servicios de la sociedad de la información.

QUINTA.- APLICACIÓN AL CASO DEL PRINCIPIO DE CULPABILIDAD.

El ya citado artículo 28 de la LRJSP, consagra igualmente el llamado "principio de culpabilidad", también recogido en el artículo 25.1 de nuestra Constitución. La Audiencia Nacional lo ha analizado en múltiples ocasiones, acostumbrando a citarlo en sus sentencias en los siguientes términos:

"El Tribunal Constitucional ha declarado reiteradamente que los principios del orden penal, entre los que se encuentra el de culpabilidad, son de aplicación, con ciertos matices, al derecho administrativo sancionador, al ser ambos manifestaciones del ordenamiento punitivo del Estado (STC 18/1987, 150/1991), y que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo

de culpabilidad aun a título de mera negligencia (SSTC 76/1990 y 164/2005).

El principio de culpabilidad, garantizado por el artículo 25 de la Constitución, limita el ejercicio del ius puniendi del Estado y exige, según refiere el Tribunal Constitucional en la sentencia 129/2003, de 20 de junio, que la imposición de la sanción se sustente en la exigencia del elemento subjetivo de culpa, para garantizar el principio de responsabilidad y el derecho a un procedimiento sancionador con todas las garantías (STS de 1 de marzo de 2012, Rec 1298/2009).

Ciertamente, el principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, de 26 noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone que solo pueden ser sancionados por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Obviamente, ello supone que dicha responsabilidad sólo puede ser exigida a título de dolo o culpa, quedando desterrada del ámbito del derecho administrativo sancionador la llamada "responsabilidad objetiva", y comprendiendo el titulo culposo la imprudencia, negligencia o ignorancia inexcusable. Esta "simple inobservancia" no puede ser entendida, por tanto, como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, pues la jurisprudencia mayoritaria de nuestro Tribunal Supremo (a partir de sus sentencias de 24 y 25 de enero y 9 de mayo de 1983) y la doctrina del Tribunal Constitucional (después de su STC 76/1990), destacan que el principio de culpabilidad, aún sin reconocimiento explícito en la Constitución, se infiere de los principios de legalidad y prohibición de exceso (artículo 25.1 CE), o de las propias exigencias inherentes a un Estado de Derecho, por lo que se requiere la existencia de dolo o culpa (en este sentido STS de 21 de enero de 2011, Rec 598/2008)".

XFERA considera que este análisis debe ser puesto en relación con la doctrina del Tribunal Supremo, tantas veces invocada por la Agencia en sus resoluciones, conforme a la cual "no basta... para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa"(STS 23 de enero de 1998). De ahí que se analicen a continuación los dos supuestos de los que trae causa este expediente, acreditando la ausencia de culpa:

- En el primero de los casos, el personal de una tienda de Yoigo fue sujeto pasivo de un delito de estafa, perpetrado por un individuo que acudió a la tienda exhibiendo documentación oficial falsa. Como recoge el Código Penal, este tipo delictivo es cometido por quienes, "con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno"; y como expresa el Tribunal Supremo (sentencias de 1 de marzo de 2004, en el recurso 3056/2002, y de 9 de octubre de 2005, en el recurso 86/2004):

  "el concepto de engaño bastante, no puede servir para desplazar en el sujeto pasivo del delito todas las circunstancias concurrentes desplegadas por el ardid del autor del delito, de manera que termine siendo responsable de la maquinación precisamente quien es su víctima".

  En el caso de la parte RECLAMANTE UNO, es evidente que el estafador hizo cuanto estaba en su mano para conseguir el resultado engañoso que en efecto se produjo, incluyendo la manipulación mediante programas informáticos de edición de imagen de un DNI y de una denuncia policial. Esta documentación fue conservada en los sistemas de XFERA y ha sido aportada al expediente, demostrando que el procedimiento de verificación de identidad estaba siendo

efectivamente aplicado por parte de las tiendas. No puede derivarse de este hecho, por tanto, ningún tipo de responsabilidad sustentada en una supuesta culpabilidad o falta de diligencia, pues la documentación presentada aparentaba estar en regla; y así lo ha reconocido la jurisprudencia en casos similares (Sentencia de la Audiencia Nacional de 20 de marzo de 2013 (rec. 581/2011, en relación al PS/00130/2011) y Sentencia de la Audiencia Nacional de 29 de octubre de 2009 (rec. 797/2008, en relación al PS/00290/2008). Las sentencias de 18 de marzo de 2010 (rec. 342/2009) y de 22 de marzo de 2012 (rec. 9/2009) reproducen este criterio.

- El segundo de los casos, fue el primero de una operativa nunca antes detectada en la marca Masmóvil: el solicitante contaba con una tarjeta no activada, algo que solo podía haber obtenido, conforme a los procedimientos de la empresa, tras haberse identificado y superando la política de seguridad entonces vigente. Los agentes especializados en resolver incidencias técnicas, como el que atendió su llamada, no tenían instrucciones de someter a los solicitantes al procedimiento de identificación en casos como el aquí descrito, pues quienes llamaban lo habían superado al solicitar el duplicado, y solo ellos podían haber recibido la tarjeta SIM en su domicilio, mediante el procedimiento de "***SERVICIO.1". Sin embargo, en este caso, el delincuente se había agenciado con una de estas tarjetas de forma ilícita, por canales ajenos al control de XFERA.

  Los procedimientos de la empresa no lograron el objetivo de identificar el fraude, simplemente, porque se trata de un modus operandi novedoso: fue el primer caso de estas características, por lo que el riesgo no había sido identificado y, como es lógico, no se habían adoptado medidas para mitigarlo. En cuanto estas conductas delictivas fueron identificadas por la compañía, se adoptaron todas las medidas para detectarlas y reaccionar frente a ellas de la forma más rápida posible, como ha sido demostrado.

  Al respecto, conviene traer a colación la sentencia del Tribunal Supremo de 1 de octubre de 1988 (recurso 1652/1996), según la cual "el reproche culpabilístico tendría que centrarse, esencialmente, en la previsibilidad del resultado dañoso"; previsibilidad que la Agencia no ha logrado acreditar en los hechos de los que trae causa este expediente.

SEXTA.- VULNERACIÓN DEL DERECHO A NO DECLARAR CONTRA UNO MISMO.

En otro orden de cosas, y en relación con el "listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes", XFERA entiende que el proceder de esta Agencia ha supuesto una vulneración del derecho a la defensa de XFERA, reconocido en el artículo 24 de nuestra Constitución. El requerimiento de información remitido a esta Agencia fue recibido solo dos días después de que el jefe adjunto de secretaría de dirección, enviase a XFERA una convocatoria para una reunión que tuvo lugar el día 20 de enero de 2020, a las 12:00h., en la sede de la Agencia (se acompaña el correo electrónico, como Documento 12). El primer punto del orden del día de esa reunión era "la duplicidad de tarjetas SIM", y XFERA contestó al requerimiento entendiendo que la información solicitada iba a ser utilizada en el marco de dicha reunión, en el contexto de los planes de auditoría preventivos previstos en el artículo 54 de la Ley Orgánica 3/2018 (en adelante, LOPDGDD) :"La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las

disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría".

Esta creencia se vio reforzada porque a la reunión fueron convocadas igualmente las demás empresas líderes del sector, que manifestamos en ella nuestra firme voluntad de cooperar con la Agencia para poner coto a esta problemática, prestando especial atención a los casos que pudiésemos identificar y endureciendo las medidas de seguridad a aplicar; en lo que supuso todo un ejemplo de colaboración público-privada para tratar de erradicar este tipo de prácticas.

Tanto es así, que en distintas reuniones con la Agencia Española de Protección de datos, concretamente en fechas, 20 de enero de 2020, 4 de diciembre de 2020 y 18 de enero de 2021, a los que acudió incluso la directora de la propia Agencia Española de Protección de Datos, tanto XFERA como el resto de operadoras convocadas, fueron proactivos en la amplia y extensa explicación de medidas adoptadas y a adoptar para controlar potenciales casos de SIM Swapping fraudulento, en la total convicción de que el "Grupo de Trabajo" (así llamado por la propia Agencia), se había concebido con la idea de la colaboración abierta y sincera entre las partes para erradicar una práctica que, además, todos los operadores de telecomunicaciones consideraron ajena a ellos, en la medida en que todos estos problemas traen causa de un phishing bancario previo y una vulneración de medidas de seguridad de las entidades financieras.

En el acta de una de esas reuniones, redactada por la propia Agencia y que se aporta como Documento 13, se recoge: "Todas ellas manifestaron su preocupación por este asunto. Informan de las medidas que para evitar fraudes en la obtención de duplicados han ido adoptando últimamente: limitar las posibilidades de procesos no presenciales, mejoras en sus sistemas, políticas y protocolos de seguridad adicionales enfocados a los procesos presenciales, sanciones a distribuidores y comerciales que no guarden los protocolos de seguridad establecidos, exigencia de documentación, canales de prevención del fraude, refuerzo de auditorías, robotización del proceso.... También se ha informado de un proyecto basado en reconocimiento biométrico (se solicitó que remitieran información de estas medidas)".

En la medida en que la Agencia goza de la potestad de recabar la colaboración de administrados, como recoge el artículo 52.1 de la LOPD, en cuya virtud, "las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación"; XFERA facilitó la información, esperando que el resultado de la cooperación fuese la elaboración de unas directrices por parte de la Agencia, en línea con lo previsto en el apartado segundo del mencionado artículo 54, y no la apertura de un procedimiento sancionador. Téngase en cuenta que la propia Agencia propuso, en el marco de estas reuniones, lo siguiente (consta en la citada acta):"Propone la creación de un repositorio común sobre buenas prácticas, para lo que se solicita a las operadoras que hagan llegar las medidas y prácticas adoptadas para evitar los casos de fraude de las que han informado y estén dispuestas a compartir, de manera que se pueda disponer de un repertorio de buenas prácticas accesible a los actores implicados".

Sin embargo, la Agencia optó por emplear dicha información –facilitada en el marco de la transparencia y total colaboración de las operadoras de telecomunicaciones con la propia AEPD, con el ánimo trabajar conjuntamente para la erradicación de prácticas

ilegales–como prueba en el procedimiento que nos ocupa, vulnerando así las garantías propias del Derecho administrativo sancionador y privando a XFERA de su derecho a no incriminarse. Así, ha aprovechado un procedimiento de naturaleza no sancionadora, como son los planes de auditoría preventivos, para nutrir de evidencias una investigación dirigida a ejercitar la potestad sancionadora, conculcando las garantías de todo imputado de una infracción.

Es opinión de XFERA que no cabe ejercitar la potestad prevista en el artículo 52.1 LOPDGDD respecto del administrado que puede resultar objeto de una imputación en un procedimiento sancionador. Y, desde luego, si el requerimiento a ese administrado llega a tener lugar, y la imputación finalmente se produce, la AEPD no puede emplear ningún elemento de juicio obtenido en virtud del deber de colaboración en el marco de un procedimiento sancionador, puesto que supondría una vulneración de su derecho a no incriminarse. En efecto, la AEPD tendría que emplear elementos de juicio que no fueran frutos del árbol envenenado, para lo cual tendría que acreditar que los ha obtenido con total ajenidad respecto de los requerimientos de colaboración.

A este respecto, cabe destacar que la LOPDGDD no establece ninguna limitación al derecho a no incriminarse, por lo que el deber de colaboración sólo puede entenderse exigible respecto a terceros ajenos a la imputación que se plantea, o al ejercicio de competencias distintas a la sancionadora. Por ello, teniendo lugar una imputación ulterior a un administrado que aportó elementos de juicio referentes a su conducta, en ejercicio del deber de colaboración, se concluye que sólo cabe efectuar un expurgo de los mismos, de manera que el eventual ejercicio de la potestad sancionadora no se base en ellos ni en ninguna consecuencia lógica de los mismos. Es decir, tal imputación deberá evitar fundarse en un fruto del árbol envenenado, entendiendo por tal la situación de vulneración del derecho a no incriminarse.

SÉPTIMA.- APLICACIÓN AL CASO DEL PRINCIPIO DE ESPECIALIDAD.

En caso de no apreciarse una total falta de culpabilidad, XFERA entiende que el Acuerdo vulnera el principio de especialidad que rige el derecho administrativo sancionador, a la hora de calificar los hechos objeto de análisis.

En efecto, la Agencia califica los citados, en la página 48 del Acuerdo, como susceptibles de infringir, por un lado, “el artículo 5.1.f) y 5.2 del RGPD”, cuya sanción se recoge en el artículo 83.5.a) del RGPD; y por otro, “de los artículos 25 y 32 del RGPD”, sancionado en el artículo 83.4.a) del RGPD. Ante la concurrencia de dos posibles sanciones por los mismos hechos, la Agencia se acoge a lo previsto en el artículo 29.5 de la LRJSP, según la cual “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”.

XFERA discrepa de este criterio, por tres motivos principales:

a) El artículo 29.5 de la LRJSP se refiere a lo que se conoce como “concurso medial de infracciones administrativas”, que resulta de aplicación cuando una infracción más leve sirve como medio para cometer otra más grave. Para que resulte de aplicación, es necesario que se verifique la concurrencia de una pluralidad de acciones, que, a su vez, den lugar a una pluralidad de infracciones (por ejemplo, dos hechos y dos infracciones); con la particularidad de que una de ellas sea instrumento o medio necesario para la perpetración de la otra. En el caso que nos ocupa, no cabe hablar de pluralidad de acciones: existe una única acción (supuestamente, “no utilizar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales de los

clientes", página 41 del Acuerdo), que podría llegar a ser encuadrada, en principio, en dos infracciones diferentes. Al no concurrir varias acciones, no se está ante un "concurso medial", ni cabe aplicar al caso el citado artículo 29.5.

b) En ambas supuestas infracciones, la conducta antijurídica sería la misma: la insuficiencia de las medidas técnicas y organizativas aplicadas por XFERA; y el desvalor que se imputa en ambas es también el mismo, consistente en el presunto incumplimiento del deber de proteger la información de los clientes. Calificar unos mismos hechos, con un mismo autor y un mismo fundamento, como dos infracciones supone incurrir en duplicidad, lo que resulta disconforme a Derecho, al conculcar el principio non bis in idem. Tal principio se encuentra consagrado en el artículo 31.1 de la LRJSP, que dispone que "no podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento".

En definitiva, la base fáctica de la infracción imputada es coincidente, y el fundamento para sancionarla también. La única diferencia entre las dos infracciones imputadas radica en que, en la grave, la conducta sancionada consiste en la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento; y en la muy grave, la conducta sancionada consiste en vulnerar el principio del RGPD del que se deriva la necesidad de adoptar dichas medidas.

c) En el presente caso, se está ante lo que la doctrina denomina "concurso aparente de leyes". Se trata de una figura analizada en múltiples ocasiones por el Tribunal Supremo, que lo define como sigue en su sentencia de 22 de mayo de 2009 (rec. 10084/2008):"El llamado conflicto o concurso de normas se produce cuando sobre un mismo supuesto de hecho recaen dos o más preceptos normativos en cuyas respectivas hipótesis es subsumible enteramente el supuesto en conflicto (...) El conflicto de normas -en efecto-debe resolverse con la aplicación de solo una de ellas, que excluya a las demás (razón por la que algunos hablan de aparente conflicto, ya que éste finalmente desaparece a favor de una sola norma)".Sobre cuál de las normas aplicar en tales situaciones, el Tribunal Supremo lo aclaró en sentencia de 22 de septiembre de 2011 (recurso 4289/2009), al decir que "en caso de conflicto, la norma que se ajusta más exactamente al supuesto de hecho expresa de modo más complejo la valoración que del mismo efectúa el ordenamiento jurídico y prevalece sobre la que lo contempla de manera más vaga y abstracta". Al respecto, dado que la infracción específica es la grave, se concluye que, en la peor hipótesis para XFERA, la resolución sancionadora sólo podría declarar la infracción grave.

OCTAVA.- CIRCUNSTANCIAS APLICABLES AL CASO INDIVIDUAL, CONFORME AL ART. 83.2 RGPD.

En caso de no apreciarse una total falta de culpabilidad, no puede obviarse que la conducta desplegada tiene menor gravedad que la considerada en el Acuerdo:

> 8.1) SOBRE LAS "EVIDENCIAS PARA UNA POSIBLE GRADUACIÓN DE LA CUANTÍA DE LA SANCIÓN".
>
> El Informe de Actuaciones Previas de Investigación recoge, en su Anexo I (páginas 13 y 14) una serie de criterios que se listan a efectos de graduar la posible sanción a imponer a XFERA. Sobre este listado, conviene hacer una serie de matizaciones:
>
> - En relación con el carácter continuado de los hechos constatados, se refleja que "la entidad declara 44 casos detectados anualmente (2019)".

Tras revisar internamente ese dato, se ha concluido que diez de los casos inicialmente declarados 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, en el marco de la implementación de las nuevas capas de seguridad implementadas, y que se describen en el apartado 2.1. de las presentes alegaciones. Por tanto, la cifra debe ser reducida a ***CANTIDAD.6.

Llama la atención, por otra parte, que el Acuerdo de Inicio (página 46) incrementa la cuantía a ***CANTIDAD.7, entendemos que debido a alguna errata. Se insiste en que la cifra correcta es de ***CANTIDAD.6.

- A pesar de que el Informe de Actuaciones Previas reconoce que "no consta que se hayan resuelto procedimientos por infracciones a partir de los mismos hechos por parte de la entidad investigada", el Acuerdo de Inicio no tiene esta circunstancia atenuante en cuenta.

8.2) SOBRE LOS CRITERIOS DE GRADUACIÓN EFECTIVAMENTE RECOGIDOS EN EL ACUERDO.

En sus páginas 45 y siguientes, el Acuerdo analiza las supuestas circunstancias agravantes y atenuantes aplicables al caso. Al respecto:

- Sobre la "naturaleza, gravedad y duración de la infracción", la Agencia entiende que su naturaleza es muy grave, porque conlleva "una pérdida de disposición y control sobre datos personales". XFERA discrepa de esta afirmación, porque:
    - Lo que se produce es un duplicado de una tarjeta SIM, que no de datos personales: una tarjeta SIM es un dispositivo que no contiene información personal de ningún tipo; y
    - La pérdida de disposición y control sobre los datos se produce en plataformas de terceros, que emplean los mensajes SMS como método de autenticación, aun a sabiendas de su manifiesta falta de seguridad.

  Como se ha expuesto, la responsabilidad administrativa derivada de la falta de diligencia de los titulares de dichas plataformas no puede ser atribuida a XFERA.

- En el mismo apartado, y en cuanto a la duración, la Agencia manifiesta que los hechos abarcan "un periodo superior a 9 meses", puesto que el "último de los casos no presentados ante esta Agencia" se produjo el 12 de abril de 2020. Como se ha acreditado, ese concreto caso fue detectado por las sucesivas capas de seguridad implementadas por XFERA, y no dio lugar a fraude alguno. A estos efectos, las fechas a tener en cuenta deberían ser las siguientes:
    - El 28 de noviembre de 2019, fecha en la que se activaron las nuevas medidas de seguridad por parte de Masmóvil, que funcionó con 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; o en su defecto

- El 20 de enero de 2020, fecha del último de los casos obrantes en el expediente en los que se corroboró fraude;

- Número de interesados afectados: como se ha dicho, el número de casos detectados en 2019 fue de ***CANTIDAD.6, y no de ***CANTIDAD.7, como indica el Acuerdo. Esta cifra se redujo a 3 en 2020, teniendo en ese año XFERA casi 7,2 millones de líneas móviles, como resultado de la aplicación de las nuevas medidas de seguridad por parte de XFERA;
- Nivel de los daños y perjuicios sufridos: la Agencia los considera graves, pero XFERA discrepa de esta afirmación. Los únicos daños sufridos son los derivados del coste de la duplicación de la tarjeta SIM (6€ + IVA), que han sido restituidos a todos los afectados que los han reclamado. El fraude bancario que recoge el Acuerdo no es responsabilidad de XFERA, sino de las entidades financieras que utilizan los SMS como medida de autenticación, aun a sabiendas de su falta de seguridad. Responsabilizar administrativamente a XFERA supone una quiebra inadmisible del principio de personalidad, recogido en el artículo 28 de la LRJSP y en el artículo 25.1 de la Constitución;
- Supuesta negligencia de XFERA: no ha podido ser acreditada por la Agencia. El personal de XFERA fue engañado por delincuentes, y presumir su falta de diligencia supone vulnerar la doctrina de la Audiencia Nacional, según la cual “no cabe apreciar culpabilidad alguna (ni siquiera a título de culpa o falta de diligencia) en la actuación de la entidad recurrente, que actuó en la creencia de que la persona con la que contrataba era quien decía ser y se identificaba como tal con una documentación en apariencia auténtica y a ella correspondiente”;
- Grado de responsabilidad: la Agencia estima que es “alto”, pero no justifica por qué, a pesar de que el artículo 83.2.d) RGPD establece que debe ser puesto en relación a “las medidas técnicas u organizativas que se hayan aplicado en virtud de los artículos 25 y 32”de la misma norma. Se ha acreditado que existían unos procedimientos de seguridad razonables, en relación con el riesgo previsible para la empresa en el momento de los hechos; y que con posterioridad, los procedimientos de seguridad se han reforzado de forma extraordinaria, con resultados sobresalientes. Entender como “alto” el grado de responsabilidad, a la vista de lo anterior, carece de toda lógica;
- Categorías de datos personales afectados: sorprende que la Agencia considere que una tarjeta SIM es una categoría de datos personales cuyo acceso no autorizado es “particularmente grave”. Las tarjetas SIM no son datos de carácter personal: son meros soportes, y cuando se activa un duplicado, están vacíos de contenido. Lo cierto y verdad es que no hay categoría alguna de datos personales afectados por esta operativa, en lo que a los operadores de telefonía móvil se refiere.

8.3) SOBRE LA DESPROPORCIÓN DEL IMPORTE DE LA SANCIÓN PROPUESTA.

Cabe destacar que, en caso de no apreciarse una total falta de culpabilidad, en cualquier caso debería apreciarse una cualificada disminución de la culpabili-

dad de XFERA o, cuando menos, de la antijuridicidad de los hechos de los que trae causa el presente procedimiento, lo que determinaría la procedencia de reducir la gravedad de las infracciones a ella atribuidas y, por ende, a reducir la sanción a imponer. En efecto, atendidos los argumentos anteriores de culpabilidad, aunque no fueran estimados, no podría obviarse que, por las circunstancias concurrentes, la conducta desplegada tiene menor gravedad que la considerada por el Acuerdo. Habida cuenta, además, de que la práctica totalidad de las circunstancias agravantes en él incluidas no resultan de aplicación al caso, se concluye que sólo cabe reducir las sanciones que eventualmente se impongan. Máxime, cuando el esfuerzo realizado por XFERA para adecuar sus procedimientos de seguridad a la nueva realidad derivada del "SIM swapping" es más que notable, y sus resultados, excepcionales.

DÉCIMO QUINTO: Con fecha 5 de mayo de 2021, la instructora del procedimiento acuerda la apertura de un período de práctica de pruebas, que se notifica a XFERA, en fecha 5 de mayo de 2021, en los siguientes términos:

*"1. Se dan por reproducidas a efectos probatorios las reclamaciones interpuestas por **A.A.A., E.E.E.** y su documentación. También, los documentos obtenidos y generados por los Servicios de Inspección ante XFERA MÓVILES, S.A, y el Informe de actuaciones previas de la Subdirección General de Inspección de Datos que forman parte del expediente **E/11418/2019.***

*2. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio **PS/00027/2021** presentadas por XFERA MÓVILES, S.A. en fecha 8 de marzo de 2021 a través del Registro General de esta Agencia, y la documentación que a ellas acompaña:*

- *Doc. 1. Oficio del Juzgado de Instrucción N.º 9 de Alicante*
- *Doc. 2. Requerimiento SEAD*
- *Doc. 3. Evaluación de impacto en materia de protección de datos*
- *Doc. 4. Análisis de riesgos*
- *Doc. 5. Protocolo cambio de SIM*
- *Doc. 6. Tabla duplicados de SIM*
- *Doc. 7. Archivo de audio: *****TELEFONO.4***
- *Doc. 8. Archivo de audio: *****TELEFONO.7***
- *Doc. 9. Archivo de audio: *****TELEFONO.10***
- *Doc. 10. Archivo de audio: *****TELEFONO.13***
- *Doc. 11. Archivo de audio: *****TELEFONO.19***
- *Doc. 12. Convocatoria AEPD*
- *Doc. 13. Acta AEPD"*

DÉCIMO SEXTO: Con fecha 4 de octubre de 2021, la instructora del procedimiento formula Propuesta de Resolución, en la que propone que por la directora de la AEPD se sancione a ***XFERA MÓVILES, S.A.***, con NIF ***A82528548***, por infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1.a) de la LOPDGDD, con una multa administrativa de 250.000'00 (doscientos cincuenta mil euros).

Con fecha 4 de octubre de 2021, a través del Servicio de Notificaciones Electrónicas y

Dirección Electrónica Habilitada, se notifica la Propuesta de Resolución.

DÉCIMO SÉPTIMO: Con fecha 8 de octubre de 2021, XFERA solicita la ampliación del plazo para formular alegaciones a la Propuesta de resolución.

DÉCIMO OCTAVO: Con fecha 13 de octubre de 2021, la Agencia concede la ampliación instada.

DÉCIMO NOVENO: Con fecha 26 de octubre de 2021, XFERA formula alegaciones a la Propuesta de Resolución, en las que manifiesta, en síntesis, lo siguiente:

PRIMERA. Disconformidad con la calificación de la supuesta infracción.

Alega que la AEPD realizó una incorrecta calificación del supuesto de hecho, derivada de una inadecuada interpretación del llamado "principio de especialidad".

XFERA recuerda que en el Acuerdo de Inicio del procedimiento, la Agencia calificó los hechos como susceptibles de infringir, por un lado, *"el artículo 5.1.f) y 5.2 del RGPD"*, cuya sanción se recoge en el artículo 83.5.a) del RGPD; y por otro, *"de los artículos 25 y 32 del RGPD"*, sancionado en el artículo 83.4.a) del RGPD. Y que ante la concurrencia de dos posibles sanciones por los mismos hechos, la Agencia alegó lo previsto en el artículo 29.5 de la LRJSP: *"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"*.

La mencionada calificación jurídica era, en opinión de XFERA, contraria a Derecho, y así se reflejó en el escrito de alegaciones al Acuerdo de Inicio del presente procedimiento sancionador, principalmente por tres motivos:

1. Porque el artículo 29.5 de la LRJSP se refiere al concurso medial de infracciones administrativas, para el cual es necesario que se verifique la concurrencia de una pluralidad de acciones que, a su vez, den lugar a una pluralidad de infracciones; con la particularidad de que una de ellas sea instrumento o medio necesario para la perpetración de la otra. Algo que no ocurre en este supuesto, en el que se produce una única acción;

2. Porque tanto los hechos, como la conducta antijurídica y el desvalor imputado mediante ambas infracciones serían los mismos, lo que vulneraría el principio *"non bis in idem"*; y

3. Porque realmente nos encontramos ante un *"concurso aparente de leyes"*, y tal supuesto debe resolverse con la aplicación de solo una de ellas, que debe ser la que se ajuste más exactamente al supuesto de hecho. Esta máxima es conocida por la doctrina como *"principio de especialidad del derecho administrativo sancionador"*.

XFERA alega que la propuesta de resolución acoge parcialmente esta alegación, pero lo hace reconduciendo la imputación de las infracciones inicialmente consideradas a una única infracción, derivada de la vulneración del artículo 5.1.f) del RGPD. Y que es esta reconducción la que, en opinión de XFERA, continúa vulnerando el citado princi-

pio de especialidad, como se expondrá a continuación.

La figura del concurso aparente de leyes fue analizada en múltiples ocasiones por el Tribunal Supremo, que lo define como sigue en su sentencia de 22 de mayo de 2009 (rec. 10084/2008):

"El llamado conflicto o concurso de normas se produce cuando sobre un mismo supuesto de hecho recaen dos o más preceptos normativos en cuyas respectivas hipótesis es subsumible enteramente el supuesto en conflicto (…) El conflicto de normas -en efecto- debe resolverse con la aplicación de solo una de ellas, que excluya a las demás (razón por la que algunos hablan de aparente conflicto, ya que éste finalmente desaparece a favor de una sola norma)".

Sobre cuál de las normas aplicar en tales situaciones, el Tribunal Supremo lo aclaró en sentencia de 22 de septiembre de 2011 (recurso 4289/2009), en los siguientes términos:

"Este conflicto de leyes debe resolverse mediante la aplicación del principio genérico de especialidad, que se desglosa en una serie de reglas que, como es sabido, en la actualidad se contienen en el art. 8 CP, y que responden a una misma idea, a saber: la de que en caso de conflicto, la norma que se ajusta más exactamente al supuesto de hecho expresa de modo más complejo la valoración que del mismo efectúa el ordenamiento jurídico y prevalece sobre la que lo contempla de manera más vaga y abstracta. (…)
Conviene aclarar que la circunstancia de que tales reglas se contengan en un precepto del CP y que la LGT no efectúe una expresa remisión al mismo no implica, sin embargo, que no deban emplearse en el ámbito del procedimiento administrativo sancionador, dado que el referido art. 8 del CP no viene más que a recoger criterios de interpretación para determinar la Ley o precepto legal aplicable que ya venían siendo asumidos por la doctrina penalista y aplicados por la jurisprudencia del Tribunal Supremo".

Pues bien, XFERA entiende que la instructora yerra al subsumir las conductas, no en el artículo más exacto y concreto, sino en aquel otro más vago y abstracto, vulnerando así la doctrina del Tribunal Supremo. En concreto, califica la conducta como *"el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679"*, cuando la LOPDGDD tipifica otra conducta que se ajusta de forma mucho más exacta al supuesto de hecho, a su entender, cual es *"la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679"*.

Además, XFERA entiende que, en el presente caso, la propia Agencia reconoce en múltiples ocasiones que el motivo de la sanción no es la ausencia de medidas de seguridad, sino su supuesta insuficiencia. Así se expresa, por ejemplo, en la página 84 de la propuesta de resolución, donde se afirma que:

"Así, la infracción deviene no por la carencia de una política específica de seguridad para la expedición de los duplicados SIM, sino por la necesidad de su revisión y refuerzo".

Es más, en la página 79 de la propuesta se verbaliza la intención de la Agencia con la sanción:

"En este sentido, esta Agencia quiere reforzar la necesidad de mejorar esta primera capa de seguridad que es la que da acceso a la obtención fraudulenta de un duplicado de una tarjeta SIM por parte de los delincuentes".

XFERA considera que si tanto la LOPDGDD como el propio Reglamento recogen una infracción específica derivada del incumplimiento del artículo 32 de esta última norma, es porque la intención del legislador era que los incumplimientos en materia de seguridad contasen con una tipificación propia. Y que al no aplicarla en el presente caso, la Agencia se aparta del espíritu de la norma, vacía de contenido el artículo 73.f) de la LOPDGDD e ignora el principio de especialidad aplicable al derecho administrativo sancionador, apartándose así de la doctrina consolidada del Tribunal Supremo.

Del mismo modo, XFERA entiende que la Agencia incurre en una clara incongruencia con sus propios actos y, en concreto, con procedimientos anteriores en los que las entidades responsables no habrían adoptado las medidas de seguridad adecuadas, y se les sanciona (aplicando correctamente el principio de especialidad, y a pesar de la gravedad de los hechos) por incumplimiento del artículo 32 del RGPD, y no del artículo 5.

Se citan, por ejemplo:

i. El ***PS/00362/2021***, donde el BBVA es sancionado porque *"la entidad reclamada facilita el detalle de los últimos movimientos de la tarjeta Affinity Card mediante un sistema de atención telefónica automatizado en el teléfono ***TELÉFONO.1 en el que únicamente se pide como dato identificativo el DNI del cliente"*, y la sanción se apoya en *"la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) del RGPD"*; y

ii. El ***PS/00179/2020***, donde Air Europa es sancionada porque un *"hacker comprometió una serie de sistemas"* de la empresa, habiéndose confirmado *"que el atacante había recopilado 488847 tarjetas de crédito únicas"* de sus clientes; y la sanción se basa de nuevo en *"una infracción del artículo 32.1 del RGPD, tipificada en el Artículo 83.4.a) del RGPD"*.

XFERA alega que, a pesar de haberse planteado este argumento en las alegaciones planteadas frente al Acuerdo de Inicio, esta Agencia no ha aclarado el motivo por el cual ha decidido calificar la conducta como infracción del artículo 5 del RGPD, y no del artículo 32. Y que ello es causa suficiente para hablar no solo de una clara incongruencia omisiva (por incumplir el deber de motivación de las resoluciones previsto en el artículo 89.3 de la Ley 39/2015), sino también de una actuación arbitraria, proscrita por el artículo 9.3 de la Constitución, en la que se evidencia un trato discriminatorio con otros administrados.

Habida cuenta de lo anterior, XFERA entiende que la calificación de la conducta debería basarse, también en este caso, en la infracción de lo establecido en el artículo 32 del RGPD, tipificada en el artículo 83.4.a) del citado Reglamento, y calificada como grave a efectos de prescripción en el artículo 73.f) de la LOPDGDD. Y que, en la medi-

da en que, en el Acuerdo de Inicio, se valoró inicialmente la multa administrativa por esta causa en 100.000€, tal debería ser la cuantía máxima de la sanción a imponer.

SEGUNDA. XFERA no ha quebrantado el principio de confidencialidad del dato.

Según se refleja en el Fundamento de Derecho (en lo sucesivo, FD) quinto de la Propuesta de Resolución, *"esta Agencia considera que, en ambos casos, lo que se está analizando es la vulneración del principio de confidencialidad del dato al haber realizado el duplicado de la tarjeta SIM sin contar con las medidas de seguridad adecuadas"*. También se afirma que *"tanto los datos que se tratan para emitir un duplicado de tarjeta SIM como la tarjeta SIM (Subscriber Identity Module) que identifica de forma inequívoca y unívoca al abonado en la red, son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos"*.

XFERA entiende que la Agencia se equivoca al realizar ambas afirmaciones.

Dado que dato personal se define como *"**toda información** sobre una persona física identificada o identificable"* (la negrita es de XFERA). XFERA alega que, por definición, tanto los datos como la información son recursos intangibles, por lo que resulta inaceptable que una "tarjeta SIM", que es un objeto físico, sea considerada por esta Agencia como "dato personal". No lo es, como tampoco lo son un teléfono móvil, un ordenador, una memoria USB o una tarjeta de crédito: todos ellos son meros soportes; y de hecho, su naturaleza encaja plenamente con la definición que de "soporte" ofrecía el Real Decreto 1720/2007, de 21 de diciembre, que desarrollaba la antigua LOPD: *"Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos".*

XFERA aduce que una tarjeta SIM es un objeto físico, que como reconoce la propia Propuesta de Resolución, (1) es susceptible de almacenar datos, (2) puede ser utilizado en sistemas de información, por medio de un teléfono móvil y (3) permite grabar y recuperar información; y de hecho, la propuesta recoge, en su página 72, que *"la tarjeta SIM constituye el soporte físico a través del cual se accede a los datos de carácter personal"*.

Y alega que la contradicción en la que incurre la propia Agencia es evidente.

Asentado lo anterior, XFERA aduce que, tal y como se ha destacado en las alegaciones realizadas al Acuerdo de Inicio, la tarjeta SIM que se entrega al usuario al realizar un duplicado está en blanco, esto es, todavía no contiene datos de carácter personal de ningún tipo. Y que, al contrario de lo que afirma la Agencia en su resolución, el MSISDN (esto es, el número de teléfono del usuario) no se almacena en la tarjeta SIM. Recuerda XFERA que se ha aportado al expediente información, publicada por el regulador nacional en la materia (la CNMC) en la que se expresa, negro sobre blanco y literalmente, que *"en la tarjeta SIM no se almacena nuestro número de teléfono MSISDN"*; pero a pesar de ello, y persistiendo en su error, la Agencia insiste en afirmar que esta tipo de tarjetas *"contiene[n] un chip en el que se almacena el MSISDN"* y que *"la tarjeta SIM identifica un número de teléfono"*. XFERA considera que esas afirmaciones son, sencillamente, ajenas a la realidad.

XFERA alega que la tarjeta SIM únicamente incluye claves criptográficas y un número de serie, denominado IMSI, que no se refiere a persona alguna: únicamente identifica a la propia tarjeta. Y que 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 un MSISDN al IMSI de dicha tarjeta SIM. Considera XERA que 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, cuyo contenido permanece inalterado y, por tanto, vacío de todo dato personal.

XFERA destaca que, en relación con el IMSI incluido en la tarjeta duplicada, en ningún momento es utilizado en el teléfono móvil del titular de la línea, por lo que tampoco es posible asociarlo con esta persona: en todo caso, podría llegar a asociarse con el delincuente que realiza el duplicado ilícito de la citada tarjeta, pero toda vez que su identidad es desconocida, no estaríamos ante un dato de carácter personal.

XFERA también llama la atención sobre que, en la Propuesta de Resolución, se hace referencia al IMEI, dado que 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. En el caso que nos ocupa, el IMEI sería nuevamente el del teléfono del delincuente, toda vez que estamos hablando del duplicado de tarjetas SIM, no de clonado de teléfonos móviles; e insistimos en que su identidad es desconocida. De ahí que XFERA entienda que carece de sentido utilizarlo para justificar la existencia de un tratamiento de datos personales, más allá de que la instructora se haya podido confundir por la profusión de acrónimos utilizados en el sector.

En definitiva, XFERA alega que el usuario que obtiene un duplicado de una tarjeta SIM recibe un soporte en blanco, que no contiene información alguna. Los datos personales del titular de la línea permanecen, en todo momento, custodiados en los servidores de XFERA, por lo que el acceso a una copia de la tarjeta SIM no supone ningún tipo de pérdida de disposición o control sobre dichos datos. Por tanto, en opinión de XFERA, en el presente caso no existe vulneración alguna de la confidencialidad de los datos de los afectados en el tratamiento consistente en el duplicado de la tarjeta SIM, y no se ha aportado una sola prueba en este procedimiento que contradiga esta afirmación.

TERCERA. Vulneración de los principios de personalidad de la sanción y de tipicidad.

XFERA destaca de la Propuesta de Resolución lo siguiente:

“Al respecto, esta Agencia recuerda que para completar la estafa objeto del «SIM swapping», es necesario que un tercero “suplante la identidad” del titular de los datos ante la entidad financiera. Lo que conlleva a priori, un tratamiento al margen del principio de licitud pues un tercero está tratando datos, ya que tiene acceso a ellos, sin base legal alguna, además de la vulneración de otros principios como el de confidencialidad.”

Y manifiesta que “escapa a toda lógica” que, siendo consciente esta autoridad de control de que son el delincuente y la entidad financiera los sujetos responsables de la conducta antijurídica que se pretende erradicar (cual es *“evitar este tipo de estafas”*,

según la Propuesta de Resolución), este expediente se dirija únicamente contra esta compañía de comunicaciones. Y señala que, en lenguaje coloquial, en lugar de dirigirse al origen del problema, parece que esta Agencia opta por "atacar al mensajero"; algo que, como se ha expuesto en anteriores alegaciones, es contrario al principio de personalidad de la sanción, previsto en el artículo 25.1 de nuestra Constitución. Se trata de uno de los pilares del derecho punitivo del Estado, que conlleva *"la imposibilidad de la traslación de las consecuencias sancionadoras sobre personas o entidades distintas de los autores de los hechos punibles"*, en palabras de la Audiencia Nacional, que cita la doctrina de nuestro Tribunal Constitucional en la materia como sigue:

"La Sentencia del Tribunal Constitucional 219/1988 , de 22 de diciembre , proclamó que el principio de personalidad de las sanciones o de responsabilidad personal por hechos propios impide un indebido traslado de la responsabilidad punitiva a persona ajena al hecho infractor, pues ello comportaría aceptar un régimen de responsabilidad objetiva que vulneraría la exigencia de dolo o culpa necesarios para la existencia de infracción administrativa".[1]

XFERA aduce que, en el presente caso, la Agencia ancla la responsabilidad de la conducta en que, al facilitar XFERA duplicados SIM a terceras personas distintas al titular de la línea, se concede un acceso no autorizado a los datos personales de los afectados, y por tanto se dan los elementos para atribuir responsabilidad a mi representada. Sin embargo, XFERA entiende que este planteamiento es contrario a Derecho, por tres motivos:

1. En primer lugar porque, como se ha expuesto, la SIM a la que accede el delincuente está vacía de todo contenido. El delincuente no accede a ningún dato personal de la víctima durante el proceso del duplicado de la tarjeta, porque todos los tratamientos de datos del cliente necesarios para activar la tarjeta se realizan exclusivamente en los servidores de XFERA, que no se ven violentados en esta operativa. Y XFERA entiende que en ningún momento ha logrado demostrar esta Agencia que se haya producido, en este procedimiento, acceso no autorizado a datos personales que sean objeto de tratamiento por XFERA;

2. En segundo lugar, porque el duplicado de la SIM únicamente da acceso al delincuente a la línea telefónica de la víctima, y a través de ella, al contenido de los mensajes que se puedan enviar y recibir. Sin embargo:

   a. La actividad de XFERA, en relación con dichos mensajes, es de mera intermediación en la transmisión de datos. Por tanto, no puede considerarse responsable a XFERA ni por transmitir ni por facilitar acceso a dicha información, pues está exenta de toda responsabilidad al respecto, conforme al artículo 14.1 de la LSSI, que reza:

   "Los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que presten un servicio de intermediación que consista en transmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o en facilitar acceso a ésta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado éstos o a los destinatarios de dichos datos."

   b. Adicionalmente, dicho acceso no supone una vulneración del derecho

a la protección de datos, sino, en todo caso, de otro derecho fundamental muy relacionado, pero autónomo e independiente: el secreto de las comunicaciones, cuya tutela escapa al ámbito competencial de esta Agencia; y

3. En tercer lugar porque si bien, a través de los mensajes recibidos, el delincuente podría acceder a datos personales de la víctima, XFERA no puede ser considerada responsable de tales hechos. Aunque sea innegable que, tras lograr el duplicado de la tarjeta, el delincuente puede lograr *"el control de los SMS dirigidos al teléfono vinculado a la tarjeta SIM inicial"* (página 74 de la propuesta), también lo es que 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 LOPD.

A este respecto, XFERA alega que el considerando 74 del RGPD, invocado por esta Agencia en la Propuesta de Resolución, es claro cuando afirma que *"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales* ***realizado por él mismo o por su cuenta****"* (la negrita es XFERA). No es el caso, por lo que, en opinión de XFERA, de acuerdo con el principio de tipicidad, la conducta de XFERA no puede ser objeto de sanción, en relación con dichos tratamientos.

XFERA aduce que, en definitiva, el único argumento esgrimido por esta Agencia (página 83) es que *"si se evitara desde las operadores el acceso a las tarjetas SIM por parte de estos delincuentes, éstos no podrían beneficiarse las posibilidades que ofrece la banca online para obtener su beneficio"*. Y que es una valoración basada en meras suposiciones que obvia que el mismo objetivo se conseguiría si la banca online dejase de utilizar el SMS, un método manifiesta e intrínsecamente inseguro, para enviar credenciales de autenticación a sus clientes; o si en vez de enviar las propias claves de autenticación como parte de los mensajes, realizasen preguntas más robustas, como se sugiere a este operador en la página 76 de la Propuesta de Resolución. Todo ello, por lo demás, en línea con lo resuelto por los tribunales en casos similares: sin ir más lejos, así lo ha analizado el Tribunal Supremo (sala segunda) en su reciente sentencia de 12 de febrero de 2020 (recurso 10.169/2019), que atribuye la responsabilidad en estos supuestos a las entidades bancarias:

"En casos como el presente, es claro que la actividad propuesta por la entidad bancaria a sus clientes mediante la operativa online presenta algunos riesgos derivados de la posibilidad de suplantación de la identidad de quien contrata con la entidad para la realización de operaciones sin la autorización del auténtico contratante. Es claro también que, excluyendo actuaciones dolosas o gravemente negligentes por parte de los clientes, la entidad bancaria es responsable de ofrecer y poner en práctica un sistema seguro, de manera que las consecuencias negativas de los fallos en el mismo no deberán ser trasladados al cliente".

XFERA entiende que la posición del Supremo es clara: es el banco, y no la compañía de telecomunicaciones, el *"responsable de ofrecer y poner en práctica un sistema seguro"*; y en ningún momento ha sido XFERA contratada (o siquiera contactada) por las

entidades financieras para *securizar* sus sistemas, por lo que no tiene sentido culpar a XFERA por las consecuencias negativas derivadas de la debilidad del método de autenticación elegido. Una debilidad que la propia Agencia reconoce en su propio sitio web, en el que recomienda a los usuarios, literalmente: *"Evitar los SMS como método de autenticación en dos pasos"*.[2]

Lo cierto y verdad, continúa XFERA, es que las entidades bancarias optaron por activar la autenticación mediante SMS sin contar en ningún momento con la opinión de los operadores de telecomunicaciones, y sin considerar que sus obligaciones en materia de seguridad no son únicamente las dictadas por la Directiva PSD2, sino también las impuestas por el RGPD. Y considera que sancionar a XFERA por la irresponsabilidad de la banca, por tanto, no es solo materialmente injusto, sino que carece de sostén normativo.

CUARTA. Vulneración del principio de culpabilidad.

4.1. XFERA no había identificado el riesgo, simplemente, porque no existía antes de PSD2.

XFERA cita el RGPD, en su artículo 32, que establece: *"el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*. Y recuerda que, en cuanto al concepto de "riesgo", esta Agencia lo analiza en su "Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD", en cuya página 5 se recoge lo siguiente:

"Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados: en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar."

Alega XFERA que, en el presente caso, la amenaza que originó el riesgo del que trae causa este expediente nació en 2019, con la entrada en vigor de una normativa (la Directiva (UE) 2015/2366, o PSD2) que comenzó a aplicarse el 14 de septiembre de dicho año. Hasta entonces, las entidades financieras no utilizaban el SMS como doble factor de autenticación, por lo que no se producían casos de duplicado fraudulento de tarjetas SIM para cometer estafas.

Dado que la identificación del riesgo implica considerar la amenaza que lo puede originar, y habida cuenta de que la amenaza no existía con anterioridad a la aplicación de la Directiva PSD2, entiende que era imposible que XFERA hubiese identificado dicho riesgo. Así se manifestó en el escrito de alegaciones, al indicar que XFERA no tuvo conocimiento efectivo de esta problemática 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.

Ante estas noticias, XFERA reforzó los procedimientos de identificación y se activaron dos capas de seguridad adicionales, que comenzaron a aplicarse el 28 de noviembre de 2019. Todo ello, en línea con lo recomendado por la Agencia en la citada Guía:

"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".

Se alega que eso fue, exactamente, lo que hizo XFERA; y a pesar de cumplir con lo recomendado por esta Agencia, con todo, se la sanciona, basándose en una suerte de responsabilidad objetiva derivada de su condición de *"depositaria de datos de carácter personal a gran escala"*. Por desgracia, y en contra de lo que parece manifestar esta autoridad de control, aduce XFERA que las grandes empresas no cuentan con dotes adivinatorias, en especial cuando el riesgo nace de la forma en la que determinadas entidades financieras aplicaron una nueva normativa, sin contar para ello con los operadores de telecomunicaciones.

Y manifiesta que le resulta particularmente sorprendente el siguiente extracto de la Propuesta de Resolución (página 84):

"Es decir, desde la óptica de la culpabilidad, estamos ante un error vencible, ya que con la aplicación de las medidas técnicas y organizativas adecuadas, estas suplantaciones de identidad se hubieran podido evitar. Máxime cuando XFERA admite en sus alegaciones que antes del 26 de septiembre de 2019 ni tan siquiera había identificado el riesgo".

XFERA indica que le resulta sorprendente porque, en el presente caso, no se trata de que XFERA no hubiese identificado un riesgo previamente existente, por falta de cuidado en el análisis de las amenazas que se pudieren materializar. Antes al contrario, se trata de un riesgo que, directamente, no existía. Y se pregunta: ¿cómo cabe, pues, calificarlo de "error vencible"? Continúa diciendo XFERA que la propia Agencia reconoce que no tuvo noticias de esta operativa hasta que (página 5):

"Con fecha 27 de noviembre de 2019, la directora de la AEPD, ante las noticias aparecidas en medios de comunicación relativas a la utilización de prácticas fraudulentas basadas en la generación de duplicados de tarjetas SIM sin el consentimiento de sus legítimos titulares con objeto de acceder a información confidencial con fines delictivos (conocidas como "SIM Swapping"), insta a la Subdirección General de Inspección de Datos (en lo sucesivo, SGID) a iniciar de oficio las Actuaciones Previas de Investigación tendentes a analizar estas prácticas y las medidas de seguridad existentes para su prevención".

Y que, para cuando la directora de la AEPD conoció de la existencia de la práctica conocida como SIM swapping, XFERA ya había reaccionado, mediante el desarrollo de su nuevo sistema de seguridad Alerta FSM, que fue implementado esa misma semana, con unos resultados magníficos. Y a pesar de la importante y ágil mejora en sus medidas de seguridad, que la propia Agencia alaba, XFERA se ve abocada al pago de una importantísima sanción, que vulnera de forma grosera el principio de culpabilidad consagrado en los artículos 28 de la LRJSP, y 25.1 de la Constitución. Como reconoció el Tribunal Supremo, en su sentencia de 1 de octubre de 1988 (recurso 1652/1996), *"el reproche culpabilístico tendría que centrarse, esencialmente, en la pre-*

visibilidad del resultado dañoso"; previsibilidad que, en opinión de XFERA, la Agencia no ha logrado acreditar en los hechos de los que trae causa este expediente.

4.2. XFERA actuó en la creencia de que la persona que solicitaba el duplicado era quien decía ser.

Recuerda XFERA que el personal de la entidad fue sujeto pasivo de un delito de falsedad documental en concurso medial con otro de estafa, perpetrado por delincuentes que acuden a sus establecimientos exhibiendo documentación oficial falsa. Y que, como recoge el Código Penal, el tipo de estafa es cometido por quienes, *"con ánimo de lucro, utilizaren* ***engaño bastante para producir error en otro****, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno"*; y como expresa el Tribunal Supremo (sentencias de 1 de marzo de 2004, en el recurso 3056/2002, y de 9 de octubre de 2005, en el recurso 86/2004):

"el concepto de engaño bastante, no puede servir para desplazar en el sujeto pasivo del delito todas las circunstancias concurrentes desplegadas por el ardid del autor del delito, de manera que termine siendo responsable de la maquinación precisamente quien es su víctima"

XFERA cita como ejemplo el caso del Sr. Torrado, donde, en su opinión, es evidente que el estafador hizo cuanto estaba en su mano para conseguir el resultado engañoso que en efecto se produjo, incluyendo la manipulación mediante programas informáticos de edición de imagen de un DNI y de una denuncia policial. Esta documentación fue conservada en los sistemas de XFERA y ha sido aportada al expediente, demostrando que el procedimiento de verificación de identidad estaba siendo efectivamente aplicado por parte de las tiendas. XFERA considera que no puede derivarse de este hecho, por tanto, ningún tipo de responsabilidad sustentada en una supuesta culpabilidad o falta de diligencia, pues la documentación presentada aparentaba estar en regla; y así lo ha reconocido la jurisprudencia en casos similares, de los que se aportan como ejemplo los siguientes:

i. Sentencia de la Audiencia Nacional de 20 de marzo de 2013 (rec. 581/2011, en relación con el PS/00130/2011): *"La Sala considera que sobre esos dos contratos del mismo nombre sobre el que constan, aunque sea a posteriori, todos los documentos acreditativos, no hay falta de diligencia, en el sentido exigido en el art. 130.1 LRJyPAC, al constar los documentos que acreditaban el supuesto consentimiento inequívoco, que posteriormente se revelaron fraudulentos".*

ii. Sentencia de la Audiencia Nacional de 29 de octubre de 2009 (rec. 797/2008, en relación con el PS/00290/2008): *"Por todo lo cual y a la vista de las especiales circunstancias concurrentes en el caso de autos, no cabe apreciar culpabilidad alguna (ni siquiera a título de culpa o falta de diligencia) en la actuación de la entidad recurrente, que actuó en la creencia de que la persona con la que contrataba era quien decía ser y se identificaba como tal con una documentación en apariencia auténtica y a ella correspondiente, por lo que estaba legitimada para el tratamiento de sus datos de carácter personal"*. Las sentencias de 18 de marzo de 2010 (rec. 342/2009) y de 22 de marzo de 2012 (rec. 9/2009) reproducen este criterio.

XFERA aduce que es innegable que, como afirma la Agencia, las medidas de seguri-

dad implementadas no lograron evitar que se duplicaran las tarjetas SIM; pero también lo es que si las medidas no alcanzaron su objetivo se debió a que los delincuentes lograron engañar al personal de XFERA, superando los procedimientos establecidos mediante documentación falsa; y que al detectarse esta nueva operativa, XFERA reforzó estas medidas de seguridad, logrando detectar y bloquear la inmensa mayoría de los intentos de fraude perpetrados por los delincuentes.

Por otra parte, XFERA cita la Propuesta de Resolución (página 76):

"Si bien esta Agencia reconoce la mejora producida en los procedimientos implantados, no deja de resultarle llamativo que en el canal presencial no se revisaran elementos del DNI en sí que pudieran dar pistas sobre si se trataba de un documento original o una falsificación. Tampoco se ha constatado que se hubiera dado formación o material al respecto a los agentes encargados de esta tarea, que son los que realizan esa comprobación de la identificación de la persona".

Al respecto, XFERA alega que impartió formación a los trabajadores sobre la comprobación de los elementos de seguridad de DNI y pasaporte, pues forma parte del curso que reciben al comenzar a trabajar en la empresa. Y que, como se puede apreciar en el material que se acompaña como **Documento 1** de las presentes alegaciones, la información es exhaustiva y recoge los tipos de documentos identificativos más utilizados en España. Menciona XFERA que esta información permanecía publicada en el "Portal Comercial" de la empresa, disponible para su consulta por el personal en cualquier momento. Y que si no se facilitó en un momento anterior es porque la Agencia, simplemente, no lo solicitó; por lo que se solicita que sea tenido en cuenta a los efectos oportunos.

También afirma la Agencia que *"no se cuestiona que los agentes de XFERA no cumplieran con los procedimientos establecidos, sino que se trata de que las medidas previstas no eran adecuadas"*. Ahora bien, destaca XFERA que la norma no exige la absoluta eficacia de las medidas de seguridad, sino que resulten *"apropiadas para garantizar un nivel de seguridad adecuado al riesgo"* (artículo 32 del RGPD), y, en su opinión, la AEPD no ha logrado demostrar esa falta de adecuación al riesgo conocido, con la información disponible en el momento en el que tuvieron lugar los hechos de los que trae causa el presente procedimiento.

QUINTA. Circunstancias aplicables al caso individual, conforme al art. 83.2 RGPD.

En sus páginas 99 y siguientes, la Propuesta de Resolución analiza las supuestas circunstancias agravantes y atenuantes aplicables al caso. Al respecto, XFERA señala:

- Sobre la naturaleza, gravedad y duración de la infracción, la Agencia entiende que su naturaleza es muy grave, porque conlleva *"una pérdida de disposición y control sobre datos personales"*. XFERA discrepa de esta afirmación, porque como ya se ha expuesto:
    - Lo que se produce es un duplicado de una tarjeta SIM, que no contiene datos personales: una tarjeta SIM es un dispositivo que no contiene información personal de ningún tipo; y
    - La pérdida de disposición y control sobre los datos se produce en plataformas de terceros, que emplean los mensajes SMS como método de

autenticación, aun a sabiendas de su manifiesta falta de seguridad. XFERA entiende que la responsabilidad administrativa derivada de la falta de diligencia de los titulares de dichas plataformas no puede ser atribuida a XFERA, porque únicamente ostenta la posición de "tercero" en relación con dichos tratamientos.

- Sobre el nivel de los daños y perjuicios sufridos: la Agencia los considera altos, pero XFERA discrepa de esta afirmación. Entiende que los únicos daños sufridos son los derivados del coste de la duplicación de la tarjeta SIM (6€ + IVA), que han sido restituidos a todos los afectados que los han reclamado. Alega que el fraude bancario que recoge el Acuerdo no es responsabilidad de XFERA, sino de las entidades financieras que utilizan los SMS como medida de autenticación, aun a sabiendas de su falta de seguridad. Y que responsabilizar administrativamente a XFERA supone una quiebra inadmisible del principio de personalidad, recogido en el artíuclo 28 de la LRJSP y en el artículo 25.1 de la Constitución.

- . Sobre la supuesta negligencia de XFERA: XFERA entiende que no ha podido ser acreditada por la Agencia. Y que el personal de XFERA fue engañado por delincuentes, y presumir su falta de diligencia supone vulnerar la doctrina de la Audiencia Nacional, según la cual *"no cabe apreciar culpabilidad alguna (ni siquiera a título de culpa o falta de diligencia) en la actuación de la entidad recurrente, que actuó en la creencia de que la persona con la que contrataba era quien decía ser y se identificaba como tal con una documentación en apariencia auténtica y a ella correspondiente"*.

  Apunta la AEPD que *"resulta acreditado en el expediente que no se ha garantizado una seguridad adecuada en el tratamiento de los datos personales, habida cuenta del resultado que ha producido la suplantación de identidad"*. Entiende XFERA que se acerca esta afirmación a la figura de la responsabilidad objetiva, contraviniendo el principio de culpabilidad; y es que la existencia de dolo o negligencia no depende del resultado, sino de las circunstancias subjetivas que dan lugar a la supuesta infracción.

  En cuanto a la afirmación de que *"un tercero ha conseguido acceder a los datos personales de los titulares de las líneas"*, XFERA considera que no es "responsable" ni "encargada" de ninguno de los tratamientos a los que logra acceder el delincuente de forma indebida a través de los SMS recibidos: 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 LOPD. Los responsables de dichos tratamientos y, por ende, los sujetos obligados a garantizar su seguridad, son, exclusivamente, las entidades financieras.

- Grado de responsabilidad: la Agencia estima que es "alto", pero, a juicio de XFERA, no justifica por qué, a pesar de que el artículo 83.2.d) RGPD establece que debe ser puesto con relación a *"las medidas técnicas u organizativas que se hayan aplicado en virtud de los artículos 25 y 32"* de la misma norma. XFERA alega que se ha acreditado que existían unos procedimientos de seguridad razonables, en relación con el riesgo previsible para la empresa en el momento de los hechos; y que con posterioridad, los procedimientos de seguridad se han

reforzado de forma extraordinaria, con resultados sobresalientes.

- Categorías de datos personales afectados: XFERA se sorprende de que la Agencia considere que una tarjeta SIM es una categoría de datos personales cuyo acceso no autorizado es "particularmente grave". Y que lo justifica diciendo que *"no se trata del dato personal que se requiere para la expedición del duplicado de la tarjeta, sino de la tarjeta misma como dato personal"*. Sin embargo, considera XFERA que las tarjetas SIM no son datos de carácter personal: son meros soportes, y cuando se activa un duplicado, está vacíos de contenido. Y que no hay categoría alguna de datos personales afectados por esta operativa, en lo que a los operadores de telefonía móvil se refiere, por lo que no procede aplicar esta circunstancia agravante.

SEXTO. Sobre la desproporción del importe de la sanción propuesta.

XFERA alega que, en caso de no apreciarse una total falta de culpabilidad, en cualquier caso debería apreciarse una cualificada disminución de la culpabilidad de XFERA o, cuando menos, de la antijuridicidad de los hechos de los que trae causa el presente procedimiento, lo que determinaría la procedencia de reducir la gravedad de las infracciones a ella atribuidas y, por ende, a reducir la sanción a imponer.

En efecto, atendidos los argumentos anteriores de culpabilidad, aunque no fueran estimados, XFERA entiende que no podría obviarse que, por las circunstancias concurrentes, la conducta desplegada tiene menor gravedad que la considerada por el Acuerdo. Habida cuenta, además, de que la práctica totalidad de las circunstancias agravantes en él incluidas no resultan de aplicación al caso, XFERA concluye que sólo cabe reducir las sanciones que eventualmente se impongan. Máxime, cuando el esfuerzo realizado por XFERA para adecuar sus procedimientos de seguridad a la nueva realidad derivada del "SIM swapping" es más que notable, y sus resultados, excepcionales.

A pesar de que la cuantía de la sanción se ha reducido notablemente con respecto a la prevista en el Acuerdo de Inicio, XFERA considera sorprendente su importe, teniendo en cuenta que únicamente se han producido 37 casos de SIM swapping; y ello porque en un caso infinitamente más grave, a su parecer, cual es el recogido en el expediente PS/00179/2020, donde un "hacker comprometió una serie de sistemas" de la empresa, habiéndose confirmado "que el atacante había recopilado 488.847 tarjetas de crédito únicas" y había accedido a "1.500.000 registros", la multa impuesta fue de 500.000€. Y ello, a pesar de que la empresa sancionada facturaba casi el doble que XFERA, y a que XFERA cooperó en gran medida con la autoridad de control y adoptó medidas positivas para paliar los perjuicios sufridos por los afectados, como reconoce la propia Agencia.

XFERA entiende que la desproporción entre uno y otro caso es evidente.

Por todo lo expuesto, XFERA solicita que:

a. Se resuelva la finalización del procedimiento, con archivo de las actuaciones, debido a que los Hechos Probados no constituyen, a su parecer, de modo manifiesto, infracción administrativa y a la ausencia de culpabilidad por parte de XFE-

RA; y

b. Subsidiariamente, y únicamente en caso de que se entienda que procede la imposición de una sanción:

i. Se imponga exclusivamente una sanción de apercibimiento; o

ii. Subsidiariamente, que se califique la conducta como infracción de lo establecido en el artículo 32 del RGPD, tipificada en el artículo 83.4.a) del citado Reglamento, imponiendo una sanción máxima de 100.000€.

Estas Alegaciones serán objeto de respuesta en los FD de la presente Resolución.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes

HECHOS PROBADOS

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 **B.B.B.** 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 ***C.C.C.*** *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 ***B.B.B.****, 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* ***D.D.D..***

--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, (****B.B.B.****), 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.3***, de fecha 25 de septiembre de 2019 las 19:24 hs, por importe de 2000'00 euros a favor de ***D.D.D.***

- Transferencia inmediata desde la cuenta ******CUENTA.3***, de fecha 25 de septiembre de 2019 las 19:32 hs, por importe de 800'00 euros a favor de

D.D.D.

- Transferencia inmediata desde la cuenta ******CUENTA.3***, de fecha 25 de septiembre de 2019 las 21:29 hs, por importe de 100'00 euros a favor de ***D.D.D.***

- Transferencia desde la cuenta *******CUENTA.4***, de fecha 25 de septiembre de 2019 las 19:07 hs, por importe de 1000'00 euros a favor de ***C.C.C.***

- Reintegro en cajero automático desde la cuenta *******CUENTA.4***, 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.3***, 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 ***RRRRR/RR,*** en la que la parte RECLAMANTE DOS manifestó lo siguiente:

"Que el denunciante manifiesta que ha observado en su número de cuenta ******CUENTA.1*** *de la entidad ING dos cargos que él no ha realizado ni autorizado.*

Que los movimientos han sido realizados con la tarjeta con número ******TARJETA.1*** *la cual está asociada a la cuenta arriba referida, siendo los movimientos los siguientes:*

El día 10/07/2019, disposición en cajero número ******CAJERO.1****, por un valor de 1700 euros.*

El día 10/07/2019, disposición en cajero número ******CAJERO.1****, 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 ***SSSSS/SS,*** de fecha 29 de julio de 2019, manifiesta:

"Que las presentes son ampliatorias del atestado número ***RRRRR/RR*** *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.2*** *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 ***E.E.E.***, con NIF ******NIF.2***, 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.1***, de fecha 10 de julio de 2019, por importe de 1700 euros.

- Reintegro en cajero automático desde la cuenta ******CUENTA.1***, 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 "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 seguri-

dad:

(…)

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 detallan 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.4***	MásMóvil	Telefónico
14/01/2020	***TELEFONO.5***	Yoigo	Tienda
15/01/2020	***TELEFONO.6***	MásMovil	Telefónico
20/01/2020	***TELEFONO.7***	MásMóvil	Telefónico
25/01/2020	***TELEFONO.8***	Yoigo	Telefónico
27/01/2020	***TELEFONO.9***	MásMóvil	Telefónico
27/01/2020	***TELEFONO.10***	Yoigo	Tienda
28/01/2020	***TELEFONO.11***	Yoigo	Tienda
04/02/2020	***TELEFONO.12***	Yoigo	Telefónico
25/02/2020	***TELEFONO.13***	Yoigo	Telefónico
27/02/2020	***TELEFONO.14***	Yoigo	Telefónico
29/02/2020	***TELEFONO.15***	Yoigo	Telefónico
03/03/2020	***TELEFONO.15***	Yoigo	Telefónico
05/03/2020	***TELEFONO.16***	Yoigo	Telefónico
05/03/2020	***TELEFONO.12***	Yoigo	Telefónico
11/03/2020	***TELEFONO.17***	Yoigo	Tienda
13/03/2020	***TELEFONO.18***	Yoigo	Telefónico
03/04/2020	***TELEFONO.19***	MásMóvil	Telefónico
04/04/2020	***TELEFONO.20***	MásMóvil	Telefónico
08/04/2020	***TELEFONO.21***	Yoigo	Tienda
12/04/2020	***TELEFONO.22***	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.21*** 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.5***, 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.5***".

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 locali-

zadas 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.4*** 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.7*** de fecha 20 de enero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona su (…). También el solicitante le indica el número ICC de la tarjeta SIM.

En el Documento 9, se aporta grabación correspondiente a la línea ******TELEFONO.10*** de fecha 27 de enero de 2020 para la activación de la tarjeta SIM nueva. En la que el solicitante proporciona su (…). 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.13*** 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.19*** 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.4***	MásMóvil	Telefónico	05/01/2020 22:12	05/01/2020 22:24
******TELEFONO.5***	Yoigo	Tienda	14/01/2020	15/01/2020

			20:18	21:43
TELEFONO.6	MásMovil	Telefónico	15/01/2020 12:43	15/01/2020 13:20
TELEFONO.7	MásMóvil	Telefónico	20/01/2020 21:01	20/01/2020 22:51
TELEFONO.8	Yoigo	Telefónico	25/01/2020 16:48	25/01/2020 17:50
TELEFONO.9	MásMóvil	Telefónico	27/01/2020 14:20	27/01/2020 17:50
TELEFONO.10	Yoigo	Tienda	27/01/2020 17:07	27/01/2020 17:28
TELEFONO.10	Yoigo	Tienda	27/01/2020 19:56	27/01/2020 21:50
TELEFONO.11	Yoigo	Tienda	28/01/2020 12:29	28/01/2020 12:59
TELEFONO.12	Yoigo	Telefónico	04/02/2020 16:08	04/02/2020 16:26
TELEFONO.13	Yoigo	Telefónico	25/02/2020 23:05	25/02/2020 23:12
TELEFONO.14	Yoigo	Telefónico	27/02/2020 18:31	27/02/2020 19:19
TELEFONO.15	Yoigo	Telefónico	29/02/2020 21:38	29/02/2020 21:51
TELEFONO.15	Yoigo	Telefónico	03/03/2020 7:37	03/03/2020 7:48
TELEFONO.16	Yoigo	Telefónico	05/03/2020 17:07	05/03/2020 22:23
TELEFONO.12	Yoigo	Telefónico	05/03/2020 21:07	05/03/2020 21:37
TELEFONO.17	Yoigo	Tienda	11/03/2020 13:59	11/03/2020 14:42
TELEFONO.18	Yoigo	Telefónico	13/03/2020 12:51	13/03/2020 13:24
TELEFONO.19	MásMóvil	Telefónico	03/04/2020 15:11	03/04/2020 15:22
TELEFONO.20	MásMóvil	Telefónico	04/04/2020 13:45	04/04/2020 14:04
TELEFONO.21	Yoigo	Tienda	08/04/2020 21:03	08/04/2020 22:04
TELEFONO.22	Yoigo	Telefónico	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.4, ***TELEFONO.8, ***TELEFONO.10*** (en dos ocasiones), ***TELEFONO.11, ***TELEFONO.14, ***TELEFONO.18, ***TELEFONO.19, ***TELEFONO.21, ***TELEFONO.22***. 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.6, ***TELEFONO.10, ***TELEFONO.12*** (en dos ocasiones), ***TELEFONO.13, ***TELEFONO.15*** (en dos ocasiones), ***TELEFONO.17, ***TELEFONO.20***. 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.16***, 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.5, ***TELEFONO.7***.

De estos dos casos, es importante señalar que, en lo tocante al número de teléfono ******TELEFONO.5***, 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 portabilidad 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 (…)".

FUNDAMENTOS DE DERECHO

PRIMERO: **Competencia.**

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada Autoridad de Control, y según lo establecido en los artículos 47, 48, 64.2 y 68.1 de la LOPDGDD, la directora de la AEPD es competente para iniciar y resolver este procedimiento.

En la incoación del procedimiento sancionador la AEPD ha actuado conforme a los principios generales del artículo 3.1 de la LRJSP, entre los que se halla el servicio efectivo a los ciudadanos, la buena fe, la confianza legítima o la transparencia de la actuación administrativa.

La AEPD tiene atribuidas una serie de competencias, poderes y funciones previstas en los artículos 55 y siguientes del RGPD que según dispone el artículo 8 de la LRJSP, son irrenunciables y se ejercerán por los órganos administrativos que las tengan atribuidas como propias.

En el ejercicio de las funciones y poderes que le atribuyen los artículos 57 y 58 del RGPD, controla la aplicación del RGPD, realiza investigaciones e impone, en su caso, sanciones administrativas entre las que se pueden incluir las multas administrativas, y ordena las medidas correctoras correspondientes, según las circunstancias de cada caso particular. Así, puede realizar las investigaciones que considere oportunas (artículo 67 de la LOPDGDD), tras lo que puede decidir iniciar de oficio un procedimiento sancionador (artículo 68 LOPDGDD).

En el supuesto examinado, las investigaciones realizadas en aras de determinar la comisión de unos hechos y el alcance de estos pusieron de manifiesto la existencia de unas medidas de seguridad insuficientes, que ocasionaron un acceso indebido a datos personales, que ha afectado directamente al deber de mantener la confidencialidad de los datos de los clientes.

SEGUNDO: **Normativa aplicable**.

El artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la*

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

TERCERO**: Infracción**.

Las actuaciones reseñadas en los Antecedentes tuvieron como objeto analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM por parte de XFERA, identificando las vulnerabilidades que pudieran existir en los procedimientos operativos implantados, para detectar las causas por las cuales se podrían estar produciendo estos casos, así como encontrar puntos de incumplimiento, mejora o ajuste, para determinar responsabilidades, disminuir los riesgos y elevar la seguridad en el tratamiento de los datos personales de las personas afectadas.

Los hechos declarados anteriormente probados, vulneran el artículo 5.1.f) del RGPD y son constitutivos de la infracción prevista en el artículo 83.5.a) del RGPD que considera infracción muy grave la vulneración de:

> *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9*,"

Asimismo, consta tipificada con sanción de multa administrativa de 20.000.000,00 euros 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.

También son constitutivos de la infracción tipificada en el artículo 72.1.a) de la LOPDGDD que considera infracción muy grave a los efectos de la prescripción:

> *"El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".*

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. Pues bien, de la instrucción resultó, 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, que XFERA a pesar disponer de unas medidas de seguridad que se deberían adoptar en los tratamientos de datos personales necesarios para la prestación de los servicios contratados y a lo largo de su ciclo de vida, estas medidas han resultado a todas luces insuficientes para evitar el acceso indebido a duplicados de tarjeta SIM solicitados de forma fraudulenta.

El concepto de responsabilidad proactiva se encuentra ligado con el concepto de cumplimiento normativo o *compliance*, ya presente en otros ámbitos normativos (nos referimos, por ejemplo, a la previsión del artículo 31 bis del Código Penal).

Así, el artículo 24 del RGPD determina que:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es

conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos".

La responsabilidad proactiva implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina el cumplimiento generalizado de las obligaciones en materia de protección de datos. Comprende el análisis, planificación, establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización, especialmente si es una gran empresa, -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas, entre otros-, desde la privacidad desde el diseño y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que permitan al responsable demostrar su cumplimiento.

Pivota sobre la gestión del riesgo. Tal y como se establece en el Informe 0064/2020 del Gabinete Jurídico de la AEPD se muestra la metamorfosis de un sistema que ha pasado de ser reactivo a convertirse en proactivo, puesto que "en el momento actual, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «*accountability*» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la LOPDGDD: *"la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan".*

Requiere de una actitud consciente, comprometida, activa y diligente. La consciencia supone el conocimiento de su organización por parte del responsable del tratamiento y de cómo se ve afectada por la protección de datos y de los riesgos inherentes a los tratamientos de datos personales; el compromiso involucra la voluntad de cumplir y el hacerse verdaderamente responsable de la implantación de las políticas de protección de datos en la organización; la actitud activa está relacionada con la proactividad, la eficacia, la eficiencia y la operatividad; y la diligencia es el cuidado, el celo y la dedicación puesta en el cumplimiento.

Por otra parte, conforme al principio de responsabilidad proactiva que el RGPD consagra en su artículo 5.2, la AEPD no puede indicar a ningún responsable del tratamiento cuáles son las medidas de seguridad a implantar, pues sólo este último es conocedor en profundidad de su organización, de los tratamientos que lleva a cabo, de los riesgos asociados a los mismos y de las medidas de seguridad precisas a implementar para hacer efectivo el principio de integridad y confidencialidad.

Ahora bien, ha quedado probado que las medidas implantadas por XFERA son insuficientes y no sólo porque se haya producido su superación y la cesión de datos personales a un tercero.

De una manera no exhaustiva y a título de ejemplo nos fijaremos en la deficiente configuración de las preguntas formuladas en la política de seguridad para poder obtener el duplicado de la tarjeta SIM.

Así, de la documentación remitida por XFERA se comprueba que se realizan distintas comprobaciones para acreditar la identidad de quien realiza la solicitud o la activación del duplicado de la tarjeta SIM según la marca de que se trate.

En general, los datos personales asociados a la política de seguridad son los básicos de cualquier cliente: (…). En algunos supuestos (LLAMAYA) se añade la petición del (…), datos básicos también asociados a cualquier cliente. Basta con poseer datos básicos de un cliente para poder superar la política de seguridad, sin que ninguna pregunta adicional sea formulada respecto de algún dato que conozcan únicamente la operadora y su cliente. Ningún requisito suplementario es requerido.

Llama la atención que solo en alguna de las marcas se realizan comprobaciones adicionales más rigurosas, como pueden ser datos de uso que solo la persona que utiliza la línea en cuestión podría contestar correctamente. Así, respecto de la marca LEBARA se establece la superación de la política de seguridad en dos capas, figurando en segunda de ellas la formulación y respuesta correcta de dos o tres preguntas de uso para verificar datos muy concretos que podrían identificar fehacientemente al cliente. Esto muestra que XFERA sí tenía establecidas medidas de seguridad muy sencillas más apropiadas para identificar de manera fidedigna a un cliente y que no implementó en todas sus marcas.

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. Por todo lo expuesto, centramos los hechos en la infracción derivada del artículo 5.1.f) del RGPD.

Así las cosas, el fraude conocido como “SIM Swapping” es una técnica delincuencial consistente en obtener un duplicado de la tarjeta SIM asociada a una línea de telefonía titularidad de un usuario, con la finalidad de suplantar su identidad para obtener acceso a sus redes sociales, aplicaciones de mensajería instantánea, aplicaciones bancarias o comercio electrónico, con la finalidad de interactuar y realizar operaciones en su nombre, autenticándose mediante un usuario y contraseña previamente arrebatados a ese usuario, así como con la autentificación de doble factor al recibir el SMS de confirmación en su propio terminal móvil donde tendrán insertada la tarjeta SIM duplicada.

Hay que destacar que en la primera fase de este tipo de estafas el suplantador consigue, de manera fraudulenta, los datos de acceso o las credenciales de la banca online del cliente, pero le falta poder conocer el código de verificación, segundo factor de autentificación, para poder ejecutar cualquier operación. En el momento en el que logra la tarjeta SIM duplicada ya tiene también acceso a este segundo factor de autenticación y, por tanto, desde ese instante puede realizar los actos de disposición patrimonial que desee.

Retomando el análisis de la política de seguridad utilizada por XFERA para la comprobación de la identidad de quien solicita o activa el duplicado de la tarjeta SIM, y a

modo de ejemplo, es de suponer que unos delincuentes que ya han obtenido una serie de datos como los datos de acceso o las credenciales de la banca online de una persona y el número de línea de teléfono asociada a dicha cuenta, seguramente ya cuentan con la información básica de esa persona, como puede ser su nombre y apellidos y número de identificación personal. Esta Agencia no puede considerar suficiente esa mera comprobación que resulta a todas luces inútil para los fines para los que está prevista.

En resumen, es responsabilidad de la operadora establecer unos requisitos adecuados efectivos y eficaces que, si bien de una lectura rápida pueden parecer muy estrictos, de una lectura mucho más cuidadosa se ha evidenciado que no lo eran. Con lo cual, la estafa o suplantación, que aparentemente podría parecer compleja y difícil, se ve que no lo ha sido tanto por la falta de adecuación de las medidas de seguridad a la hora de vigilar que es el titular de la tarjeta SIM o persona por éste autorizada la que peticiona el duplicado, lo cual denota una falta de diligencia debida en la gestión del riesgo en cuestión.

CUARTO: **Tratamiento de datos personales y responsable del tratamiento.**

El artículo 4 del RGPD, bajo la rúbrica “Definiciones”, dispone lo siguiente:

*“1) «**datos personales**»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;*

*2) «**tratamiento**»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.*

*7) «**responsable del tratamiento**» o «**responsable**»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.*

*8) «**encargado del tratamiento**» o «**encargado**»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;*

XFERA es la responsable de los tratamientos de datos referidos en los antecedentes expuestos, toda vez que conforme a la definición del artículo 4.7 del RGPD es la que determina la finalidad y medios de los tratamientos realizados con las finalidades señaladas en su Política de Privacidad, conforme se ha acreditado en los Hechos Proba-

dos, apartado Primero.

Asimismo, la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular ya que *se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador* (artículo 4.1) del RGPD).

En este sentido, conviene aclarar que, dentro del terminal móvil, va insertada la tarjeta SIM. Es una tarjeta inteligente, en formato físico y de reducidas dimensiones, que contiene un chip en el que se almacena la clave de servicio del suscriptor o abonado usada para identificarse ante la red, esto es, el número de línea telefónica móvil del cliente MSISDN (Mobile Station Integrated Services Digital Network -Estación Móvil de la Red Digital de Servicios Integrados-), así como el número de identificación personal del abonado IMSI (International Mobile Subscriber Identity -Identidad Internacional del Abonado móvil-) pero también puede proporcionar otro tipo de datos como la información sobre el listado telefónico o el de llamadas y mensajes.

La tarjeta SIM es posible introducirla en más de un terminal móvil, siempre que éste se halle liberado o sea de la misma compañía.

En España, desde el año 2007, mediante la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (en adelante, Ley 25/2007), se exige que los titulares de todas las tarjetas SIM, ya sean de prepago o de contrato, estén debidamente identificados y registrados. Esto es importante por cuanto la identificación del abonado será imprescindible para dar de alta la tarjeta SIM, lo que conllevará que a la hora de obtener un duplicado de esta la persona que lo solicite haya de identificarse igualmente y que su identidad coincida con la del titular.

En suma, tanto los datos personales (nombre, apellidos y DNI) que se tratan para emitir un duplicado de tarjeta SIM como la propia tarjeta SIM (Subscriber Identity Module) que identifica de forma inequívoca y unívoca al abonado en la red, son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos.

QUINTO: **Alegaciones aducidas a la Propuesta de resolución.**

Se procede a dar respuesta a las mismas según el orden expuesto por XFERA:

PRIMERA. Disconformidad con la calificación de la supuesta infracción.

El artículo 5 "*Principios relativos al tratamiento*" dispone: "*1. Los datos personales serán: (…) f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".*

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.

Por su parte, hay que destacar, que la Memoria 2021 de la Fiscalía General del Estado dedicado a la "Criminalidad informática" 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 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 beneficio, 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."*

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.

Asimismo, cita en su descargo el PS/00362/2021 y el PS/00179/2020, teniendo que señalar que es perfectamente admisible que la AEPD haya considerado 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.

En relación con el PS/00362/2021 reseñar que XFERA recoge como si fueran Hechos Probados lo contenido en la reclamación presentada en el procedimiento sancionador al que ahora nos referimos, esto es, "*Los motivos en que basa la reclamación son que el reclamado facilita el detalle de los últimos movimientos de la tarjeta Affinity Card mediante un sistema de atención telefónica automatizado en el teléfono* ******** *en el que únicamente se pide como dato identificativo el DNI del cliente. Se manifiesta por el reclamante que la entidad reclamada no adopta ninguna otra medida de seguridad para confirmar la identidad del cliente por lo que cualquier persona puede llamar, dar un número de DNI y obtener información asociada a ese DNI, sin comprobar que la*

persona que llama sea el titular de dicho documento identificativo". Lo cierto es que la reclamación se formula porque un cliente detecta medidas de seguridad insuficientes razón por la que se les sanciona, sin que el cliente denuncie la cesión de sus datos a un tercero (el tiempo verbal en que se recoge el contenido de la reclamación puede dar a entender lo contrario, pero no se concluyó tal posibilidad de las actuaciones previas de investigación), ni que se acreditase en ningún momento en el procedimiento sancionador que se había procedido a la cesión de datos a terceros.

En cuanto al PS/00179/2020 deviene de la notificación de una brecha de seguridad, generada por la intervención de un hacker que roba directamente datos personales de clientes de la base de datos de la mercantil que sufre la brecha de seguridad, lo que no constituye en sí mismo una cesión de datos por parte del responsable del tratamiento a un tercero. Realizadas las investigaciones oportunas y verificado lo acontecido, se les sancionó por falta de medidas de seguridad.

Del examen de los hechos concurrentes en el presente supuesto y de las actuaciones de investigación efectuadas, así como de la instrucción del procedimiento sancionador se ha considerado para este supuesto ahora examinado que se ha producido una vulneración del artículo 5.1.f) del RGPD, considerando que las actuaciones de la Agencia tuvieron por objeto analizar los procedimientos aplicados a las solicitudes de cambio de tarjeta SIM. La tarjeta SIM constituye el soporte físico a través del cual se accede a los datos de carácter personal de la persona afectada. Si no se garantiza su disposición y control, el acceso a los datos personales del titular, así como el uso o usos posibles por terceros, se convierte en una amenaza que puede tener efectos devastadores en la vida de estas personas.

Hay que recordar que el derecho a la protección de datos deriva de la CE, que establece la limitación del uso de la informática por la Ley para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (artículo 18.4).

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

El enfoque de riesgos y el modelo flexible al riesgo impuesto por el RGPD -partiendo de la doble configuración de la seguridad como un principio relativo al tratamiento y una obligación para el responsable o el encargado del tratamiento- no impone en ningún caso la infalibilidad de las medidas, sino su adecuación constante a un riesgo,

que, como en el supuesto examinado es cierto, probable y no desdeñable, alto y con un impacto muy significativo en los derechos y libertades de los ciudadanos.

En la instrucción del procedimiento se ha constatado que no se había garantizado una seguridad adecuada en el tratamiento de los datos personales, habida cuenta del resultado que produjo la suplantación de identidad. Es decir, un tercero consiguió acceder a los datos personales de los titulares de las líneas sin que las medidas de seguridad de XFERA, pudieran evitarlo.

Por consiguiente, no ha quedado demostrado por parte de XFERA el cumplimiento de los principios relativos al tratamiento de los datos personales afectados.

SEGUNDA. XFERA no ha quebrantado el principio de confidencialidad del dato.

La tarjeta SIM identifica un número de teléfono y este número a su vez, identifica a su titular. En este sentido la Sentencia del TJUE en el asunto C -101/2001(Lindqvist) de 6.11.2003, apartado 24, Rec. 2003 p. I-12971: *"El concepto de "datos personales" que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva "toda información sobre una persona física identificada o identificable". Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones"».*

También, esta opinión se singulariza en relación con los dispositivos de telefonía móvil que permiten la localización del interesado, en el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes (documento WP185):

"Dispositivos móviles inteligentes. Los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas. Normalmente existe una identificabilidad directa e indirecta. En primer lugar, los operadores de telecomunicaciones que proporcionan acceso a Internet móvil y a través de la red GSM poseen normalmente un registro con el nombre, la dirección y los datos bancarios de cada cliente, junto con varios números únicos del dispositivo, como el IMEI y el IMSI. (…)"

Igualmente, la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 19 de octubre de 2016 Asunto C-582/14, considera que incluso la dirección IP dinámica ha de considerarse dato de carácter personal en la medida en que el proveedor de servicios tiene medios puede conocer la identidad del titular de esa dirección IP de carácter dinámico.

O la más reciente STJUE de 17 de junio de 2021 Asunto C-579/19 que en su apartado 102 recuerda que *"(…) Un dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal en el sentido del artículo 4, punto 1, del Reglamento 2016/679, cuando este disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional con que cuenta el proveedor de acceso a Internet de esa persona (…).*

Quiere decir esto que mientras exista la posibilidad de realizar la identificación estaremos ante un dato de carácter personal.

Es importante esta consideración en relación con el caso concreto, pues recuérdese que la dirección IP dinámica es aquella que cambia cada cierto tiempo, por ejemplo por cambios en la red, o por la reiniciación del dispositivo con el que el proveedor de servicios proporciona la conexión, en contraposición a la dirección IP estática que siempre es la misma.

Si el TJUE considera dato personal dicha dirección IP dinámica, "que cambia cada cierto tiempo" es lógico considerar que el IMSI y el IMEI (International Mobile Estation Equipment Identity), que tienen un carácter permanente y del que se deriva por tanto, una mejor individualización del usuario y también su identificación, puedan también tener dicha consideración.

Por lo tanto, se deduce que tanto el IMEI, como el IMSI en la medida que permiten singularizar a un individuo, y por tanto identificarle, han de ser considerados datos de carácter personal de acuerdo con el artículo 4.1 del RGPD que considera como tal: *Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

Asimismo, la Sentencia de la Audiencia Provincial de Barcelona núm. 390/2019 de 30 de mayo, 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."*

TERCERA. Vulneración de los principios de personalidad de la sanción y de tipicidad.

Las operaciones de tratamiento que son objeto de este expediente están relacionadas con el ejercicio de los derechos que como usuarios finales de los servicios de comunicaciones electrónicas están realizando los clientes del operador. En este sentido, la normativa de este sector confiere una naturaleza pública tanto a la propia prestación del servicio ("servicios de interés general") como al régimen específico de protección de los usuarios ("obligaciones de carácter público").

Dentro de los derechos específicos de este sector, la regulación reglamentaria se encuentra en la Carta de Derechos del usuario de servicios de comunicaciones electrónicas (Real Decreto 899/2009, de 22 de mayo). En su artículo 5 (Celebración de contratos) se especifica lo siguiente:

"2. Los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco".

Conviene recordar que los hechos enjuiciados en el presente expediente han consistido precisamente en eso, es decir, en la expedición inadecuada de tarjetas SIM que

han permitido a terceros ajenos a la línea acceder a ella. Queda afectado, por lo tanto, el derecho del usuario final que tiene la consideración de obligación de carácter público.

Pero no solo eso, sino que en la captación de clientes, y de modo particular en la expedición de tarjetas SIM, es preciso cumplir lo establecido en la Ley 25/2007. Esta Ley está dictada en uso de la competencia estatal en materia de Seguridad pública, y tiene como fin garantizar que los operadores conservan y ponen a disposición de las Fuerzas y Cuerpos de Seguridad, los datos relativos a los titulares de servicios de comunicaciones electrónicas y sus datos de tráfico. El artículo 2 establece lo siguiente:

"Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones."

El artículo 3 y, de modo específico para líneas prepago, la disposición adicional única, establece que deberán ser identificados todos los usuarios finales titulares de servicios de comunicaciones electrónicas.

Como ha quedado acreditado en este expediente, los puntos de venta y centros de atención de llamadas telefónicas eran utilizados para la expedición de duplicados de tarjetas SIM. A estos efectos sería de aplicación, en la identificación de los clientes, la mencionada Ley 25/2007.

Por lo tanto, se encuentran involucrados en la gestión de clientes por parte de los operadores de telecomunicaciones, aspectos directamente relacionados con los servicios de interés general, las obligaciones de carácter público y, sobre todo, la Seguridad pública del Estado.

No obstante, estos aspectos no pueden ser atendidos por parte de los operadores de cualquier forma, conculcando la normativa de protección de datos en lo que sea aplicable. Si bien se les reconoce un carácter específico, no es menos cierto que de ninguna manera pueden considerarse una dispensa para la protección de un derecho fundamental como es el derecho a la protección de los datos personales de los individuos. Y es obligación de los operadores de telecomunicaciones, como XFERA, prestar el citado servicio implementando unas medidas de seguridad apropiadas, que garanticen el cumplimiento del principio de confidencialidad de los datos personales de los que el operador en cuestión es responsable.

Por su parte, respecto de la responsabilidad de las entidades financieras, la Directiva PSD2, se aplica a los servicios de pago prestados dentro de la Unión (artículo 2), y no a XFERA, pero también es cierto que la expedición de un duplicado de tarjeta SIM a favor de un tercero que no es el titular de la línea, proporciona a los suplantadores el control de la línea telefónica, y por lo tanto, de los SMS dirigidos al teléfono vinculado a la tarjeta SIM inicial y de esta manera a poder acceder a conocer el código de autentificación de la transacción.

Conforme al artículo 4.30 de la Directiva, la "autenticación reforzada" se basa en la utilización de dos o más elementos categorizados como conocimiento (algo que solo co-

noce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario). Estos elementos o factores son independientes entre sí y, por tanto, la vulneración de uno no compromete la fiabilidad de los demás.

El fundamento es muy sencillo: cuantos más elementos se tengan para verificar la identidad del usuario, más segura es la transacción.

Recordemos que, en estos casos, el suplantador en primer lugar deberá, introducir el usuario y contraseña o password en la aplicación o en el sitio web del proveedor de servicio de pagos o de banca online. En segundo lugar, para completar la transacción o gestión electrónica que desee realizar, el suplantador recibirá, normalmente a través de un SMS, un código alfanumérico de verificación en el teléfono móvil vinculado a ese perfil. Dicho código tiene una validez temporal limitada y es de un solo uso, es decir, únicamente se genera para esa transacción concreta y durante un tiempo limitado. Una vez introducido el código de verificación, se realizaría y completaría la transacción. Se presupone que solo el usuario tiene el dispositivo móvil en su poder (sería el "algo que tiene"), por lo que al recibir en dicho teléfono móvil el código de verificación a través del SMS, su identidad quedaría doblemente autenticada. Por tanto, a los suplantadores no les bastaría para poder cometer el fraude con conocer el usuario y contraseña con los que se identifique la víctima, sino que será necesario que intercepten dicho código de confirmación. En consecuencia, para poder efectuar una transferencia, transacción o compra no consentida, es decir, para llevar a cabo la estafa informática, el ciberdelincuente deberá acceder ilegítimamente a los códigos de verificación asociados a cada una de esas operaciones remitidos por la entidad bancaria a través de SMS y la manera más habitual de hacerlo es a través de la obtención de un duplicado de la tarjeta SIM.

Por lo tanto, es necesario ejecutar dos acciones completamente diferentes pero complementarias entre sí.

En primer lugar se han de obtener los datos de acceso a la banca online o proveedor de pago titularidad de la persona a defraudar, si nos centramos en la búsqueda del enriquecimiento patrimonial.

Y en segundo lugar, se habrá de obtener el duplicado de la tarjeta SIM titularidad de la persona a defraudar con la finalidad de hacerse con los SMS de confirmación que el cliente recibirá en su terminal móvil como autentificación de doble factor.

Pues bien, en la última de estas acciones -obtención del duplicado-, es donde se han centrado los hechos objeto de este procedimiento y no en los acontecidos en la primera fase, que quedan al margen de la responsabilidad que se imputa a XFERA.

En cuanto a la responsabilidad de los delincuentes que realizan estos fraudes, indudablemente, queda fuera de la responsabilidad que se imputa a XFERA en el presente procedimiento sancionador.

Respecto a que la tarjeta SIM proporcionada cuando se facilita un duplicado de esta está vacía y no se accede a datos personales tratados por XFERA, nos remitimos al apartado 2 del presente FD.

En relación a que XFERA es la mera intermediaria de los mensajes que se envían y se reciben a través de estos duplicados de tarjeta SIM obtenidos de forma fraudulenta, de acuerdo con lo previsto en el artículo 14.1 de la LSSI y que en todo caso se estaría ante una vulneración del secreto de las comunicaciones, el cual no es competencia de la AEPD, reiteramos que no es objeto del presente procedimiento sancionador lo que ocurre en la fase anterior a obtener el duplicado de la tarjeta SIM (la obtención de los datos necesarios para realizar el fraude) ni lo que ocurre en la fase posterior a obtener el mencionado duplicado de la tarjeta SIM (el enriquecimiento ilícito mediante el acceso a la cuenta bancaria del afectado y la utilización de los códigos que se envíen a través de dicha tarjeta SIM). El objeto del presente procedimiento sancionador y sobre lo cual se le atribuye responsabilidad a XFERA es únicamente por facilitar a una persona distinta del titular el acceso a un duplicado de su tarjeta SIM por no haber implantado medidas de seguridad apropiadas para impedir ese fraude.

CUARTA. Vulneración del principio de culpabilidad.

4.1. XFERA no había identificado el riesgo, simplemente, porque no existía antes de PSD2.

La vulneración de la infracción administrativa imputada responde a un precepto incluido dentro de “Principios relativos al tratamiento” que exige se asegure la confidencialidad de los datos personales mediante una seguridad adecuada en el tratamiento de los datos personales, seguridad que no se ha garantizado de acuerdo con los Hechos Probados.

En el presente procedimiento, no se está analizando el riesgo existente antes de la aplicación de la llamada PSD2 sino el que se produce a partir de su aplicación, que es cuando se empieza a realizar el tipo de fraude detallado en los apartados anteriores mediante la utilización de un duplicado de tarjeta SIM obtenido indebidamente por persona distinta a su titular.

Así, la infracción devino no por la carencia de unas medidas de seguridad para la expedición de los duplicados SIM, sino por la necesidad de su revisión y refuerzo.

No basta con disponer de unas medidas de seguridad, sino que hay que adecuarlas para mitigar los riesgos. El continuo avance de la tecnología y la evolución de los tratamientos propician la aparición continua de nuevos riesgos que deben ser gestionados. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los “riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas” (artículo 24.1) aplicando las medidas oportunas.

En el presente caso, las medidas de seguridad implementadas no resultan suficientes para garantizar la confidencialidad del dato personal en cuestión, tal y como ha sido explicado en detalle en el apartado 1 del presente FD.

4.2. XFERA actuó en la creencia de que la persona que solicitaba el duplicado era quien decía ser.

No se discute la condición de víctima de XFERA, sino el acceso no autorizado a un duplicado de tarjeta SIM, que se considera particularmente grave ya que posibilita la suplantación de identidad con una finalidad, la de interactuar y realizar operaciones en nombre de un tercero.

XFERA no puede negar el hecho de que trata datos de carácter personal a gran escala. Es la propia operadora la que reconoce tener más de 4 millones de clientes postpago y más de un millón y medio de clientes prepago.

Efectivamente, en materia sancionadora rige el principio de culpabilidad (STC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa. Como dice la STS de 23 de enero de 1998 , *"...puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril , al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho"*.

La falta de diligencia a la hora de implementar en origen las medidas de seguridad adecuadas para comprobar que la persona que solicita o activa el duplicado de una tarjeta SIM es el titular de esta es, precisamente, lo que constituye el elemento de la culpabilidad.

En cuanto a que XFERA fue víctima de fraude, cabe señalar, además, que XFERA debe estar en disposición de establecer mecanismos que impidan que se produzca la duplicación fraudulenta de las tarjetas SIM, medidas que respeten la integridad y 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 (considerandos 76, 77, 78, 79, 81 y 83 RGPD; artículo 32 del RGPD y artículo 28 de la LOPDGDD)

Las pruebas periódicas, la medición y la evaluación de la efectividad de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento son responsabilidad de cada responsable y encargado del tratamiento conforme al artículo 32.1.d) del RGPD.

Por lo tanto, XFERA como responsable del tratamiento está obligada a verificar tanto la selección como el nivel de efectividad de los medios técnicos utilizados. La exhaustividad de esta verificación debe evaluarse a través del prisma de adecuación a los riesgos y la proporcionalidad en relación con el estado del conocimiento técnico, los costos de implementación y la naturaleza, el alcance, el contexto y los propósitos del tratamiento.
Tal y como indicaba la instructora en la propuesta de resolución, en los casos descritos en el apartado de Hechos Probados, no se garantizó la seguridad de los datos de forma efectiva, y en particular, su correcta custodia para evitar la pérdida, sustracción o acceso no autorizado.

Ciertamente, el principio de responsabilidad previsto en el artículo 28 de la LRJSP, dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción admi-*

nistrativa 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."

No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo 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).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, Rec 1067/2006, que *"aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa".*

La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable del tratamiento, que es quien determina la existencia del tratamiento y su finalidad. Recordemos que, con carácter general las operadoras tratan los datos de sus clientes al amparo de lo previsto en el artículo 6.1 b) del RGPD, por considerarse un tratamiento necesario para la ejecución de un contrato en el que el interesado es parte (…). Por tanto, es responsabilidad de las operadoras (XFERA, en el presente caso) implementar las medidas apropiadas que garanticen el cumplimiento del principio de confidencialidad consagrado en el artículo 5.1.f) del RGPD, de modo que, si tal principio se ve comprometido debido a la falta de diligencia a la hora de implementar medidas suficientes para ello, se imputará la responsabilidad de tal infracción a la operadora en cuestión.

QUINTA. Circunstancias aplicables al caso individual, conforme al art. 83.2 RGPD.

Nos remitimos al FD Séptimo.

SEXTO. Sobre la desproporción del importe de la sanción propuesta.

En cuanto al incumplimiento del principio de proporcionalidad, el RGPD prevé expresamente la posibilidad de graduación, mediante la previsión de multas susceptibles de modulación, en atención a una serie de circunstancias de cada caso individual efectivas, proporcionadas y disuasorias (artículo 83.1 y 2 RGPD), condiciones generales para la imposición de las multas administrativas que sí han sido objeto de análisis por esta Agencia, a las que hay que sumar los criterios de graduación previstos en la LOPDGDD, objeto de desarrollo en el FD Séptimo.

Hay que señalar que la multa administrativa acordada será efectiva porque conducirá a la compañía a aplicar las medidas técnicas y organizativas que garanticen un grado de seguridad correspondiente al valor de criticidad del tratamiento.

También es proporcional a la vulneración identificada, en particular a su gravedad, el círculo de personas físicas afectadas y los riesgos en los que se han incurrido y a la situación financiera de la compañía.

Y por último, es disuasoria. Una multa disuasoria es aquella que tiene un efecto disuasorio genuino. 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)."*

La Sentencia de fecha 11 de mayo de 2006 dictada en el recurso de casación 7133/2003 establece que: "*Ha de tenerse en cuenta, además, que uno de los criterios rectores de la aplicación de dicho principio régimen sancionador administrativo (criterio*

recogido bajo la rúbrica de «principio de proporcionalidad» en el apartado 2 del artículo 131 de la citada Ley 30/1992) es que la imposición de sanciones pecuniarias no debe suponer que la comisión de las infracciones tipificadas resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas".

También es importante la jurisprudencia que resulta de la Sentencia de la Sala Tercera del Tribunal Supremo, dictada en fecha 27 de mayo de 2003 (rec. 3725/1999) que dice: *La proporcionalidad, perteneciente específicamente al ámbito de la sanción, constituye uno de los principios que rigen en el Derecho Administrativo sancionador, y representa un instrumento de control del ejercicio de la potestad sancionadora por la Administración dentro, incluso, de los márgenes que, en principio, señala la norma aplicable para tal ejercicio. Supone ciertamente un concepto difícilmente determinable a priori, pero que tiende a adecuar la sanción, al establecer su graduación concreta dentro de los indicados márgenes posibles, a la gravedad del hecho constitutivo de la infracción, tanto en su vertiente de la antijudicidad como de la culpabilidad, ponderando en su conjunto las circunstancias objetivas y subjetivas que integran el presupuesto de hecho sancionable -y, en particular, como resulta del artículo 131.3 LRJ y PAC, la intencionalidad o reiteración, la naturaleza de los perjuicios causados y la reincidencia-. (SSTS 19 de julio de 1996, 2 de febrero de 1998 y 20 de diciembre de 1999, entre otras muchas).*

En todo caso, frente a la alegación formulada por XFERA sobre la desproporción de la multa afirmando que "únicamente" se han producido 37 casos de SIM swapping, reiterar de nuevo que la AEPD, a raíz de 37 reclamaciones por fraude de identidad, que implicaban por parte del responsable del tratamiento la emisión del duplicado de la tarjeta SIM del cliente (tras lo cual se han producido gravosos daños económicos a los afectados) investiga en profundidad el origen del problema en aras de averiguar si o se debía a un fallo en el modelo de protección de la privacidad.

El foco no se sitúa en los terceros que han superado las políticas de seguridad, sino en el por qué las han superado; esto es, se examina la condición, características y adecuación de las políticas citadas a la normativa de protección de datos y la actuación del responsable del tratamiento al respecto.

SEXTO: **Principios relativos al tratamiento.**

Considerado el derecho a la protección de datos de carácter personal como el derecho de las personas físicas a disponer de sus propios datos, es necesario determinar los principios que lo configuran.

En este sentido, el artículo 5 RGPD, referido a los "Principios relativos al tratamiento" dispone:

"1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; (…);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; (…)

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

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de nuestros datos.

En este sentido, el considerando 75 del RGPD determina: *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a 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 o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*.

Asimismo, el considerando 83 del RGPD establece: "*A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la téc-*

nica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

Hemos de atender a las circunstancias singulares de las dos reclamaciones presentadas, a través de las cuales puede constatarse que, desde el momento en el que la persona suplantadora realiza la sustitución de la SIM, pasa el control de la línea a las personas suplantadoras. En consecuencia, los reclamantes ven afectados sus poderes de disposición y control sobre sus datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos según ha señalado el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre de 2000 (FJ 7). De manera que, al conseguir un duplicado de la tarjeta SIM, se posibilita bajo determinadas circunstancias, el acceso a los contactos o a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder modificar las contraseñas. En definitiva, podrán suplantar la identidad de los afectados, pudiendo acceder y controlar, por ejemplo: las cuentas de correo electrónico; cuentas bancarias; aplicaciones como WhatsApp; redes sociales, como Facebook o Twitter, y un largo etc. En resumidas cuentas, una vez modificada la clave de acceso por parte de los suplantadores pierden el control de sus cuentas, aplicaciones y servicios, lo que supone una gran amenaza.

De ahí que la seguridad y la confidencialidad de los datos personales se consideren esenciales para evitar que los interesados sufran efectos negativos.

En consonancia con estas previsiones, el considerando 39 RGPD dispone: "*Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento.*

Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que

los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. 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."

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

El considerando 7 del RGPD dispone: "*(…) Las personas físicas deben tener el control de sus propios datos personales. (…)"*

Los hechos declarados anteriormente probados, son constitutivos de una vulneración del artículo 5.1.f) del RGPD al facilitar XFERA duplicados de la tarjeta SIM a terceras personas que no son las legítimas titulares de las líneas móviles, tras la superación por las personas suplantadoras de las políticas de seguridad implantadas por la operadora, lo que evidencia un incumplimiento del deber de proteger la información de los clientes.

Este acceso no autorizado a los datos personales de los afectados resulta determinante para las actuaciones posteriores desarrolladas por las personas suplantadoras, ya que aprovechan el espacio de tiempo que trascurre hasta que el usuario detecta el fallo en la línea, se pone en contacto con la operadora, y ésta detecta el problema, para realizar operaciones bancarias fraudulentas -que se han reproducido en los dos casos denunciados- y que sin el duplicado de la tarjeta SIM hubiera devenido imposible su realización.

La emisión y entrega del duplicado a un tercero no autorizado supone para los afectados la pérdida del control de sus datos personales. 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 tienen el deber legal de garantizar su seguridad, tal como lo haría con cualquier otro activo.

Cabe traer a colación la sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional, que configura el derecho a la protección de datos como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o qué datos puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Así, de acuerdo con los Fundamentos jurídicos 4, 5, 6 y 7 de la sentencia del alto tribunal:

> **"4.** Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en

un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.

Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y finalidad del constituyente que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo, fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

5. (…) Pues bien, en estas decisiones el Tribunal ya ha declarado que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6, reiterado luego en las SSTC 143/1994, FJ 7, 11/1998, FJ 4, 94/1998, FJ 6, 202/1999, FJ 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comporta-

mientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.

De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado.

De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art.

18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7).

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele." (el subrayado de todos los párrafos es nuestro)

Por tanto, cualquier actuación que supone privar a la persona de aquellas facultades de disposición y control sobre sus datos personales, constituye un ataque y una vulneración de su derecho fundamental a la protección de datos.

SÉPTIMO: **Condiciones generales para la imposición de la multa administrativa.**

En el artículo 83.2 del RGPD se dispone que:

"Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso,

en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 "*Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado. (…)"

De acuerdo con los preceptos transcritos a efectos de fijar el importe de la sanción como responsable de la infracción tipificada en el artículo 83.5.a) del RGPD, procede graduar la multa que corresponde imponer, previa valoración de las alegaciones aducidas a los efectos de una correcta aplicación del principio de proporcionalidad.

Por una parte, se han tenido en cuenta los siguientes agravantes:

- Artículo 83.2.a) RGPD:

  · La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido:

XFERA aduce que la tarjeta SIM no tiene información personal. No obstante, este punto ya fue rebatido en el FD Quinto, apartado 2. También alega, que la pérdida de control de los datos de los interesados se produce en las entidades financieras y que XFERA es un mero tercero. Este punto fue rebatido en el FD Quinto, apartado 3.

En cuanto a la naturaleza de la infracción, la violación del principio del artículo 5.1.f) RGPD entraña un riesgo importante para los derechos de los afectados. La Agencia considera que la naturaleza de la infracción es muy grave puesto que acarrea una pérdida de disposición y control sobre los datos personales. Ha permitido a los criminales robar la identidad mediante el secuestro del número del número de teléfono tras obtener un duplicado de su tarjeta SIM. Tras la entrada en vigor de la Directiva PSD2, el teléfono móvil ha pasado a desempeñar un rol muy importante en la realización de pagos online al ser necesario para la confirmación de transacciones, y convierte a este dispositivo -y por extensión a la tarjeta SIM-, en objetivo claro de los ciberdelincuentes.

Con relación al periodo temporal respecto al que acontecen los hechos, si bien los hechos denunciados por las partes reclamantes acontecen en fechas determinadas, XFERA declaró que se produjeron ***CANTIDAD.6 casos en el ejercicio 2019 y ***CANTIDAD.5 casos en el ejercicio 2020.

En cuanto al número de interesados afectados: XFERA declaró que se produjeron ***CANTIDAD.6 casos en el ejercicio 2019 y ***CANTIDAD.5 casos en el ejercicio 2020. Por tanto, sería un total de ***CANTIDAD.9 afectados.

Con relación al nivel de los daños y perjuicios sufridos, XFERA aduce que los perjuicios producidos estarían ceñidos únicamente al coste de la solicitud de duplicado SIM, que ya fue devuelto a todo aquel que lo reclamó, además, de que, los perjuicios ocasionados por el fraude bancario no son de su responsabilidad. No obstante, esta Agencia ya ha determinado que la responsabilidad que se le imputa a XFERA es por haber facilitado un duplicado de tarjeta SIM solicitado de forma fraudulenta debido a la insuficiencia de las medidas implantadas por XFERA para evitarlo.

La Agencia considera que el nivel de los perjuicios causados es alto, ya que el acceso a los duplicados de dichas tarjetas SIM ha derivado en operaciones bancarias fraudulentas sucedidas en un corto espacio de tiempo. Mediante la duplicación de las tarjetas SIM, los supuestos suplantadores han conseguido el control de la línea del abonado y en concreto la recepción de SMS dirigidos al legítimo abonado para realizar operaciones on-line con entidades bancarias suplantando su personalidad. Estos SMS los envían las entidades bancarias como parte de la verificación en dos pasos de operaciones como transferencias monetarias o pagos por Internet, y el acceso a estos SMS suele ser el motivo

de la duplicación fraudulenta de las tarjetas SIM.

Es cierto que XFERA no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias ni se le puede atribuir la responsabilidad por fraude bancario. No obstante, también es cierto, que si XFERA asegurase el procedimiento de identificación y entrega, ni siquiera podría activarse el sistema de verificación de las entidades bancarias. La persona estafadora tras conseguir la activación de la nueva SIM, toma el control de la línea telefónica, pudiendo así, a continuación, realizar operaciones bancarias fraudulentas accediendo a los SMS que las entidades bancarias envían a sus clientes. Esta secuencia de hechos puesta de manifiesto en las reclamaciones interpuestas genera una serie de daños y perjuicios graves que deberían haberse tenido en cuenta en una evaluación de impacto relativa a la protección de datos (considerando 89, 90, 91 y artículo 35 del RGPD). En definitiva, desde el momento que se entrega un duplicado a una persona distinta a la titular de la línea o persona autorizada, el cliente pierde el control de la línea y los riesgos, daños y perjuicios, se multiplican. Además, los hechos acontecen con una inmediatez abrumadora.

En suma, la aplicación del agravante del artículo 83.2.a) del RGPD se refiere a la gravedad de los Hechos Probados, que se pone de manifiesto, entre otras cuestiones, en la alarma social generada por la realización de estas prácticas fraudulentas y por la altísima probabilidad de materialización del riesgo, sin que sea determinante el número de reclamaciones presentadas. Y ello, porque lo que se ha analizado en el presente procedimiento sancionador son las medidas de seguridad implantadas por el responsable del tratamiento (XFERA) a raíz de diversas reclamaciones presentadas ante la AEPD.

- Artículo 83.2.b) RGPD:

  · Intencionalidad o negligencia en la infracción:

  XFERA alega que no ha sido negligente, sino que fue engañada por delincuentes. Que, además, la negligencia no depende del resultado (es decir, de si se facilitó o no los duplicados de tarjeta SIM a personas que lo solicitaron de forma fraudulenta). Y que XFERA es un tercero, dado que no trata los datos a los que se accede mediante la obtención fraudulenta de ese duplicado de tarjeta SIM.

  En cuanto a que XFERA no fue negligente, sino que fue engañada por delincuentes, se reitera lo explicado en el FD Quinto, apartado 4. Si XFERA hubiera sido diligente a la hora de implementar medidas adecuadas para identificar correctamente a la personas que solicitan y activan las tarjetas SIM, no se producirían accesos indebidos a las mismas.

  Respecto a que la negligencia no depende del resultado, esta Agencia considera que se ha producido una vulneración del principio de confidencialidad como consecuencia de una negligencia a la hora de imple-

mentar las medidas adecuadas a que hace referencia el artículo 5.1.f) del RGPD para garantizar esa confidencialidad, tal como se ha desarrollado en el FD Tercero y Quinto, apartado 4.

Sobre que XFERA es un tercero, dado que no trata los datos a los que se accede mediante la obtención fraudulenta de un duplicado de tarjeta SIM, se reitera lo desarrollado en el FD Quinto, apartado 3, en el sentido de que este procedimiento sancionador se centra únicamente en la fase posterior a la obtención de los datos necesarios para la solicitud de la tarjeta SIM. Tampoco valora la responsabilidad de XFERA sobre el momento posterior a la obtención de ese duplicado de tarjeta SIM, en el que se realiza el enriquecimiento ilícito. Solamente se analiza la actitud negligente de XFERA en lo que atañe a la facilitación de un duplicado de tarjeta SIM a persona distinta de su titular sin comprobar correctamente si quien lo solicita es efectivamente quien dice ser.

En cuanto a la antijuricidad de la conducta de XFERA, se considera que responde al tipo infractor y al título de culpa. Se considera que XFERA ha actuado con negligencia. Como depositaria de datos de carácter personal a gran escala, por lo tanto, habituada o dedicada específicamente a la gestión de los datos de carácter personal de los clientes, debe ser especialmente diligente y cuidadosa en su tratamiento. Es decir, desde la óptica de la culpabilidad, estamos ante un error vencible, ya que con la aplicación de las medidas técnicas y organizativas adecuadas, estas suplantaciones de identidad se hubieran podido evitar.

Si bien la Agencia considera que no hubo intencionalidad por parte de XFERA, concluye que fue negligente al no asegurar un procedimiento que garantizase la protección de los datos personales de los clientes. De manera que, se produce un resultado socialmente dañoso que impone la desaprobación de la política de seguridad implantada que resultaba ineficaz, independientemente del nivel de compromiso demostrado, que resulta incuestionable.

Negar la concurrencia de una actuación negligente por parte de XFERA equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no compartimos esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida. Una gran empresa que realiza tratamientos de datos personales de sus clientes a gran escala, de manera sistemática y continua, debe extremar el cuidado en el cumplimiento de sus obligaciones en materia de protección de datos, tal y como establece la jurisprudencia. 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 re-*

currente 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".

Se establece como fundamental el análisis de riesgos del tratamiento de datos atendiendo a las circunstancias concretas de la operadora, tales como volumen y tipología de datos. Es de vital importancia establecer e implantar los procedimientos y medidas necesarios, en función de las características y entidad de esta, que permitan demostrar que se ha tenido una debida diligencia a la hora de intentar evitar que se produjese una suplantación de identidad. Así, aunque el perjuicio haya sido realizado por un tercero ajeno a la empresa, se ha de poder demostrar que se han adoptado las necesarias precauciones durante el desarrollo de la actividad empresarial, exigidas por la normativa, para evitar un daño que fuera previsible. Se trata de tener un nivel de cuidado objetivo atendiendo a las concretas circunstancias del caso que posibilite hacer patente que se estaba al tanto de la posibilidad de sufrir una suplantación de identidad, y que, con ello, se aplicaron las medidas oportunas para reducir la concreción de tal riesgo al mínimo posible.

- Artículo 83.2.d) RGPD:

  · Grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32:

  XFERA alega que no se justifica por qué se valoró como “Alto” su grado de responsabilidad, toda vez que había adoptado medidas adecuadas según el riesgo que era previsible.

  Al respecto, esta Agencia considera que la responsabilidad de las vulnerabilidades en el procedimiento para la expedición del duplicado de tarjeta SIM corresponde a XFERA, que es la persona jurídica a quien le corresponde implantar las medidas adecuadas para evitar que se produzcan situaciones como las aquí analizadas.

  Dado que se ha concluido que XFERA carecía de estas medidas adecuadas, se considera que es responsable de no haber hecho todo lo que podía esperarse que hiciera, máxime cuando dispone de medios de toda índole más que suficientes para cumplir adecuadamente, habida cuenta de la naturaleza, los fines o el ámbito de la operación de tratamiento, a la luz de las obligaciones que le impone el RGPD.

- Artículo 83.2.g) RGPD:

  · Categorías de datos personales afectados por la infracción:

  Alega XFERA que la tarjeta SIM no es un dato personal y que, por tanto, no hay ninguna categoría de datos afectados. No obstante, esta observación ya fue analizada en el FD Quinto, apartado 2. En conclusión,

esta Agencia considera que la tarjeta SIM sí que es un dato personal y que, como tal, tiene una naturaleza especialmente sensible, ya que posibilita la suplantación de identidad.

La entrega de un duplicado de SIM a favor de un tercero distinto del legítimo titular se considera particularmente grave ya que imposibilita el envío o recepción de llamadas, SMS, o el acceso al servicio de datos, que pasa a estar en manos de la persona suplantadora.

Obtenido el duplicado, se abre la vía de acceso a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder cambiar las contraseñas. En suma, posibilita la suplantación de identidad.

Y si bien, no se han visto afectados "Categorías especiales de datos personales" según define el RGPD en el artículo 9, ello no significa que los datos sustraídos no fueran de naturaleza sensible. No se trata del dato personal que se requiere para la expedición del duplicado de la tarjeta, si no de la tarjeta misma como dato personal asociada a una línea de telefonía titular de un usuario, que se obtiene con la finalidad de suplantar su identidad para obtener acceso -entre otros- a las aplicaciones bancarias o comercio electrónico, con la finalidad de interactuar y realizar operaciones en su nombre, autenticándose mediante un usuario y contraseña previamente arrebatados a ese usuario, así como con la autentificación de doble factor al recibir el SMS de confirmación en su propio terminal móvil donde tendrá inserida la tarjeta SIM duplicada.

- Artículo 76.2.b) LOPDGDD:

  · Vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal:

  El desarrollo de la actividad empresarial que desempeña XFERA requiere un tratamiento continuo y a gran escala de los datos personales de los clientes, según el número de líneas de telefonía móvil de voz informadas por XFERA (4.739.191 de clientes postpago y 1.758.708 de clientes prepago, en el año 2019), que posiciona a XFERA como una de las cuatro operadoras de telecomunicaciones más grandes de nuestro país.

Por otra parte, se toman en consideración los siguientes atenuantes:

- Artículo 83.2.c) RGPD:

  · Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados:

  Positivas.

  A saber:

(…)

- Artículo 83.2.f) RGPD:

  · Grado de cooperación con la autoridad de control:

  Alto.

  La Agencia considera que XFERA ha cooperado de forma favorable con la investigación, proporcionando respuesta a la mayoría de los requerimientos y formando parte del grupo de trabajo de esta Agencia respecto a la problemática de los duplicados de tarjeta SIM, lo que se valora de forma positiva.

- Artículo 76.2.c) LOPDGDD:

  · Los beneficios obtenidos como consecuencia de la comisión de la infracción:

  No considera esta Agencia que XFERA haya obtenido un beneficio económico más allá de percibir el precio del coste fijado para la emisión de los duplicados de las tarjetas SIM.

- Artículo 76.2.h) LOPDGDD:

  · Sometimiento a mecanismos de resolución de conflictos:

  Diversos operadores de telecomunicaciones, entre los que se encuentra XFERA, suscribieron con AUTOCONTROL un Protocolo que, sin perjuicio de las competencias propias de la AEPD, prevé mecanismos para la resolución privada de controversias relativas a la protección de datos en el ámbito de contratación y publicidad de servicios de comunicaciones electrónicas, con fecha 15 de septiembre de 2017. Protocolo cuya aplicación efectiva debe ser considerado como atenuante.

Se desestiman las alegaciones aducidas por XFERA en relación con el artículo 83.2.a), b) y c), tal y como se ha expuesto en este mismo FD.

Desaparece de la Resolución el factor agravante previsto en el artículo 83.2.e) del RGPD, tras considerarse que la sanción citada no es pertinente o relevante en relación con el procedimiento sancionador ahora tramitado (considerando 148 del RGPD).

Idéntico destino hemos aplicado al factor atenuante dispuesto en el artículo 76.2.a) de la LOPDGDD, relativo al carácter continuado de la infracción, pues la falta de concurrencia del presupuesto para su aplicación conlleva que no pueda ser tomado en consideración, siguiendo el criterio expresado por la SAN, Sala de lo Contencioso-administrativo, Sección 1ª, de 5 Mayo 2021, Rec. 1437/2020, que dice: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para*

la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante".

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la directora de la AEPD, RESUELVE:

PRIMERO: IMPONER a ***XFERA MÓVILES, S.A.***, con NIF ***A82528548***, 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 administrativa por importe de 200.000'00 (doscientos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a ***XFERA MÓVILES, S.A.***

TERCERO: Advertir a la sancionada que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el artículo 98.1.b) de la LPACAP, en el plazo de pago voluntario establecido en 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, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la AEPD en la entidad bancaria CAIXABANK, S.A. 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 LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al artículo 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la directora de la AEPD en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el artículo 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el intere-

sado 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 LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. 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

938-26102021

Mar España Martí
Directora de la AEPD