Expediente N.º: PS/00022/2021

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) con fecha 6 de agosto de 2019 interpone una reclamación ante la AEPD. La reclamación se dirige -entre otros- contra ***ORANGE ESPAGNE, S.A.U.*** con NIF ***A82009812*** (en adelante, ORANGE) por los siguientes motivos:

"Quiero denunciar el tratamiento de mis datos por parte de Orange y del Banco Santander, que ha permitido que me hayan realizado un fraude en mis cuentas bancarias de casi 15.000 euros.

Respecto a Orange, alguien suplantó mi identidad frente a un operador y consiguió cambiar mi email de contacto, sin que la llamada se realizara de mi móvil. Y después, consiguieron un duplicado de mi tarjeta SIM, paso imprescindible para conseguir los datos de acceso a mi banca online.

Tras darme cuenta, a pesar de haber puesto una palabra de seguridad para cualquier trámite con operadores de Orange, no siempre me la han preguntado (sobre todo los primeros días), por lo que no puedo estar segura de que pueda volver a pasar.

Respecto al Banco Santander, a través de varias llamadas a la línea telefónica y acceso a mis claves online con el duplicado de la tarjeta SIM, consiguieron cambiar mi firma electrónica y realizar dos tarjetas a mi nombre y varias operaciones (traspaso del crédito de dichas tarjetas y transferencias de mis cuentas a otras de desconocidos), todo esto en un breve lapso de tiempo (del 22 de julio al 23 de julio, se cree que desde las 19.30h a las 13h en que me doy cuenta), sin que el Banco se pusiera en contacto conmigo al detectar tantos movimientos (sobre 7 movimientos en 3 cuentas).

Aparte de las reclamaciones interpuestas, tanto al Banco como a Orange, y de las medidas judiciales que pueda llevar a cabo, desearía esta Agencia tomara las medidas precisas y oportunas. (…)"

Junto a la reclamación aporta la denuncia presentada ante la Guardia Civil de Baiona (Pontevedra), en fecha 24 de julio de 2019, con número de atestado ******ATESTADO.1*** en la que manifiesta:

'Que la dicente en el día de hoy, sobre las 09:00 horas comprobó que su teléfono móvil XIAOMI Mi A1-con número ******TELÉFONO.1*** *de la compañía ORANGE, con número de IMEI's* ******IMEI.1*** *y* ******IMEI.2****, dejó de funcionar.*

Se dirigió a la tienda de ORANGE para preguntar que habla sucedido, comprobando en la tienda que la tarjeta SIM ******SIM.1*** *que tenía instalada en el teléfono móvil no le funcionaba, por lo que le realizaron una nueva tarjeta SIM* ******SIM.2****.*

La empleada de la tienda se percató que la tarjeta SIM que tenía instalada en su teléfono no correspondía con la que figuraba en la base de datos de ORANGE. Que la tarjeta SIM que constaba en la base de datos de ORANGE es ******SIM.3****.*

Que en el momento que la dicente instaló la nueva tarjeta SIM ******SIM.2*** *recibió dos mensajes de texto (SMS) de SANTEVIÓS, con un código SMS para transferencias de 5000 euros y un SMS de INFOSNET con un código SMS para transferencia de 5000 euros.*

Que la manifestante, una vez le entregan el formulario de solicitud de cambios observa que el correo electrónico ******CUENTA DE CORREO.1*** *no corresponde con el correo facilitado a ORANGE. Que el correo que les facilitó es* ******CUENTA DE CORREO.2****(…)*

Que la manifestante se pone en contacto telefónico con ORANGE a través del 1470 y le informan que a ORANGE se realizaron dos llamadas, una para cambiar el correo electrónico y otra para solicitar el duplicado de la tarjeta SIM, llamadas que se realizaron el 22/07/20219, una a las 14:00 horas y la otra a las 19:15 horas constando el número de esta última ******NÚMERO.1****.*

Que desde la tienda de ORANGE entran en el perfil de usuario y se observa que figuran cinco llamadas al número de teléfono ******TELÉFONO.2*** *que corresponde a la banca online del Santander (…)*

Que la manifestante examina los movimientos de sus tres cuentas bancarias y de sus dos tarjetas y observa:

Que autor/es desconocidos habían realizado un traspaso de la tarjeta VISA ******VISA.1*** *por las cantidades de 700 y 500 euros a la ***CUENTA.1 (Banco Popular) siendo la cuenta espejo de la cuenta* ******CUENTA.2*** *(B. Santander).*

La manifestante se percata que el 22 de julio de 2019 autores desconocidos dieron de alta una nueva tarjeta de crédito VISA con numeración ******VISA.2.***

Que autor/es desconocidos realizan un traspaso de la tarjeta ******VISA.2*** *de 5000 euros a la cuenta bancaria numeración* ******CUENTA.3****(Banco Popular) siendo la cuenta espejo de la cuenta* ******CUENTA.4*** *(B. Santander).*

Que autor/es desconocidos realizan tres transferencias de su cuenta bancaria ******CUENTA.5,*** *(…) fueron de 1000 euros cada una, enviadas a las cuentas* ******CUENTA.6*** *(EVO BANCO);* ******CUENTA.7*** *(EVO BANCO) y* ******CUENTA.8*** *(OPEN BANK) que por cada una de estas transferencias le cobran la cantidad de 6 euros.*

Que autor/es desconocidos realizan una transferencia de la cuenta ******CUENTA.3****(…) a la cuenta* ******CUENTA.8*** *(OPEN BANK) por la cantidad de 250 euros constando un cargo de 6 euros en concepto de gastos.*

Que autor/es desconocidos de la cuenta con numeración ******CUENTA.1*** *(…) rea-*

lizaron tres transferencias, siendo la primera por la cantidad de 5000 euros a la cuenta ******CUENTA.6*** *(EVO BANCO). Una segunda transferencia de 250 euros a la cuenta* ******CUENTA.8*** *(OPEN BANK), una tercera transferencia de 250 euros a la cuenta* ******CUENTA.8*** *(OPEN BANK). (…)*

Asimismo, aporta justificante del resguardo de "Solicitud de cambios en el servicio Pospago de comunicaciones móviles" de fecha 23 de julio de 2019, que incluye el email de la persona suplantadora y el nuevo número de tarjeta SIM asignado.

También aporta el listado de llamadas desde dicha SIM a la línea telefónica del Santander (***TELÉFONO.2), y un resumen de las transferencias e ingresos realizados sin su consentimiento.

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 30 de septiembre de 2019, se dio traslado de la reclamación a ORANGE, para que procediera a su análisis y diera respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, ORANGE manifestó -entre otros argumentos- lo siguiente:

"(…) Los mencionados hechos ya habían sido puestos en conocimiento de Orange por parte de la reclamante, procediendo esta compañía al análisis de los hechos y a la consecución de una solución a favor de la reclamante con anterioridad a la notificación del requerimiento de información que nos ocupa, dando satisfacción así a su reclamación.

Pues bien, tras realizar el análisis y las comprobaciones oportunas sobre el caso, se verificó que tras la adquisición de una tarjeta SIM (…) que habitualmente cuenta con una alta afluencia de público para agilizar ciertos trámites, como el pago de facturas impagadas, las recargas de tarjetas de prepago, etc.), se procedió (…) el día 22 de julio de 2019 a las 18:52 horas.

Interesa destacar que (…) se realizó (…) incumpliendo las directrices establecidas por esta mercantil (…).

(…).

Segunda. - Informe sobre las medidas adoptadas para evitar que se produzcan Incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

En el presente supuesto, tan pronto como Orange ha tenido constancia (…), ha reforzado y robustecido los Protocolos implantados para la tramitación de determinados actos (entre los que se encuentran los de duplicado de tarjetas SIM) estableciendo para ello mayores controles y sistemas de verificación de la identidad con el objetivo de que esta situación no vuelva a repetirse.

En efecto, se viene a manifestar que, en primer lugar, Orange ha eliminado la posibilidad de (…), limitando así las operaciones permitidas en los citados (…) desde el 29 de julio de 2019.

En segundo lugar, y como medida adicional, Orange ha adoptado la decisión, con fecha de implantación 20 de septiembre de 2019, de que, (…) (entre las que se halla, (…), por los riesgos asociados inherentes a la misma), no puedan ser tramitadas a través (…), sino que el usuario está obligado para su activación (…) (tras autenticarse satisfactoriamente).

Este nuevo modelo de gestión ha sido implantado con la finalidad de evitar que se repitan situaciones similares a la que nos ocupa. Acompañamos como documento anexo nº 1 el citado nuevo modelo.

En este sentido, para mejor entendimiento por parte de la Agencia a la que tenemos el honor de dirigirnos, conviene aportar un mayor detalle en la explicación de este nuevo modelo de gestión de la solicitud y activación de duplicados de tarjetas SIM.

En orden a lograr mayor claridad expositiva, es importante diferenciar dos momentos o actuaciones diferenciadas en las solicitudes de duplicados de tarjetas SIM:

a) (…). La solicitud debe realizarse:

- (…).
- (…).

b) (…) debe realizarse:
- (…).
- (…).

(…).

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 26 de febrero de 2020, en el expediente con núm. de referencia *E/08994/2019*.

SEGUNDO: 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

TERCERO: ***B.B.B.*** (en adelante, la parte reclamante dos), en fecha 12 de marzo de 2020, presenta una reclamación ante el Registro del Ayuntamiento de Murcia, que es registrada en la AEPD en fecha 5 de junio de 2020, dirigida contra ORANGE, por los siguientes motivos:

> *"El día 8 de enero de 2020 me hicieron un duplicado de la tarjeta SIM sin mi conocimiento ni consentimiento. Se hicieron con mi línea del teléfono. Pidieron claves a Bankia y me hicieron reintegro de 300 euros desde Barcelona, Plaza de Cataluña 1, Sant Boi de Llobregat. Me han hecho suplantación de identidad."*

Junto a la reclamación aporta una denuncia con número de atestado ***XXX/YY*** de fecha 9 de enero de 2020, presentada ante la Dirección General de la Policía Nacional en las dependencias de San Andrés (Murcia), en la que manifiesta:

> *"Que en el día de la fecha la mujer del denunciante recibe un SMS el cual le informa de que a través del número del dicente ha solicitado un duplicado de tarjeta de su número de teléfono.*
>
> *Que el dicente manifiesta que no ha autorizado tal operación con su número por lo que se pone en contacto con su compañía de teléfono, ORANGE, confirmándole este la tramitación del duplicado, alegando que puede haber sido un error por parte de ORANGE.*
>
> *Que el dicente en ese momento se percata de que no dispone de cobertura en su teléfono móvil.*
>
> *Que decide comprobar sus cuentas bancarias percatándose de que le han sustraído 300 euros desde un cajero automático sito en el lugar del hecho sin autorización. (…)"*

Asimismo, también aporta la carta de respuesta de ORANGE de fecha 20 de enero de 2020, en la que le confirman la correcta activación del servicio de voz, una compensación por las molestias ocasionadas equivalente a un mes completo de la tarifa contratada, y trasladan las disculpas por las molestias ocasionadas.

En fecha 26 de junio de 2020, se dio traslado de la reclamación a ORANGE, para que procediera a su análisis y diera respuesta en el plazo de un mes.

En respuesta a dicho requerimiento, ORANGE manifestó -entre otros argumentos- lo siguiente:

> *"En primer lugar cumple destacar que, el duplicado de tarjeta SIM expuesto en el requerimiento que nos ocupa, fue detectado por Orange el mismo día de su activación, 08/01/2020, al asociarse la activación de la línea (…) al IMEI (…).*
>
> *En relación a lo anterior, los mencionados hechos ya habían sido puestos en co-*

nocimiento de Orange por parte de la reclamante, procediendo esta compañía al análisis de los hechos y a la consecución de una solución a favor de la reclamante con anterioridad a la notificación del requerimiento de información que nos ocupa, dando satisfacción así a su reclamación. En este sentido, Orange procedió a dar respuesta a la Reclamación Oficial notificada, (…).

En este sentido, tras realizar el análisis y las comprobaciones oportunas sobre el caso, se verificó que la activación del duplicado de tarjeta SIM de la línea ******TELÉFONO.3****, fue realizada con fecha 08/01/2020 (…). El duplicado de tarjeta (…). En ese sentido, tras un exhaustivo estudio de las circunstancias del caso que nos ocupa, Orange procedió a (…).*

Por todo lo anterior, esta compañía desconoce las razones que han llevado a reclamar ante la Agencia a la que tenemos el honor de dirigirnos los hechos que traen causa del presente requerimiento, al ser los mimos depurados e informados al afectado hace meses.

Segunda. - Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación y controles efectuados para comprobar su eficacia.

En el presente supuesto, tan pronto como Orange ha tenido constancia (…), se ha reforzado y robustecido los Protocolos implantados para la tramitación de determinados actos (entre los que se encuentran los de duplicado de tarjetas SIM) estableciendo para ello mayores controles y sistemas de verificación de la identidad con el objetivo de que esta situación no vuelva a repetirse.

En este sentido, para mejor entendimiento por parte de la Agencia a la que tenemos el honor de dirigirnos, conviene aportar un mayor detalle en la explicación de las tecnologías empleadas por mi representada en los procesos de identificación de la identidad del titular. (…)

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 31 de agosto de 2020, en el expediente con núm. de referencia *E/05031/2020****.***

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 ORANGE, en distintas fechas:

Requerimiento	Código Seguro de Verificación	Fecha requerimiento	Fecha notificación requerimiento
Primero	******CÓDIGO.1***	13/01/2020	13/01/2020

Segundo	***CÓDIGO.2	23/06/2020	25/06/2020
Tercero	***CÓDIGO.3	16/09/2020	17/09/2020

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.

Número de clientes de telefonía móvil total de la entidad.

En el segundo de los requerimientos, de fecha 23 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 ORANGE 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 (…).

B). Se pide copia del procedimiento establecido donde consten los controles en el caso de la tramitación de solicitudes (…) para la marca ORANGE. (En la información aportada no se describen, indicando en la tabla de controles "No disponible").

Se pide copia de las políticas de seguridad (Solicitud de SIM) para la marca ORANGE, 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) Se pide copia de las políticas de seguridad (solicitud de SIM y activación) para las marcas JAZZTEL y AMENA 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.

D). Información sobre los controles establecidos para tramitar el cambio de dirección de correo electrónico de un usuario.

Implicaciones de un cambio de dirección de correo electrónico en la activación de un nuevo duplicado de SIM. Forma en la que los supuestos suplantadores han podido activar una nueva SIM cambiando previamente este dato del usuario.

E) Para todas las marcas, en las entregas a domicilio, se pide información sobre si es posible cambiar la dirección de entrega de la SIM y bajo qué circunstancias y controles.

F). En la tabla de controles aportada se menciona, en los casos de empresas de mensajería: "Entrega sin validación de Documento de Identidad".

Se pide las 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 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 reclamados como suplantación de identidad o fraudulentos por los clientes, de la marca ORANGE. 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 únicamente:

- la fecha del cambio de SIM,

- el número de línea,

- canal de la solicitud,

- canal de entrega.

PUNTO 3

Sobre casos presentados ante esta Agencia que se resumen en la tabla: (que se da por íntegramente reproducida en este acto de trámite):

Se pide:

A) Circunstancias por las cuales se tramitó (…). Información si se comprobó (…).

Se pide aportar acreditación documental.

B) Motivo por el cual fue posible el duplicado de SIM en este caso. Acreditación de los controles que se pasaron sobre la identidad del solicitante tanto en la propia solicitud (…) como en la activación del SIM.

C) En este caso se cambió la dirección de correo electrónico de forma previa a la solicitud.

Se pide información de cómo cambiaron la dirección de correo del cliente y acreditación documental de los controles que se pasaron para la identificación del cliente.

D) Acciones emprendidas por la entidad 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 han realizado cambios en el procedimiento para evitar casos futuros similares.

- 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 16 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: (cuyo contenido se da por íntegramente reproducido en este acto de trámite):

A. Se pide, en los casos de solicitud y entrega en punto de venta, copia de los DNIs o documentos identificativos aportados por los solicitantes del cambio de SIM.

B. Para el caso de solicitud (…):

- Copia de la grabación de la conversación donde el solicitante supera la po-

lítica de seguridad. Si la autenticación se realizó mediante (…), aportar documentación acreditativa.

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

C. Para cada uno de los casos de solicitud (…):

- Información sobre si de forma previa (menos de 2 días) a la solicitud de los SIM se ha procedido al cambio/solicitud de contraseña de acceso app para la cuenta del cliente. Aportar documentación acreditativa.

- Información sobre si en los casos de solicitud o modificación previa de la contraseña, se ha seguido el procedimiento de seguridad del sistema "(…)". Aportar documentación acreditativa.

Si se ha modificado la contraseña por otros medios informar de cuales han sido y aportar documentación acreditativa de ello.

D. Activación de la SIM.

Para cada uno de los casos de entrega por mensajería:

- Información sobre la vía de activación de la tarjeta.

- En caso de activación presencial en punto de venta, se pide copia del documento identificativo presentado.

En caso de activación telefónica, grabación de la llamada durante la cual el solicitante supere la política de seguridad.

En caso de activación mediante (…), se solicita con carácter general si se solicita alguna acreditación de identidad adicional al cliente para activar la tarjeta, además de las credenciales de entrada a (…).

PUNTO 2

Sobre el siguiente caso presentado ante esta Agencia: (cuya tabla se da por íntegramente reproducida en este acto de trámite):

Se pide copia del DNI o documentación identificativa aportada, así como resto de documentación asociada, aportada por el solicitante.

Se pide información detallada sobre el tipo de alerta que se generó en el sistema y chequeo de IMEI, según manifestaciones en la carta dirigida al afectado "*(…)".*

Tiempo transcurrido entre el duplicado del SIM y la restricción de la línea.

Acciones emprendidas por la entidad 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 han realizado cambios en el procedimiento para evitar casos futuros similares.

- Si se ha contactado con el cliente para alertarle de lo sucedido y sobre la

resolución de su caso.

QUINTO: Con fecha 28 de enero, 1 de julio y 24 de septiembre de 2020, ORANGE solicita la ampliación del plazo legal conferido para contestar dichos requerimientos.

Con fecha 31 de enero y 15 de julio de 2020, la Subdirectora General de Inspección de Datos acuerda la ampliación del plazo para responder por un periodo de cinco días, que deberán computarse a partir del día siguiente a aquel en el que finalice el primer plazo otorgado.

SEXTO: En respuesta a los tres requerimientos formulados, ORANGE 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:

Las medidas de control en la solicitud y activación del duplicado de SIM son distintas en función de la marca y del canal utilizado para solicitar el duplicado de la SIM:

Marca ORANGE:

- (…):

(…)

- (…):

(…)

- (…):

(…).

- (…).

Marca JAZZTEL:

- (..).
- (…).

(…)

- (…):
  - (…).
- (…):
  - (…).

Marca AMENA:

- (…).

- (…).

- (…).

- (…):

(…).

- (…):

- (…)

- (…):

-(…).

- (…):

-(…).

(…)

3.- Información sobre las instrucciones giradas a los operadores:

(…)

4.- Información sobre la realización de los controles:

(…)

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

(…)

6.- Acciones emprendidas por la entidad:

(…):

-. (…).

-. (…).

-. (…).

-. (…).

-. (…).

-. (…).

-. (…).

Medidas generales implementadas en distintas marcas.

-. (…).

-. (…).

-. (…):

-. (…).

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

"(…)."

Respecto a los casos presentados ante la agencia:

RECLAMANTE UNO:

-. Acciones previas: se cambió la dirección de correo electrónico de forma previa a la solicitud de SIM. Se ha pedido información de cómo cambiaron la dirección de correo del cliente y acreditación documental de los controles que se pasaron para la identificación del cliente, indicando los representantes de ORANGE(…)

.- Solicitud de cambio: Duplicado facilitado (..) (ya retiradas).

.- Activación (…).

En el fragmento de llamada que quedó grabada, (…). El agente quiso enviar a través de (…). Posteriormente, el agente (…) definidas en los procesos de ORANGE.

. - Perjuicios: Se denuncian operaciones bancarias fraudulentas utilizando la copia del SIM.

. - Acciones emprendidas por la entidad, 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 han realizado cambios en el procedimiento para evitar casos futuros similares.

Las acciones tomadas para evitar casos de “cambios de tarjetas SIM no consentidas” son:

- Tal y como se ha expuesto anteriormente, (…).

- En los supuestos de cambio de SIM no consentido que se han producido (…), se ha podido constatar que el comercial que atendió al defraudador (…).

Como medida reactiva ante esta falta de diligencia, ORANGE aplica en estos casos una penalización de XXX € al punto de venta que no observe la política de validación de documentos.

- Además, hasta el 20 de septiembre del año 2019 cabía la posibilidad en Orange de que (…). A partir de la fecha indicada, y ante los numerosos casos de cambio de SIM no autorizados realizados a través (…), se elimina esta posibilidad en la marca Orange, con la única excepción del periodo comprendido entre el 16 marzo a 28 de junio con motivo de las medidas extraordinarias adoptadas por el COVID-19.

- Se han suprimido (…). En este sentido se pretende que la política de autenticación sea cada vez más estricta y dificulte la comisión de

fraude.

- Se han implementado nuevas medidas de autenticación de clientes (…) como la relativa a (…), que se usa como dato seguro y cierto para pasar política de seguridad estricta al cliente.

< Si se ha contactado con el cliente para alertarle de lo sucedido y sobre la resolución de su caso.

Tras reiterados intentos de contactar con la afectada, finalmente se pudo localizar y se le informó de los pasos a seguir.

(…) Se intenta contestar a cuantas preguntas y otras gestiones puedan surgirle al cliente afectado y se abona el coste que le haya supuesto realizar el cambio de tarjeta SIM para recuperar su línea tras ese cambio no consentido.

Aportan impresión de pantalla (…) de una interacción con el cliente donde quedan reflejados los contactos mantenidos con cliente.

RECLAMANTE DOS:

-. Solicitud de cambio de SIM: (…).

Aportan copia del DNI aportado así como de una denuncia por robo de DNI. Los representantes de la entidad han manifestado que (…).

(…).

Se hace notar que faltan algunos documentos a entregar según el protocolo de ORANGE. (…):

- (…).
- (…).

-. Perjuicios: Se denuncian operaciones bancarias fraudulentas utilizando la copia del SIM.

-. Controles: (…) ORANGE dispone de una (…), empleada como medida de seguridad en la prevención y detección de fraude. (…). En el caso concreto de duplicados de tarjetas SIM, el sistema funciona de la siguiente forma:

- (…).
- (…).

(…).

Sobre el tiempo transcurrido entre el duplicado del SIM y la restricción de la línea los representantes de ORANGE manifiestan únicamente que en el mismo día.

Sobre otros casos no presentados ante la agencia:

Aportado el listado el desglose de los 20 casos es el siguiente:

- (…).
- (…)
- (…).

Requerida (…) para las solicitudes/recogidas presenciales en tienda, los representantes de ORANGE aportan 4 (…) para 4 de los casos. Se verifica que dos (…). En otro caso se aporta (…). Indican que para dos de los casos no ha sido posible obtener la información requerida por parte del punto de venta pero faltan en total 5 (…) de los 9 requeridos.

(…):

- (…).
- (…).

Requerida la grabación de la conversación para el caso telefónico, así como documentación acreditativa de la aplicación (…) en su caso, los representantes de la entidad indican que aportan copia de la grabación de la activación de la tarjeta correspondiente, manifestando que:

"(…).

(…)."

Se ha solicitado a ORANGE el detalle de las circunstancias que concurrieron para para acceder a la tramitación (…), indicando los representantes de la entidad que la solicitud de duplicado fue realizada en fecha 22/04/2019 y durante el periodo comprendido del 16 marzo al 28 de junio de 2020, debido a las medidas excepcionales adoptadas como consecuencia del Covid-19, se procedió a habilitar (…) como como medida de contingencia, para gestionar la solicitud de cambio y duplicado de tarjeta SIM.

Sobre los casos de activación mediante (…), se ha solicitado con carácter general, si se solicita alguna (…) al cliente para activar la tarjeta, además de (…). Ante ello, los representantes de la entidad han manifestado:

"(…).

(…)."

SÉPTIMO: Con fecha 27 de agosto de 2020, se obtiene información comercial sobre el volumen de ventas de ORANGE durante el año 2019 siendo los resultados de 4.779.670.000 euros. El capital social asciende a 1.097.665.000 euros.

OCTAVO: Con fecha 27 de enero de 2021, 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
ORANGE	2.569.156	0	8.953.958	2.204.408

NOVENO: Con fecha 11 de febrero de 2021**,** la directora de la AEPD acuerda iniciar un procedimiento sancionador contra ORANGE, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), 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 2.000.000,00 de euros (dos millones de euros), sin perjuicio de lo que resultase de la instrucción.

El Acuerdo de iniciación se notifica a ORANGE, en fecha 15 de febrero de 2021, a través de Carpeta Ciudadana, según confirmación que figura en el expediente.

DÉCIMO: Con fecha 16 de febrero de 2021, ORANGE solicita la ampliación del plazo para aducir alegaciones y aportar documentos u otros elementos de juicio.

UNDÉCIMO: Con fecha 17 de febrero 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 ORANGE en fecha 18 de febrero de 2021.

DUODÉCIMO**:** Con fecha 8 de marzo de 2021, se recibe en esta Agencia, en tiempo y forma, escrito del representante de ORANGE en el que aduce alegaciones y tras manifestar lo que a su derecho conviene, termina solicitando el archivo del procedimiento y subsidiariamente, que la AEPD considere las circunstancias atenuantes fundamentadas y termine el procedimiento mediante un apercibimiento y con la imposición de las obligaciones de implementar medidas correctivas idóneas.

En síntesis aduce que:

> PREVIA.- EXISTENCIA DE UN GRUPO DE TRABAJO SOBRE DUPLICIDAD DE LAS TARJETAS SIM LIDERADO POR LA AEPD.
>
> El hecho de que en el seno de dicho Grupo de Trabajo (GT) se requiera a ORANGE para compartir toda la información respecto a los procesos y múltiples controles preventivos y reactivos para la prevención y gestión de este tipo de fraudes, debería llevarnos a pensar que dicha compartición se realiza dentro del más absoluto y estricto marco de confianza y plena confidencialidad.
>
> Las colaboraciones público-privadas aportan a la Administración la ventaja de que, empresas especializadas en determinados servicios, aporten el conocimiento y las mejores soluciones en asuntos que son de interés para los consumidores y para los ciudadanos.
>
> También hay que destacar las mesas de trabajo abiertas con el Ministerio del Interior. Durante el año 2020 la colaboración con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), ha supuesto más de 40.308 solicitudes atendidas y derivadas de los Juzgados; 45.552 de solicitudes atendidas y derivadas de la Policía Judicial y 50.056 intervenciones telefónicas llevadas a cabo (entre altas, bajas y ceses).
>
> Además, el personal de ORANGE ha sido condecorado con la Cruz al mérito Civil con distintivo blanco.
>
> Asimismo, ha participado activamente en el informe de la ponencia de estudios sobre los riesgos derivados del uso de la red por parte de los menores en el Senado en la firma de un Protocolo de Alto Nivel.
>
> Por su parte, la AEPD, ha considerado que es el momento idóneo para proponer sanciones millonarias a las mismas entidades con las que está sentándose para acordar medidas comunes, precedente éste inaudito y sorpresivo.
>
> Lo apropiado sería esperar a tener unas conclusiones y, una vez conocidas y

dado un plazo adecuado para lograr su implantación, sea entonces, cuando se requiera a los operadores que acrediten su cumplimiento y en caso de no haberlo hecho, sea entonces cuando se propongan sanciones.

Las reuniones del GT han sufrido retrasos derivados de la pandemia COVID 19, que han ralentizado su periodicidad -retraso de la prevista el 16/03/2020 al 4/12/2020- lo que ha perjudicado el análisis de la problemática y de la propuesta e implantación de las mejoras.

Parece que la Agencia no tiene ningún tipo de pretensión de dar cumplimiento a los principios de lealtad institucional que se presumen en cualquier relación de colaboración público-privada, en tanto, al mismo tiempo que solicita la colaboración, información, participación activa y efectiva en el GT, inicia un procedimiento sancionador que versa sobre la materia tratada en el GT.

La AEPD, cruza los límites más elementales de la lealtad institucional que se presume a un organismo público en este marco colaborativo.

La apertura de este procedimiento y otros similares dificulta sobremanera la existencia de un marco de confianza entre ORANGE y la AEPD, y, de todo el sector de las telecomunicaciones a nivel nacional.

ORANGE quiere dejar constancia que esta forma de proceder afecta gravemente al principio de confianza que presumía poder depositar en la AEPD y supone un riesgo a los objetivos del GT, lo que será objeto de análisis interno y probablemente sectorial respecto al marco colaborativo con Autoridades Administrativas que persigan este bien común de los ciudadanos con planes de acción y colaboración conjunta.

PRIMERA. - INCORRECCIÓN Y FALTA DE EXACTITUD EN LAS APRECIACIONES SOBRE EL FRAUDE DE DUPLICADO DE TARJETA SIM.

La descripción realizada por parte de la AEPD contiene diversas afirmaciones inexactas e incorrecciones técnicas que inducen a una interpretación inadecuada de los hechos y de sus consecuencias jurídicas.

Las tarjetas SIM no sirven “para identificar al abonado ante la red de telefonía móvil”, sino que identifican un número de teléfono, sin incluir ninguna información que permita a terceros, distintos del propio operador de telecomunicaciones con la que tiene contratado el servicio, identificar al abonado.

El hecho de que el uso posterior de la SIM duplicada tenga como objetivo la comisión de otros delitos -realización de operaciones bancarias fraudulentas-, bajo ningún concepto puede considerarse dentro del ámbito de responsabilidad de ORANGE. Por sí mismo, este acto, no es suficiente para realizar operaciones bancarias en nombre de los titulares iniciales de las tarjetas SIM, sino que ha de producirse una actividad delictiva adicional e independiente a la anterior.

El uso por parte de las entidades bancarias de un sistema de doble factor de autenticación que implica el envío por SMS de las claves de ratificación para la realización de determinadas operaciones es una operativa sobre la que ORANGE no tiene ninguna capacidad de decisión.

No existe un nexo causal entre la suplantación de identidad para la consecución de un duplicado de la tarjeta y la realización de operaciones bancarias fraudulentas u otro tipo de operaciones de suplantación de identidad en otro

tipo de plataformas online, sino que lo que realmente se produce es una usurpación inicial de la identidad de los afectados ante la entidad bancaria y derivada de ella y con posterioridad, se produciría la confirmación de las operaciones mediante el uso de las claves remitidas por SMS.

Esta posibilidad sólo se daría cuando el medio establecido para garantizar la seguridad se correspondiese con el envío de un SMS, ya que el doble factor de seguridad (denominados de forma genérica “sistemas de autenticación con contraseña de un solo uso”, o “One Time Password”) no tiene por qué configurarse necesariamente de este modo, siendo esta una opción cuya elección compete a la entidad bancaria y/o al usuario correspondiente, dado que muchas plataformas permiten utilizar como medio para notificar el segundo factor de autenticación, el SMS, el email, o aplicaciones de generación de códigos temporales tipo Google Authenticator o semejantes.

Estos hechos son perfectamente conocidos por la AEPD que incluso tiene publicada en su web una publicación denominada “Identificación en servicios de pago online”.

Por lo tanto, las consideraciones plasmadas por la AEPD en el Acuerdo de inicio sobre que la consecuencia última de la suplantación de identidad ante ORANGE es la realización de operaciones bancarias no autorizadas deben ser matizadas, ya que esta posibilidad solo existe cuando éste sea el medio elegido para la confirmación de las operaciones y además, previa y necesariamente, la propia identidad bancaria o el usuario no hayan adoptado la diligencia suficiente para la protección de los medios iniciales de verificación de la identidad (primer factor) que permiten el acceso a la herramienta desde la que se gestionan la operativa bancaria.

El mismo efecto podría producirse también sin necesidad de suplantación de identidad. Este sería el caso de que un abonado decidiese dar de baja su número de teléfono y posteriormente fuera objeto de una portabilidad. Si el usuario no adoptase la diligencia debida para actualizar su información ante las diferentes entidades a las que hubiera facilitado el dato de su número de teléfono como medio de autenticación, posibilitaría que el tercero que recibiese ese número pudiese recibir los mensajes de confirmación emitidos por dichas entidades. Igual efecto podría darse en el caso de robo de un terminal que el usuario no hubiese protegido adecuadamente (permitiendo acceder a su contenido sin necesidad emplear contraseñas, huella dactilar u otras medidas de seguridad).

Por lo tanto, la obtención ilícita del duplicado de la tarjeta SIM no es suficiente para la realización de operaciones bancarias fraudulentas, ni tiene porqué concurrir para permitir llevar a cabo las mismas, por lo que no puede atribuírsele de forma genérica esta responsabilidad.

No obstante, ORANGE no es ajena a la problemática derivada del potencial uso de las tarjetas duplicadas con fines ilícitos. Es por ello, por lo que ha implementado mecanismos de seguridad reforzada en relación con las condiciones para su solicitud.

SEGUNDA. - GENERALIZACIÓN NO FUNDADA DE CONSECUENCIAS NEGATIVAS ASOCIADAS A LA EMISIÓN DEL DUPLICADO DE LA TARJETA SIM.

Muchas de las afirmaciones contenidas entre los argumentos esgrimidos por la

AEPD son inexactos o erróneos.

No es cierto 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".*

Ha de indicarse que estos se pueden almacenar "físicamente" en las tarjetas SIM, por lo que esta información no estaría en los duplicados que puedan emitirse, sino que se mantendrían únicamente en la SIM original, bajo control de su titular, salvo que el usuario haya elegido almacenarlas en entornos asociados a Android o Apple en cuyo caso el operador tampoco tiene capacidad de actuación, por lo que, de nuevo, la AEPD vuelve a realizar una afirmación errónea cuya única finalidad es justificar la abultada sanción propuesta en base a los supuestos daños que se han provocado al titular de la numeración.

En cuanto a la posibilidad de acceder a las cuentas de correo, bancarias y otras aludidas, es obvio que el duplicado de la tarjeta no permite, por sí solo, el acceso a las mismas, sino que es necesario, al menos, conocer el identificador del usuario para poder acceder a cualquiera de las cuentas.

A mayor abundamiento, cabe puntualizar que cuando el suplantador se dirige a ORANGE para solicitar el duplicado cuenta ya con mucha información relativa al interesado, que es necesaria para la gestión de la solicitud. Por lo tanto, la obtención de esta información, de forma presumiblemente ilícita, es responsabilidad de terceros o del propio titular de los datos, existiendo en muchos casos un comportamiento imprudente de estos últimos en la custodia de su información personal.

La responsabilidad de ORANGE no puede extenderse más allá de aquellas cuestiones que quedan bajo su ámbito de actuación. Interpretar lo contrario significa hacerla responsable de la seguridad de la información custodiada por terceros, e incluso de las posibles actuaciones negligentes de estos o del propio titular de los datos, así como del hecho de que existan auténticas mafias especializadas en cometer delitos.

En lo que se refiere a la posible vulneración de los principios de seguridad, confidencialidad de los datos y de responsabilidad proactiva, si bien es cierto que existe una incidencia relacionada con la seguridad de la información, no se ha producido en puridad un acceso a datos personales de los clientes como consecuencia de esta. La única información que los suplantadores habrían conseguido es el número de teléfono y en su caso los códigos de verificación de realización de operaciones bancarias que, si bien es información confidencial, bajo ningún concepto pueden ser considerados como datos personales por sí mismos.

Por tanto, si bien durante el proceso de solicitud del duplicado se tratan datos personales, esto no implica que haya un tratamiento ilícito derivado de la falta de diligencia de ORANGE, sino que ORANGE realiza estas operaciones solicitando datos a quien supuestamente es su titular y para hacer verificaciones, no habiéndose facilitado ningún tipo de información personal que no tuviese inicialmente el solicitante.

A este respecto, ha de remarcarse que los datos personales tratados de forma ilícita no son obtenidos de ORANGE, sino que los suplantadores los obtienen

previamente de otras fuentes (el propio interesado o terceros responsables de dichos datos). Incluso, como consta en el expediente, el delito de suplantación va acompañado de falsificaciones de documentos públicos, como copias de DNI o presuntas denuncias presentadas a la policía, que son aportados como medio para superar las medidas de control de ORANGE.

No existe regulación específica alguna que establezca las obligaciones en relación con esta operativa, y la única que podría considerarse como referencia, por tener ciertas similitudes en cuanto a la materia, es la Circular 1/2009, de 16 de abril de 2009, de la Comisión del Mercado de las Telecomunicaciones, que regula el propio procedimiento de contratación inicial de los servicios de telecomunicaciones, y en la que no se contiene ninguna exigencia de seguridad equiparable a las que la AEPD pretende exigir en relación con un procedimiento que sería secundario respecto del regulado en dicha circular.

Tampoco ha quedado acreditado ni consta en las denuncias referencia alguna a que los delincuentes hayan conseguido obtener datos personales de ORANGE, por lo que no puede hablarse de incumplimiento de medidas de protección de los datos personales.

La AEPD, y en procedimientos muy recientes, no venía considerando que concurriese un incumplimiento de medidas de seguridad en relación con los supuestos en los que se producía una suplantación de identidad en casos exactamente idénticos. Así, podemos citar, por ejemplo: E-04919, PS-00144-2019, PS-00235-2020, PS-00348-2020, E-01178-2020.

En ninguno de ellos se observa que exista una calificación como una infracción de las obligaciones de seguridad exigidas en el artículo 32 del RGPD.

Invoca el artículo 54 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (ya derogada), en su apartado primero que decía: deberán de ser motivados (…) los actos “que se separen del criterio seguido en actuaciones precedentes”. Es decir, que ante supuestos de hecho iguales la aplicación de soluciones diferentes deberá justificarse “con sucinta referencia de hechos y fundamentos de derecho” del motivo de tal disparidad a fin de no atentar frente al principio de seguridad jurídica.

La fundamentación realizada se limita a hacer referencia a posibles vulnerabilidades, que en ningún caso se identifican, ni mucho menos se expone por qué las mismas pueden ser calificadas como insuficientes o inadecuadas.

Es también destacable, que se la responsabilice de los efectos derivados de otras actuaciones que sí implican un acceso no autorizado a los datos personales de los afectados, víctimas de supuestos de phishing o similares, que sí permiten el acceso a información personal protegida por otros responsables del tratamiento.

TERCERA. - IDONEIDAD Y CUMPLIMIENTO DE LAS MEDIDAS PREVENTIVAS IMPLEMENTADAS POR ORANGE.

ORANGE ha realizado un estudio detallado de sus actividades de tratamiento de datos personales llevadas a cabo y ha adoptado las medidas pertinentes para que los mismos se realicen conforme a lo dispuesto en el RGPD.

En lo referente a la seguridad del proceso ha aportado evidencias de la existen-

cia de protocolos específicos adecuados a los riesgos identificados.

Cuenta con medidas organizativas que han sido comunicadas a todo el personal implicado en el tratamiento de datos personales.

Es importante indicar que las medidas organizativas de seguridad están soportadas por (…) que se encarga de implementar y operar la seguridad, medir (…). Con el fin de aportar confiabilidad a terceras partes sobre el adecuado funcionamiento de estas medidas, tanto técnicas como organizativas, ORANGE mantiene y certifica Sistemas de Gestión de Seguridad de la Información basados en ISO27001 y Esquema Nacional de Seguridad.

Los protocolos existentes han sido comunicados a todos los implicados en la gestión de las solicitudes de los duplicados, incluyendo penalizaciones en el caso de que se detecten incumplimientos de los procedimientos establecidos.

La operativa definida ha tenido en cuenta los riesgos asociados a la realización de este tipo de gestiones y los parámetros para su ejecución han sido puestos en conocimiento de las personas implicadas en su tramitación. El número de casos es ínfimo respecto al total de operaciones realizadas.

Si bien se han ido aumentando los medios y controles para garantizar el estricto cumplimiento del protocolo establecido, no es posible erradicar la posibilidad de su contravención por los usuarios, puesto que, en última instancia, depende de una actuación leal por parte de la persona que tramita la solicitud, que es conocedora de las instrucciones que debe seguir en cada caso.

La pretendida solución planteada por la AEPD consistente en la automatización total de los controles para evitar acciones no autorizadas, si bien hipotéticamente podría permitir un mejor control de los procedimientos, tendría un coste desorbitado ya que implicaría una monitorización sistemática de toda la actividad del usuario (a modo de ejemplo el sistema debería permitir: conocer y analizar el contenido de la conversación mantenida con los clientes, conocer y verificar el contenido de todos los posibles documentos que puedan ser puestos a disposición durante la solicitud, validando su adecuación en cada caso, conocer si la respuesta a las preguntas se corresponde con la información existente, etc.).

En este sentido, la AEPD no justifica en modo alguno la proporcionalidad de la medida propuesta, ni que la misma fuera la idónea teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento.

La medida supone, además, ignorar la realidad de la actuación de los usuarios encargados de la realización de estas gestiones que cumplen en la práctica totalidad de los casos con las indicaciones recibidas por parte de ORANGE.

Igualmente, tampoco tiene en cuenta el escaso número de supuestos en los que se ha producido una contingencia asociada a la solicitud de un duplicado de tarjeta, que concretamente representa el (…) % de los casos.

CUARTA. - ACTUACIÓN DILIGENTE DE ORANGE.

ORANGE no ha implementado “medidas de seguridad estáticas”, sino que, ha procedido sistemáticamente a implementar mejoras en las medidas adoptadas en cuanto ha tenido conocimiento de la existencia de cualquier vulnerabilidad.

En el caso analizado los datos personales de las víctimas son usurpados con anterioridad a que los delincuentes se dirijan a ORANGE y que, precisamente como consecuencia de tener acceso a información personal que solo debiera estar en posesión del interesado, permiten materializar la suplantación de identidad ante ORANGE.

Esta circunstancia en nada obsta el hecho de que ORANGE haya cumplido con sus obligaciones conforme a lo expuesto en el considerando 83 del RGPD al que alude la AEPD.

No puede hablarse en ningún caso de negligencia, ya que las circunstancias concretas en las que se producen los hechos, en la que los delincuentes bajo la apariencia de víctimas de un robo y empleando argucias y documentación fraudulenta con apariencia real (…) consiguen engañar a la persona a la que se le solicita en duplicado. (…). Por lo tanto, se trata de un engaño suficiente, por revestir éste *"apariencia de realidad y seriedad suficiente para engañar a personas de mediana perspicacia y diligencia"* (así considerado, entre otras muchas, en la STS 2362/2020).

Concurren puntualmente ciertos incumplimientos parciales de los protocolos dispuestos por ORANGE, que en determinados casos contribuyen a la consecución del fin perseguido por los defraudadores.

Sin embargo, esto no permite concluir que estos hechos pongan *"de manifiesto una serie de vulnerabilidades en las medidas de seguridad implantadas y, por lo tanto, se infiere la responsabilidad de ORANGE como responsable del tratamiento en términos de negligencia, falta de supervisión y control".*

Al contrario, las medidas implementadas por ORANGE son adecuadas para mitigar, de forma mayoritaria, los riesgos relacionados con este tipo de fraudes. En la práctica, tal y como consta informado, la eficiencia de estas medidas roza el 100% de los casos.

Ha de recordarse que, aunque se pudiesen haber incumplido puntualmente y de forma parcial por parte de las personas encargadas de la tramitación algunas de las obligaciones de verificación, existen factores de seguridad combinados que dificultan el objetivo de los defraudadores. (…)

Solo en supuestos excepcionales en los que los medios empleados para la desarrollar las estafas son especialmente sofisticados, combinado en algún supuesto con concretas omisiones de algunos de los requisitos establecidos por ORANGE por parte de los implicados en la tramitación de las solicitudes, se ha producido el resultado de suplantación de la identidad de los clientes.

En este sentido, puede emplearse como referencia la Circular 1/2016 de la Fiscalía General del Estado, relativa los protocolos de Compliance penal en la que se sostiene que *"el delito no invalida necesariamente el programa de prevención, que puede haber sido diseñado e implementado adecuadamente sin llegar a tener una eficacia absoluta".*

Según ORANGE, ha quedado acreditado que:

- Ha establecido protocolos adecuados para la prevención de suplantaciones de identidad en el proceso de solicitudes de duplicados de tarjeta.

- Ha comunicado debidamente el contenido de estos protocolos y las obligacio-

nes que corresponden a las personas implicadas en la tramitación.

- Ha realizado mejoras en los procesos cuando ha tenido conocimiento de vulnerabilidades, tales como refuerzos en las garantías y limitación de canales para la solicitud o inclusión de nuevos métodos de control más eficaces (como (…) lanzado en octubre de 2020).

- Ha adoptado medidas sancionadoras frente a los incumplimientos de los protocolos.

- Ha actuado de la manera más diligente posible, de forma inmediata, eficiente y ejecutiva, en los casos en los que ha tenido conocimiento de cualquier hecho.

- Cuenta con sistemas para la verificación del cumplimiento de sus obligaciones por parte de las personas implicadas.

- Ha presentado denuncias por las estafas cometidas y colabora para que pueda identificarse a los culpables y evitar futuros supuestos similares.

En consecuencia, la actividad de ORANGE no puede ser catalogada como negligente, ni ha existido falta de supervisión o control.

Invoca la STS 1232/2018 de 18 de julio de 2018, que recuerda lo que puede considerarse como "negligencia" o "culpa in vigilando" por parte de una empresa (sociedad) en relación con el comportamiento de sus empleados a colaboradores, exponiendo que: *"Cabría, en efecto, contemplar en abstracto una culpa in vigilando de la sociedad, partiendo del deber -ampliamente analizado por la doctrina y la jurisprudencia civiles- que pesa sobre las empresas de velar por el comportamiento de sus dependientes, apoderados o empleados para evitar que actuaciones culposas o dolosas de éstos puedan causar daños a terceros que han confiado en la compañía en cuyo nombre o por cuya cuenta actúan."*

Así, de acuerdo con el criterio del Tribunal Supremo, no cabría responsabilizar a ORANGE aun cuando su empleado o colaborador hubiera sido negligente en su actuación, ya que se requerirían "actuaciones culposas o dolosas" por parte de ORANGE, que bajo ningún concepto se han producido en los casos objeto de análisis.

Por otro lado, aun si fuera posible sancionar en caso de que la conducta fuera calificada de negligente, en esta misma Sentencia se recogen los requisitos necesarios sobre el contenido que ha de cumplir una acusación de este tipo en un expediente sancionador: "*Una calificación amparada en la culpa in vigilando, empero, necesitaría un elemento más para permitir afirmar la responsabilidad en el ámbito sancionador (en nuestro caso, por infracciones tributarias): una justificación expresa, suficiente y pormenorizada sobre la vulneración del deber de vigilar que debería ofrecer en su resolución el órgano sancionador, analizando las circunstancias del caso y determinando cuál ha sido el concreto comportamiento de la sociedad revelador de la infracción de aquella obligación. 3. En definitiva: a) No puede calificarse como dolosa una conducta como la que nos ocupa, pues -a tenor de los propios hechos que la integran- no cabe hablar de intención o de voluntad de realizar el comportamiento típico; b) Solo cabría afirmar en tales supuestos la "negligencia" si se infringen los deberes de vigilancia que pesan sobre la sociedad en relación con las personas que actúan en su nombre y siempre que tal vulneración aparezca constatada y justificada expresa y pormenorizadamente en el acuerdo sancionador, que deberá analizar*

las circunstancias del caso y en qué medida la falta de vigilancia ha contribuido a la comisión de la infracción."

De igual forma, el TSJ de Madrid en su Sentencia 568/2020 de 10 Sep. 2020 establece: *"Habrá de concurrir, pues, una conducta dolosa o negligente, ya sea negligencia grave o leve o simple. Y no existe negligencia, ni por tanto infracción, "cuando se haya puesto la diligencia necesaria en el cumplimiento de las obligaciones tributarias" (artículo 179.2.d) de la LGT 58/2003)".*

En vista de lo anterior, la jurisprudencia ampara el comportamiento de ORANGE, al haber establecido un protocolo de actuación elaborado teniendo en cuenta los riesgos existentes, que fue puesto a disposición de todos los implicados y que, si se hubiera seguido por estos, no se habría accedido a la entrega de la copia ilícita de la tarjeta.

Además, con respecto a la responsabilidad in vigilando de la sociedad, resulta incuestionable que únicamente se puede achacar cuando se trate de actuaciones culposas o dolosas, no así negligentes como ha sido identificada la actuación de ORANGE por la propia AEPD, a pesar de que dista mucho de serlo.

QUINTA. – FALTA DE PROPORCIONALIDAD DE LA SANCIÓN PROPUESTA.

No se ha producido un incumplimiento de la normativa de protección de datos, ya que, ORANGE ha tomado todas las medidas técnicas y organizativas necesarias para evitar el fraude en la solicitud de los duplicados de las tarjetas SIM.

En cuanto a la duración de la infracción no se trata de situaciones que se perpetúan en el tiempo, sino que son hechos independientes.

En cuanto al número de interesados afectados no cabe considerar el número de supuestos totales como una causa de agravación sin haber determinado la concurrencia de culpabilidad de ORANGE en cada uno de ellos.

En cuanto al nivel de los daños y perjuicios sufridos no es factible tratar de responsabilizar a ORANGE respecto de situaciones relativas al uso de los duplicados de la tarjeta que derivan de incidentes de seguridad de la información con los que ORANGE no tiene relación alguna. La duplicación de la tarjeta no deriva directamente, ni necesariamente, en operaciones bancarias fraudulentas, ya que las medidas de seguridad y los accesos a los que se tienen para realiza las operaciones bancarias son totalmente ajenos a la duplicación de la tarjeta SIM.

Tampoco cabe interpretar intencionalidad o negligencia en su actuación. En todo caso, ha de ser considerada diligente y actuar este hecho como atenuante.

Sobre el grado de responsabilidad: lejos de suponer este criterio un agravante, debería interpretarse en su favor. Destacan iniciativas como el uso de tecnologías como (…).

Categorías de datos personales afectados por la infracción: la tarjeta SIM no permite la suplantación de la identidad, sino que sirve solamente para la recepción de las claves de confirmación de operaciones bancarias en determinados supuestos. Pero esto no significa que el suplantador pueda operar en nombre del afectado, a menos que se haya saltado las medidas de seguridad de otras entidades, como las de la entidad bancaria.

En este sentido y teniendo en cuenta las circunstancias concurrentes y la nula

culpabilidad de ORANGE, en el caso de que se considere que existe algún tipo de infracción del RGPD, la propuesta de sanción económica debería ser sustituida por la adopción de las medidas correctivas contempladas en el referido artículo 58 RGPD, consistentes en la advertencia o apercibimiento al responsable del tratamiento y la imposición de la obligación de la adopción de medidas para realizar los tratamientos "de una determinada manera y dentro de un plazo especificado".

DÉCIMO TERCERO: Con fecha 27 de abril de 2021, se recibe en esta Agencia escrito del representante de ORANGE por el que formula alegaciones complementarias a las anteriores.

Adjunta la siguiente documentación:

DE CARÁCTER GENERAL:

- Documento 1: (…).
- Documento 2: (…) a seguir ante casos SimSwap.
- Documento 3: Comunicado emitido por Fraude del riesgo de SimSwap.
- Documento 4: Contenido publicado (…) sobre SimSwap.

DE CARÁCTER TÉCNICO

- Documento 5: (…).
- Documento 6: (…).

Estas alegaciones y las anteriores ya fueron contestadas en la Propuesta de Resolución y se reiteran, en parte, en los Fundamentos de Derecho (en adelante, FD) de esta Resolución.

DÉCIMO CUARTO: Transcurrido el plazo de alegaciones concedido en el Acuerdo de iniciación y presentadas alegaciones, con fecha 30 de abril de 2021, por la instructora del procedimiento se acuerda la apertura de un período de prueba en los siguientes términos:

"*Se dan por reproducidas a efectos probatorios las reclamaciones interpuestas por **A.A.A. y B.B.B.**, su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante ORANGE ESPAGNE, S.A.U, y el Informe de actuaciones previas de Inspección que forman parte del expediente E/11418/2019.*

2. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio PS/00022/2021 presentadas por ORANGE ESPAGNE, S.A.U, en fecha 8 de marzo de 2021, a través del Registro General de esta Agencia, y la documentación que a ellas acompaña:

- *Documento 1 (acta)*
- *Documento 2 (denuncias)*

3. También, se dan por reproducidas a efectos probatorios, las alegaciones "complementarias" al acuerdo de inicio PS/00022/2021 presentadas por ORANGE ESPAGNE, S.A.U, en fecha 27 de abril de 2021, a través del Regis-

tro General de esta Agencia, y la documentación que a ellas se acompaña:

- *Documento 1: (…).*
- *Documento 2: (…) a seguir ante casos SimSwap.*
- *Documento 3: Comunicado emitido por Fraude del riesgo de SimSwap.*
- *Documento 4: Contenido publicado (…) sobre SimSwap.*
- *Documento 5: (…).*
- *Documento 6: (…). (…)"*

DÉCIMO QUINTO: Con fecha 30 de septiembre de 2021, la instructora del procedimiento fórmula Propuesta de Resolución, en la que propone que por la directora de la AEPD se sancione a ***ORANGE ESPAGNE, S.A.U.***, con NIF ***A82009812***, 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 800.000'00 (ochocientos mil euros).

Con fecha 4 de octubre de 2021, a través de Carpeta Ciudadana, se notifica la Propuesta de Resolución.

DÉCIMO SEXTO: Con fecha 7 de octubre de 2021, ORANGE solicita la ampliación del plazo para formular alegaciones a la Propuesta de resolución.

DÉCIMO SÉPTIMO: Con fecha 7 de octubre de 2021, la Agencia concede la ampliación instada.

DÉCIMO OCTAVO: Con fecha 26 de octubre de 2021, ORANGE, formula alegaciones a la Propuesta de Resolución en las que se ratifica y da por reproducidas las alegaciones y argumentaciones jurídicas realizadas al Acuerdo de Inicio (antecedentes DUODÉCIMO y DÉCIMO TERCERO) y además, añade otras:

PRIMERA: INFRACCIÓN.

Es de destacar que en los FD se declara inmediatamente la comisión por parte de ORANGE de una infracción del artículo 5.1.f) del RGPD en base a los hechos tenidos por probados por parte de la Agencia. Ello, con anterioridad siquiera a tratar de justificar el motivo. Este proceder, aunque solo sea a afectos formales, resulta jurídicamente poco apropiado y podría considerarse cierta predisposición de la AEPD para sancionarla, con independencia de las alegaciones que pueda hacer en su defensa, habida cuenta que no se ha producido tal infracción.

SEGUNDA: TRATAMIENTO DE DATOS PERSONALES Y RESPONSABLE DEL TRATAMIENTO.

Se requieren una serie de matizaciones en relación con que el proceso de duplicado de una tarjeta SIM supone el tratamiento de datos personales.

La información tratada durante el proceso de duplicado de una tarjeta SIM es la información identificativa del titular de la línea, no la información técnica contenida en dicha tarjeta, con excepción del MSISDN, dado que su contenido no es otro que el propio

número de teléfono (precedido del prefijo nacional).

Estos y no otros son los datos objeto de tratamiento realizado por ORANGE en calidad de responsable.

Toda esta información ya era conocida por los delincuentes con anterioridad a solicitar el duplicado, tras haberlos obtenido previamente de forma ilícita por medio de técnicas de ingeniería social como “phishing” o “spoofing”.

Por lo tanto, no es cierta la afirmación sobre que *“ORANGE, es la responsable de los tratamientos de datos referidos en los antecedentes expuestos”,* ya que en los mismos se hace referencia a otros tratamientos que no son de su responsabilidad.

No consta que se haya tratado por los clientes ninguna información que pueda estar contenida en las tarjetas SIM, como el IMSI, ni mucho menos información sobre el listado telefónico o el de llamadas y mensajes. En cuanto al IMSI, no hay ninguna prueba o indicio de que este dato haya sido tratado con ningún fin.

Tampoco es sostenible la afirmación realizada por la AEPD de que la tarjeta SIM es, en sí misma, un dato personal. La tarjeta puede contener información personal, pero no es un dato y aunque pudiera considerarse esta información como dato personal por hacer potencialmente identificable al titular de la línea, lo cierto es que la posibilidad de identificación por parte de terceros distintos de la operadora requeriría de información adicional que no está disponible, por lo que aun en caso de calificarlos como datos personales, tendrían la consideración de dato seudoanonimizado.

TERCERA: ALEGACIONES ADUCIDAS.

1. ALEGACIÓN PREVIA.- EXISTENCIA DE UN GT SOBRE DUPLICIDAD DE LAS TARJETAS SIM LIDERADO POR LA AEPD.

La quiebra de la confianza legítima no se debe a las afirmaciones que pudo haber realizado la Agencia validando la actuación de ORANGE.

El menoscabo de este principio se debe a que la apertura del expediente sancionador se produce en el marco de una colaboración en el que se constituye un GT específico para abordar una actividad delictiva (“SIM Swapping”), en cuyo seno se integran tanto las operadoras de telecomunicaciones como la banca, así como otras Administraciones y Autoridades implicadas, creado con la intención de proteger a los afectados, y que tiene por objeto analizar de forma conjunta las amenazas y los mecanismos de defensa, con el objetivo de clarificar posibles acciones que ayuden a mitigar los riesgos de suplantación de identidad.

En este sentido, si bien la participación de la AEPD en el GT no implica la validación de la actuación de ORANGE, sí evidencia el reconocimiento de la problemática existente y la dificultad que plantea su prevención: se trata de una problemática generalizada y recurrente, que afecta a múltiples entidades y operadores de telecomunicaciones cuya solución es altamente compleja y, si bien se ha mostrado la voluntad conjunta de acabar con dichos supuestos, erradicarlos, resulta un objetivo complicado, habida cuenta de la capacidad de

los delincuentes para actualizar sus técnicas y desplegar medios cada vez más sofisticados para conseguir sus objetivos .

En este contexto, no parece lógico exigir a las operadoras, y en concreto a ORANGE, el despliegue de una diligencia de eficacia absoluta.

Sin embargo, es dentro de este marco en el que la AEPD decide abrir un expediente, empleando como pretexto la existencia de determinadas noticias en prensa cuando tiene conocimiento de primera mano, por parte de las operadoras, de la existencia y características de estos delitos.

Es más, dicha información se puso en su conocimiento en la confianza de que todas las entidades presentes emplearan la información de buena fe y no para fines distintos de aquéllos para los que se constituía el GT.

La Agencia usa este conocimiento para emplearlo con el objetivo de sancionar tratando de hacerlas responsables por unos delitos de los que son víctimas, el que dista mucho de ser leal y el que quiebra de forma obvia la confianza en una Autoridad que prefiere emprender la vía sancionadora ante entidades que, le consta fehacientemente, están trabajando de forma proactiva para la mejora de la seguridad.

Por otro lado, es obvio que la AEPD está vinculada por el principio de legalidad, pero no es cierto, como pretende, que sea este principio el que la avoca a sancionar. La normativa prevé mecanismos alternativos para situaciones en las que el objetivo debiera ser mejorar la seguridad de las operaciones de tratamiento realizadas.

La función de la AEPD es, conforme al Real Decreto 389/2021, de 1 de junio, por el que se aprueba su Estatuto, la de "*supervisar la aplicación de la normativa vigente en materia de protección de datos personales con el fin de proteger los derechos y libertades de las personas físicas*". Para dicho objetivo, sus facultades no se limitan a la actividad sancionadora, sino que el artículo 58 del RGPD dispone de alternativas correctivas, tales como la advertencia, el apercibimiento o, incluso, ordenar cuando proceda que las operaciones de tratamiento se realicen de una determinada manera y dentro de un plazo especificado.

En este sentido, como la propia AEPD recuerda, las sanciones tienen una finalidad disuasoria y es más que evidente que, no necesitan el acicate de una sanción para proteger los datos de sus clientes.

2. ALEGACIÓN PRIMERA.- INCORRECCIÓN Y FALTA DE EXACTITUD EN LAS APRECIACIONES SOBRE EL FRAUDE DE DUPLICADO.

La AEPD introduce una exposición teórica para tratar de justificar que, como consecuencia del acceso al duplicado de la tarjeta SIM, se produjo un acceso a datos personales contenidos en la propia tarjeta.

En primer lugar, ha de aclarase que la SIM no permite el acceso al IMEI.

En lo que se refiere al IMSI, no hay ninguna prueba o indicio de que este dato

haya sido tratado por los delincuentes con ningún fin, por lo que, no se ha acreditado que su confidencialidad haya sido afectada.

Adicionalmente, tampoco se ha acreditado que se accediera a ninguna otra información personal custodiada por ORANGE distinta de la que aportan los propios delincuentes obtenida mediante técnicas de ingeniería social como "spoofing" y "phishing", por lo que, ORANGE no ha permitido el acceso por terceros no autorizados a información personal a la que éstos no tuvieran acceso de forma previa y, consecuentemente, no ha habido quiebra de la confidencialidad.

La AEPD entremezcla en sus consideraciones el concepto de acceso a datos personales como consecuencia de la duplicación de la tarjeta SIM con la realización de las operaciones bancarias.

Cualquier responsabilidad derivada de la duplicación de las tarjetas, se restringiría, desde el punto de vista de la protección de datos, al tratamiento de información relacionada con los servicios que presta (consumos asociados al contrato, acceso a área privada, contrataciones, etc.) y sobre la que no existe constancia alguna que se haya producido.

Sin embargo, la AEPD trata de hacer responsable y sancionar a ORANGE por las consecuencias de las operaciones realizadas por las entidades bancarias. Confunde las obligaciones de diligencia en el tratamiento de datos personales con una supuesta obligación de dotar de seguridad las operaciones bancarias en relación con la identidad de los clientes de estas terceras entidades.

Es decir, traslada la responsabilidad en la identificación por parte de las entidades bancarias hacia las operadoras de telecomunicaciones.

Las entidades bancarias son las únicas responsables de la seguridad de sus operaciones. Así lo confirma además la Autoridad Bancaria Europea (EBA), que en su "*Opinión sobre la implementación de métodos de autenticación reforzada*", en su apartado relativo a quién decide sobre los medios a emplear para dicha autenticación (puntos 37 y 38), dictamina que las credenciales de seguridad utilizadas para realizar la autenticación segura de los usuarios de los servicios de pago son responsabilidad de la entidad gestora de servicios de cuenta (los bancos).

Que los bancos se decanten habitualmente por el sistema de confirmación mediante el envío de un SMS es una decisión de su exclusiva responsabilidad.

Es un método muy extendido y no es especialmente seguro. Remite a la Digital Identity Guidelines: Authentication and Lifecycle Management, del "National Institute of Standards Department", que dictamina que el SMS no se debería utilizar en la autenticación de dos factores, por la cantidad de riesgos de seguridad a las que está sometida en la entrega de un SMS.

Por su parte, la Autoridad Bancaria Europea (EBA), en una de sus respuestas a las preguntas planteadas desde el sector (Qualification of SMS OTP as an

authentication factor | European Banking Authority (europa.eu)) si bien contempla el SMS como factor de confirmación admisible, recuerda que el uso de SMS ordinarios no es factible para la confirmación de operaciones bancarias, por no ser suficientemente seguros conforme a los estándares de la Directiva PSD2.

Adicionalmente, señala, que este tipo de informaciones son de dominio público y remite a tres enlaces.

Por este motivo, el hecho de que el modus operandi para la realización fraudulenta de operaciones bancarias pueda realizarse mediante un SIM SWAP no puede considerarse en modo alguno una admisión de responsabilidad sobre la seguridad de estas operaciones.

De hecho, la diligencia de las operadoras está obligando a los delincuentes a buscar métodos alternativos para obtener el contenido de los SMS. Remite a noticias e información difundida por la Policía Nacional a través de redes sociales.

Reitera que, la responsabilidad de las operadoras no puede abarcar las operaciones bancarias que los delincuentes puedan realizar como consecuencia de que las medidas de seguridad implementadas por las entidades bancarias sean inadecuadas. No puede hacerse cargo de la seguridad de la información de terceras entidades por el mero hecho de que usen servicios de telecomunicaciones.

Aduce que la Agencia exige una responsabilidad objetiva, en la que a partir de un resultado se deduce una culpa, sin que medie ningún tipo de valoración sobre la diligencia desplegada, interpretación proscrita por el Derecho español.

3. ALEGACIÓN SEGUNDA.- GENERALIZACIÓN NO FUNDADA DE CONSECUENCIAS NEGATIVAS ASOCIADAS A LA EMISIÓN DEL DUPLICADO.

La AEPD no ha aportado ningún hecho o fundamento que sostenga su interpretación.

Admite que para la ejecución de operaciones bancarias el delincuente necesita, además del duplicado de la SIM, acceder adicionalmente a la información personal que obtiene de forma ilícita de la entidad bancaria o del usuario, por lo que no son una consecuencia de la obtención del duplicado.

Y en lo que se refiere a las modalidades delictivas que pretenden “otras finalidades”, las argumentaciones utilizadas para justificar la presunta responsabilidad de ORANGE son meras elucubraciones, que se refieren a riesgos potenciales, que ni se han materializado ni son objeto del presente procedimiento y, desde un punto de vista técnico, distan mucho de ser correctas.

Pretender que el acceso a una tarjeta SIM permite por sí solo determinados accesos, implica un desconocimiento interesado del funcionamiento de los mecanismos de seguridad asociados a la mayor parte, por no decir la totalidad, de

los servicios a los que se hace referencia.

La posibilidad de acceder a las cuentas de un usuario requiere de información adicional no disponible en la tarjeta SIM. Las afirmaciones sobre la facilidad de su obtención carecen de todo fundamento y, lo que es más importante, no se ha materializado ni es objeto del presente procedimiento ninguno de los riesgos a los que la AEPD hace referencia, por lo que su inclusión en este fundamento es totalmente improcedente.

La AEPD hace referencia a 20 casos de duplicados de tarjetas SIM cuando solo forman parte de este expediente las denuncias relacionadas con dos de ellos. Tratar de engrosar este número haciendo referencia a situaciones cuyas circunstancias no constan ni son objeto del presente procedimiento no es procedente y supone un aprovechamiento inadecuado de información que fue facilitada por ORANGE en el marco de una solicitud dirigida por la AEPD y sobre la que no ha sido evidenciado ningún incumplimiento relacionado con el tratamiento de datos personales.

En relación con las dos reclamaciones que sí son objeto de este procedimiento, se deben a una inadecuada aplicación de los protocolos establecidos, que según la estadística son adecuados y eficientes y sólo de manera absolutamente residual han podido ser superados por los delincuentes en su objetivo de obtener un duplicado de tarjeta SIM de forma ilícita.

Ha de tenerse en cuenta que las circunstancias en las que se producen estas suplantaciones no son irrelevantes.

En el supuesto de la parte reclamante dos, la solicitud del duplicado se acompaña de documentos con apariencia de autenticidad destinados a engañar al empleado de la tienda, a quien además se le ofrece un relato creíble en el que se le informa de que la documentación original había sido sustraída, junto con su cartera. Al tratarse de una copia del DNI, no es factible procesarlo con el software de verificación Mitek, ya que el mismo analiza características físicas y de seguridad que sólo están presentes en el original del documento.

En estas circunstancias, el empleado opta por ayudar a la persona, supuestamente víctima de un robo, cuyas circunstancias podrían agravarse precisamente por la imposibilidad de ponerse en contacto y realizar las gestiones pertinentes para evitar males mayores.

En definitiva, el dependiente optó, incumpliendo el protocolo establecido por ORANGE, por no requerir el documento acreditativo de cita para renovación del DNI o el recibo bancario acreditativo del cobro de la última factura.

Por tanto, aunque es cierto que existe un incumplimiento del protocolo (que ha sido objeto de la correspondiente sanción), el mismo es inducido por el delincuente, que generó una situación en la que consiguió aprovecharse de la buena fe del dependiente, al creerlo víctima de un delito, empleando para ello un sofisticado y elaborado plan preconcebido para este fin.

Igualmente, en el supuesto de la primera denuncia, el gestor incumple el protocolo de seguridad para la verificación de los datos, y esto posibilita que pueda llevar a cabo la solicitud de la tarjeta sin seguir todos los controles establecidos.

Sin embargo, esto no hace que las medidas no sean adecuadas, ya que han demostrado su efectividad en prácticamente la totalidad de los casos. En este sentido, que el protocolo sea susceptible de mejora, es una afirmación que ha de ser puesta en contexto, ya que su eficiencia estadística indica que han sido apropiados en un (…) % de los casos.

En cuanto a la mejora de los controles de cumplimiento de los protocolos, si bien son deseables, no pueden obviar la presencia del factor humano.

ORANGE ha dado instrucciones e información adecuada a todos los implicados pero no es factible anular la posibilidad de que las personas realicen acciones en contra de las indicaciones recibidas.

Ante estos riesgos, solo cabe la formación y concienciación de los implicados y la exigencia de responsabilidades en caso de incumplimiento, tal y como ha hecho ORANGE, salvo que la AEPD sugiera que la contratación de empleados con acceso a datos personales sea un riesgo inasumible y todos ellos deban ser sustituidos por procesos automatizados.

4. ALEGACIÓN TERCERA. – IDONEIDAD Y CUMPLIMIENTO DE LAS MEDIDAS PREVENTIVAS IMPLEMENTADAS.

La AEPD pone en duda los protocolos que ORANGE utiliza. Sin embargo, los argumentos que emplea para realizar esta afirmación son contradictorios.

ORANGE ha realizado un total de aproximadamente (…) cambios de SIM en 2019 sin que se haya producido ninguna incidencia en el (…) de los casos.

Por lo tanto, siguiendo el criterio de efectividad apuntado por la propia AEPD y aunque lo deseable es siempre conseguir la anulación del riesgo, no cabe calificarlos como inapropiados.

Una materialización del riesgo en un porcentaje como el que nos encontramos no puede ser calificado como una falta de diligencia en el despliegue de medidas de seguridad.

Imponer una sanción porque en dos supuestos aislados entre más de 800.000 se haya producido un resultado indeseado supone adoptar un principio de responsabilidad objetiva en el ámbito sancionador, vetado por nuestro Ordenamiento Jurídico, como ha sido reiterado repetidamente por el Tribunal Constitucional.

El artículo 28 de la LRJSP, anuda la responsabilidad a la concurrencia de dolo o culpa, ya no recoge el último inciso del artículo 130 de la Ley 30/1992, es decir, la posibilidad de que se responda *"... aún a título de simple inobservancia*".

El Tribunal Constitucional, desde su Sentencia 76/1990, ha venido advirtiendo sobre la responsabilidad objetiva y, la exigencia en todo caso de que la Administración, a la hora de sancionar, pruebe algún grado de intencionalidad. Exige la concurrencia de culpabilidad en los grados de dolo y culpa o negligencia grave, no siendo suficiente la mera negligencia.

Por lo tanto, la superación por un tercero de las medidas de seguridad no puede determinar por sí sola que las mismas no sean adecuadas o suficientes.

Se remite a los expedientes E/05168/2021, E/00536/2016, E/02237/2020 E/ 02723/2020, E/06963/2020, E/00722/2020, E/09882/2020 y argumentaciones de la Agencia, exponentes de una dualidad de criterios que le causa una evidente indefensión, no sabe con certeza a qué atenerse, ni qué medidas cabe implementar, cuando las mismas son consideradas adecuadas en ciertas ocasiones, y, en otras, constitutivas de una infracción de carácter muy grave.

Asimismo, se remite a los expedientes E/05272/2018, E/07129/2014, E/ 08205/2019, E/5441/2018.

No es entendible que, a pesar del volumen de datos afectados por las brechas aludidas, se aprecie un nivel de diligencia adecuado y, sin embargo, en el presente procedimiento, donde únicamente dos interesados se han visto afectados, no se valore como adecuado el nivel de diligencia mostrado, a través de las medidas de seguridad, detección y corrección, teniendo en cuenta el número de procesos de duplicado de SIM realizados.

Orange también es víctima de un “ataque” dirigido por organizaciones criminales que cuenta con técnicas digitales y de ingeniería social dirigidas exclusivamente a vencer las medidas de seguridad implantadas.

En lo que se refiere a las consideraciones de la AEPD sobre la mayor seguridad de los canales habilitados, cualquier vía es susceptible de ser objeto de intentos de fraude.

ORANGE ha eliminado la posibilidad de (…) (que cuenta con medidas reforzadas de seguridad en la autenticación).

El incumplimiento puntual y en casos absolutamente aislados por parte de un gestor de las instrucciones de verificación de la identidad no implica en absoluto que el protocolo de seguridad dependa de la voluntad del gestor interviniente, sino que supone un incumplimiento de sus obligaciones que, como se ha informado, ha dado lugar a la imposición de penalizaciones.

Así, las medidas apuntadas por la AEPD relativas a “*la inclusión de estas en el sistema de información, (…), incluso con controles en las pantallas del sistema de información (…)*” no garantizan ninguna mejora en el control de estas actividades. Cualquier agente podría aceptar los botones para continuar el proceso pese a no haber llevado a cabo la medida de seguridad concreta.

Las opciones de monitorización total de los empleados, además de no ser pro-

porcionadas conforme a la normativa de protección de datos, tendrían un coste desproporcionado, considerando que debería controlarse exhaustivamente a todos los agentes potencialmente intervinientes en una operación de este tipo (máxime teniendo en cuenta que el control debería llevarse a cabo en tiempo real), cuando la estadística demuestra que las incidencias relacionadas son ínfimas.

Por otro lado, ha quedado acreditado que todos los agentes han recibido la formación necesaria y que la información y la gestión se realiza sin ninguna incidencia en la práctica totalidad de los casos.

Adicionalmente, es posible la verificación de cumplimiento de las obligaciones, ya que la actividad de los usuarios queda registrada.

Todo lo anterior, sin perjuicio de que, en su proceso de mejora continua de la seguridad, ORANGE sigue analizando posibles mejoras en todos sus procesos.

En relación con la información detallada en la “Guía rápida”, tiene fecha de 2017 y se aporta a efectos de verificar las medidas implementadas de manera previa a que tengan lugar los hechos objeto del presente procedimiento y su progresiva mejora, revisión y refuerzo.

Sobre la documentación contractual con las empresas de entrega, hay que señalar que en los dos supuestos que nos conciernen, no interviene ninguna empresa o proveedor de servicios de entrega.

Los certificados que ORANGE ostenta, reconocidos por el Esquema Nacional de Seguridad (ENS), tienen un alcance amplio, que no engloba únicamente los sistemas de información, sino que existen una serie de controles que aplican a toda la organización, en atención a diferentes aspectos, inclusive: protección de datos, seguridad en redes, uso de sistemas de información, formación y concienciación y seguridad en el proceso de recursos humanos.

Estos controles son transversales a toda la organización.

Lejos de querer eludir la responsabilidad, lo que se solicita es, precisamente, que tal responsabilidad se ciña al tratamiento efectivamente realizado, sin extender la responsabilidad correspondiente a otras entidades, como las operaciones y transacciones efectuadas por diferentes entidades bancarias.

Por último, hay que indicar que el carácter de derecho fundamental del derecho a la protección de datos no elimina la necesidad de examinar la diligencia desplegada por ORANGE, ni la consideración del porcentaje ínfimo de incidencias que se han producido en los procesos de duplicado de tarjeta SIM.

5. ALEGACIÓN CUARTA. – ACTUACIÓN DILIGENTE DE ORANGE.

La redacción es totalmente confusa y contradictoria, de forma que cada párrafo parece afirmar lo contrario de lo que dice el anterior, para finalmente acabar

proyectando una indeterminada falta de diligencia como motivo último de la sanción.

La AEPD considera que ha incumplido el artículo 5.1.f), el denominado principio de integridad y confidencialidad.

Recalca las contradicciones de la Agencia e invoca que le provoca total indefensión, por cuanto a pesar de que ha conseguido acreditar en el procedimiento el cumplimiento de su deber de diligencia y ser este reconocido, es objeto de una propuesta de sanción por un motivo indeterminado, ante el cual no puede presentar prueba alguna.

Todo ello trae causa en que la ***AEPD está evaluando la responsabilidad de Orange atendiendo únicamente a un resultado***, constituyendo un supuesto de responsabilidad objetiva, resultándole indiferente la diligencia desplegada en sus medidas preventivas y paliativas.

Motivos por los que las mismas deben ser desechadas:

- La AEPD reconoce que "*El enfoque de riesgos y el modelo flexible al riesgo impuesto por el **RGPD** […] **no impone en ningún caso la infalibilidad de las medidas** (…)*". Sin embargo, pretende sancionar por dos supuestos puntuales entre casi un millón.

- Reprocha que en uno de los supuestos (parte reclamante dos) no se haya verificado el DNI presentado a pesar de que "*asegura disponer de un software específico para contrastar si los documentos identificativos son correctos (Mitek)".* Se trata de una imposibilidad técnica, no un error en el procedimiento de seguridad.

- Indica que "*la conducta de ORANGE se considera que **responde al título de culpa. Como depositaria de datos de carácter personal a gran escala (**…), debe ser especialmente diligente y cuidadosa en su tratamiento. (…) 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*". La culpa tiene que ver con la diligencia desplegada, no con un hecho objetivo como el número de datos tratados.

- "*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*". A pesar de haber reconocido que, *"ORANGE ha actuado diligentemente a la hora de minimizar el impacto a los posibles afectados implantando nuevas medidas de seguridad para evitar la repetición de incidentes similares en un futuro".*

- La AEPD vuelve a introducir un nuevo criterio para la responsabilidad de ORANGE en los supuestos analizados, indicando que ésta "*está directamente relacionada con la generación de consecuencias en terce-*

ros". Traslada a ORANGE la responsabilidad sobre tratamientos sobre los que no tiene ninguna capacidad de control.

- Continua la AEPD indicando que no comparte el hecho de que esos protocolos o procedimientos internos puedan considerarse como adecuados "*en tanto que son susceptibles de mejora. Hay que reforzar los mecanismos de identificación y autenticación con medidas técnicas y organizativas que resulten especialmente apropiadas para evitar suplantaciones*".
  Ese concepto de mejora, abstracto y genérico, permitiría calificar cualquier protocolo como inadecuado, en tanto todo proceso es susceptible de mejora.

- Se incluye determinada jurisprudencia relativa a la culpa, en la que se reconoce que ésta no concurre si se justifica "*que se ha empleado la diligencia que era exigible por quien aduce su inexistencia" o se indica que "no existe negligencia, ni por tanto infracción, "cuando se haya puesto la diligencia necesaria en el cumplimiento de las obligaciones"*

- La responsabilidad de una persona jurídica ha de valorarse en función de la diligencia desplegada como entidad, manifestada a través de los procedimientos e instrucciones aprobados por esta.

  Sin embargo, no se plantea por la AEPD que los riesgos generados por terceros (entidades bancarias) y que son de su responsabilidad, serían mitigables de forma mucho más sencilla si estos adoptasen medidas adecuadas para mejorar la seguridad de las operaciones que realizan.

Motivos por los que ORANGE no debe ser objeto de sanción:

La confidencialidad de los datos tratados en el proceso de la duplicación de la tarjeta SIM se quebró previamente por parte de las entidades bancarias.

ORANGE no tiene control sobre esta operativa ni puede incidir en su habilitación/procedimiento/ejecución.

La sucesión de suposiciones y posibilidades no puede servir, bajo ningún concepto, como justificación, para imponer a ORANGE una infracción sin entrar a valorar, motivadamente, el nivel de diligencia desplegado y los hechos realmente acaecidos. Estas amenazas identificadas por la AEPD recaen fuera del ámbito de actuación de ORANGE.

La AEPD aprecia culpa de la conducta de Orange, si bien, lejos de identificar y relatar la conducta concreta, se limita a referirse al resultado. Este proceder no es conforme a la legalidad vigente, como ha indicado la Audiencia Nacional, entre otras, en la Sentencia de la Sala de lo Contencioso-administrativo, Sección 1ª, de 23 de Diciembre de 2013, Rec. 341/2012:

Ha de recordarse que la referencia a la "*simple inobservancia*" ha sido eliminada por la actual Ley 40/2015, por lo que sería necesaria una falta de diligencia

cualificada.

Invoca la SAN, Sala de lo Contencioso, de 25 de febrero de 2010, nº de Recurso 226/2009".

El mero error humano no puede dar lugar, por sí mismo, a consecuencias sancionadoras.

Ha de remarcarse la similitud del presente supuesto con el recogido en la SAN de 25 de febrero de 2010: se trata de intrusiones cometidas de manera ilegal, por terceros organizados y con altos conocimientos informáticos, dirigidos a una actividad delictiva muy elaborada.

El hecho de que se venga considerando por parte de la AEPD y los Tribunales que en el caso de los ataques técnicos (hacking), dirigidos contra compañías, se considere que su diligencia no abarca tener capacidad para rechazar este tipo de ataques se interpreta de forma contraria en este caso, penalizando a ORANGE porque sus medidas de seguridad puedan depender de la actuación de personas concretas.

No puede exigirse a ORANGE, y tampoco a sus empleados o agentes, la capacidad de identificar de forma infalible los supuestos de fraude, especialmente cuando se ofrece, una "*apariencia de realidad y seriedad suficiente para engañar a personas de mediana perspicacia y diligencia*" (así considerado, entre otras muchas, en la STS 2362/2020).

Aporta copia sellada por la Jefatura de Policía y comunica la posterior aportación de la documentación acreditativa (parte reclamante dos), cuando sea facilitada por las correspondientes Unidades de Información de las Fuerzas y Cuerpos de Seguridad.

ORANGE, dentro de las funciones recogidas en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (en lo sucesivo, LGTEL) y en la Ley 25/2007, de 18 de octubre, participa de forma activa en la colaboración con los agentes facultados en el esclarecimiento de los delitos.

ORANGE debe considerarse como un perjudicado más en este tipo de procedimientos, ya que es la propia entidad la que también sufre un perjuicio y ve "atacados" sus sistemas y activos.

6. ALEGACIÓN QUINTA. – FALTA DE PROPORCIONALIDAD DE LA SANCIÓN PROPUESTA.

A pesar de que la AEPD ha modulado el importe de la sanción impuesta se considera que, habiendo sido diligente en su actuación no procede imposición de sanción alguna.

Para el hipotético caso de que se considerase la existencia de un supuesto incumplimiento, no resulta proporcional.

Conviene incidir en que no es necesaria ninguna acción disuasoria, en tanto el supuesto objeto del presente procedimiento se ha llevado a cabo en contra de todo elemento volitivo de ORANGE.

ORANGE no ha obtenido beneficio, sino que le ha supuesto un perjuicio. Por lo que, en lo que se refiere a la necesidad del efecto disuasorio, la mera comisión del delito es un perjuicio para ORANGE.

Adicionalmente, participa de manera voluntaria en el GT.

CUARTA. - PRINCIPIOS RELATIVOS AL TRATAMIENTO.

ORANGE comparte con la Agencia la relevancia de las medidas de seguridad en aras de garantizar el derecho fundamental a la protección de datos, sin embargo, ha de hacerse una serie de matizaciones:

- Ha sido reconocido el perjuicio que han sufrido ambos reclamantes: ambos recibieron una compensación por parte de ORANGE.

- No pueden considerarse circunstancias particulares de las reclamaciones presentadas ni tampoco supuestos dentro del objeto del presente procedimiento, las suposiciones y posibilidades que elucubra la AEPD: acceso a aplicaciones, uso de redes sociales, etc.

- En nada pueden justificar la Propuesta de Resolución de la Agencia.

- ORANGE no tiene control de tales procedimientos ni influencia alguna en las medidas de seguridad que se utilizan por las entidades bancarias.

- Si bien ORANGE, como responsable del tratamiento tiene la obligación de determinar sus medidas de seguridad, es el encargado del tratamiento el que asumirá la responsabilidad, configurándose como responsable, cuando no siga las instrucciones del primero e incumpla los fines y medios del tratamiento en cuestión, como así lo estipula el artículo 28.10 del RGPD.

- Reiterar, que en dos ocasiones se haya podido suplantar la identidad de los reclamantes en dos procedimientos de duplicado de tarjeta SIM de un total de aproximadamente (…) procedimientos de duplicado, mediante engaño suficiente, no puede determinar automáticamente la comisión de infracción y ausencia de diligencia por parte de ORANGE.

- ORANGE no “facilita duplicados de la tarjeta SIM a terceras personas”. Cuando el tercero obtuvo el duplicado de la tarjeta SIM fue porque engañó al agente.

- No estamos ante la presencia de un dato personal especialmente relevante. Los códigos que contiene necesitan asociarse con otros datos personales, para permitir la identificación del titular. No consta así mismo el acceso por los suplantadores de identidad a datos personales distintos de aquellos que ya conocían de manera previa a obtener fraudulentamente el duplicado de tarjeta SIM.

- Con relación a la STC 292/200 no se pone en duda la definición y consideración

del derecho a la protección de datos como derecho fundamental. Lo que no es aceptable es la intención de la Agencia de imputar dicha infracción, pese a haber llevado a cabo un despliegue de medidas de seguridad apropiado y adecuado, en los términos del artículo 32 del RGPD.

QUINTA. - SEGURIDAD DEL TRATAMIENTO.

La calificación jurídica que hace la Agencia de la infracción imputada a ORANGE no recoge el quebrantamiento del artículo 32 del RGPD.

SEXTA. - CONDICIONES GENERALES PARA LA IMPOSICIÓN DE LA MULTA ADMINISTRATIVA.

El tratamiento realizado no vulnera la normativa de protección de datos, ya que, ORANGE ha desplegado un nivel de diligencia adecuado, en la imposición de las medidas técnicas y organizativas necesarias para evitar la comisión de fraudes en las solicitudes de duplicados de tarjetas SIM.

La sanción propuesta es en todo caso desproporcionada, atendiendo a las circunstancias y contenido de las supuestas infracciones.

Los considerandos 11 y 13 del RGPD, que hacen referencia a garantizar la protección efectiva de los datos personales y hacerlo de manera coherente, apuntan que dicho objetivo también depende de que "*las infracciones se castiguen con sanciones equivalentes*".

- Agravantes:

1. Naturaleza y gravedad de la infracción:

La pérdida de control y disposición de los datos personales no se inicia cuando ORANGE realiza el duplicado, sino que tiene lugar antes, en el momento en el que los individuos consiguen acceder a datos personales de los reclamantes.

La referencia al rol del teléfono móvil no hace sino certificar el traslado de responsabilidad hacia ORANGE, sin tener en cuenta que la limitación de estos riesgos corresponde a los obligados por dicha normativa.

No se evalúa en este apartado, la naturaleza y gravedad de la infracción imputada, sino que se vuelve a analizar la actividad posterior realizada por los individuos que suplantan la identidad.

Categorizar la naturaleza y gravedad del tratamiento realizado por ORANGE, exige evaluar las medidas de seguridad establecidas en los procedimientos de duplicado de tarjeta SIM.

Reiterar, que los terceros no han tenido acceso en ninguno de los dos supuestos a los teléfonos móviles de los reclamantes, y, consiguientemente, tampoco a la información que estos pudiesen almacenar, que es diferente, en cualquier caso, de la información que pueda almacenar una tarjeta SIM.

2. Duración de la infracción:

El presente procedimiento versa sobre las reclamaciones de dos reclamantes.

En el caso de la parte reclamante uno, los hechos se suceden desde la tarde del 22 de julio de 2019, hasta la mañana del 24 de julio.

En el caso de la parte reclamante dos, la duración es de apenas unas horas en el día 8 de enero de 2020, desde que se realiza fraudulentamente el duplicado hasta que el reclamante es consciente y ORANGE gestiona la suplantación de identidad.

El tiempo durante el cual los reclamantes no tienen acceso a su tarjeta SIM es inferior a 48 horas en un caso e inferior a 8 horas en el otro.

Por ello, no puede la Agencia considerar la duración de las supuestas infracciones un elemento agravante, en tanto las mismas han sido puntuales, localizadas, identificadas y gestionadas en mínimos períodos de tiempo.

Carece de ningún sentido la referencia a los (…) casos que, junto a ORANGE VIRTUAL ESPAÑA, S.A.U (SIMYO), se contabilizaron durante el año 2019. No se ha justificado la relación de ninguno de los demás casos con la infracción imputada ni ello serviría para considerar el ámbito temporal de las mismas.

3. Número de interesados afectados:

El presente procedimiento se circunscribe a dos casos.

No puede incluirse, como elemento agravante, la existencia de más casos de procesos de duplicados de tarjetas SIM con incidencias, en tanto los hechos y supuestos concretos no han sido traídos a colación al presente procedimiento: no se han realizado reclamaciones por los titulares de los datos, ni se han analizados los hechos ni las responsabilidades derivadas de los mismos.

Por ello, esta parte considera que, lejos de considerarse un agravante, el ínfimo número de interesados debería evaluarse como elemento atenuante.

4. Nivel de los daños y perjuicios sufridos:

ORANGE no es responsable de las políticas de identificación y verificación de clientes establecidas por las entidades bancarias.

Tampoco se hubiesen podido producir las operaciones bancarias si la entidad financiera utilizase otro sistema de seguridad en la verificación, por ejemplo, el uso de datos biométricos o la identificación del terminal móvil desde el que se accede a la aplicación del banco, como ya se lleva a cabo por algunas entidades financieras.

La Agencia no entra a valorar el nivel de los daños y perjuicios, en tanto se limita a indicar que éstos “*se multiplican*” cuando se entrega el duplicado de la

tarjeta SIM a persona distinta al titular, sin explicar cuál es la relación entre esta afirmación y los hechos objeto de análisis en este procedimiento.

Con relación a la procedencia que indica de realizar una evaluación de impacto, no puede pretender que, en una evaluación de impacto llevada a cabo por ORANGE sobre emisión de duplicados de tarjeta SIM, se evalúe las posibilidades de comisión de fraude en la realización de operaciones bancarias a través de aplicaciones y banca electrónica de terceros.

Por todo lo anterior, no puede afirmarse que del proceso de duplicado deriven directamente, ni necesariamente, las operaciones bancarias fraudulentas, ya que los datos que los suplantadores precisan para realizarlas abarcan muchas más informaciones y operaciones que la duplicación de la tarjeta SIM.

5. Intencionalidad o negligencia en la infracción:

La Agencia exige a Orange una obligación de resultado absoluta, en tanto el nivel de diligencia no se está evaluando en atención a las medidas y procedimientos establecidos, sino que atiende únicamente al resulta obtenido.

La AEPD introduce así la responsabilidad objetiva rechazada por nuestro Tribunal Constitucional, como ya hemos indicado, en la jurisprudencia que emana de la STC 76/1990 de 26 de abril, en tanto no puede exigirse en el ámbito sancionador de la Administración.

La Agencia contradice igualmente la jurisprudencia (Sentencia del TS de 23 de enero de 1998): de no haber intencionalidad o elemento volitivo de ORANGE, como se está reconociendo, y habiendo desplegado éstas medidas de seguridad, previas y posteriores a los casos que nos ocupan, así como procedimientos de mejora; no cabe imputarle a ésta nivel alguno de negligencia, en tanto, dicha calificación, exige que la persona jurídica muestre un mínimo grado de intencionalidad, manifestado a través de la falta de diligencia.

Es por ello, que no puede considerarse a ésta como negligente, en tanto se han establecido procedimientos apropiados, los cuales han sido revisados y reforzados progresivamente.

6. Grado de responsabilidad del responsable:

En los dos supuestos que nos ocupan, los agentes incumplieron la política de seguridad y las medidas concretas que ésta imponía.

Además, cuenta con medidas preventivas, técnicas y organizativas, medidas paliativas y medidas coercitivas, por las que se sanciona a aquellos que no cumplan con las obligaciones impuestas.

Así, no cabe sino interpretar, que lejos de suponer este criterio un agravante, debería interpretarse en favor de ORANGE.

7. Categorías de datos personales afectados por la infracción:

Solo ha podido determinarse el tratamiento de datos personales identificativos básicos, cuyo conocimiento por los delincuentes era previo a la duplicación de la tarjeta.

Como se ha tenido oportunidad de explicar, la teoría de que la tarjeta SIM es un dato personal no tiene sustento alguno, sino un contenedor de datos y códigos que solo permiten la identificación del usuario si se dispone de información adicional.

El envío de SMS no tiene nada que ver con la tipología de datos tratados analizado en este punto.

Por lo tanto, el tipo de datos objeto de tratamiento ha de ser considerado como un atenuante.

- Atenuantes:

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

La Propuesta de Resolución recoge como atenuantes las medidas preventivas y coercitivas, pero no hace mención alguna a las medidas paliativas y compensaciones que ha implementado en los dos supuestos que nos ocupan, y que deberán ser considerados como atenuantes.

2. Los beneficios obtenidos como consecuencia de la comisión de la infracción.

Pese a que en el Acuerdo de Inicio la Agencia valora la falta de beneficio de ORANGE, debemos insistir en que no sólo se produce la ausencia de beneficio, sino que ha supuesto un perjuicio, ha tenido que llevar a cabo investigaciones internas, realizar compensaciones a los reclamantes y reevaluar procedimientos y protocolos.

ORANGE sufre también la suplantación de identidad por parte de los terceros no autorizados, en tanto engañan a los agentes y generan un perjuicio en su servicio.

Para concluir, considera plenamente aplicable al presente caso lo dispuesto en el artículo 76.3 de la LOPDGDD relativo a sanciones y medidas correctivas: *"será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679"* el cual indica que las multas administrativas se impondrán "*a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h)*".

Teniendo en cuenta las circunstancias concurrentes y la nula intencionalidad o culpa de ORANGE, en el caso de que se considere que existe algún tipo de infracción del RGPD, la propuesta de sanción económica debería ser sustituida por la adopción de las medidas correctivas contempladas en el referido artículo

58, consistentes en la advertencia o apercibimiento al responsable del tratamiento y la imposición de la obligación de adopción de medidas para realizar los tratamientos "*de una determinada manera y dentro de un plazo especificado*".

Sobre este particular, ORANGE entiende que la multa inicialmente estimada puede ser perfectamente sustituida por la obligatoria adopción de medidas correctoras.

CONCLUSIONES

1º.- Aunque pudiera considerarse la información almacenada en la tarjeta SIM -nunca la propia tarjeta en sí- como dato personal, no se ha acreditado que los mismos hayan sido objeto de tratamiento durante el tiempo en que los delincuentes tuvieron operativas las tarjetas SIM duplicadas.

2º.- Los delincuentes no obtuvieron de ORANGE ningún dato personal adicional a los que ya tenían con anterioridad a dirigirse a ORANGE, obtenidos de entidades bancarias y que son empleados para suplantar la identidad de los afectados, por lo que el tratamiento realizado no supone una infracción de la confidencialidad de los datos personales.

3º.- La responsabilidad de las teleoperadoras por supuestos de suplantación de identidad en la solicitud de copias de tarjetas SIM no puede abarcar las operaciones bancarias se puedan realizar como consecuencia de que las medidas de seguridad de las entidades bancarias sean inadecuadas. No puede hacerse cargo de la seguridad de la información de terceras entidades por el mero hecho de que usen servicios de telecomunicaciones.

4º.- Ha quedado acreditado que los dos supuestos se deben a una inadecuada aplicación de los protocolos establecidos por ORANGE que, tal y como evidencia la estadística, son adecuados y eficientes y sólo de manera absolutamente residual han podido ser superados por los delincuentes.

5º.- La superación por un tercero de las medidas de seguridad no puede determinar automáticamente que las mismas sean inadecuadas ya que supone aplicar un principio de responsabilidad objetiva en el ámbito sancionador, vetado por nuestro Ordenamiento Jurídico.

6º.- La AEPD ha declarado acreditados ciertos hechos (que dispone de una política de seguridad en la que se establece el modo de actuar para la expedición de los duplicados; que no puede colegirse una infracción del artículo 32, ni tampoco del artículo 5.2 y 25 del RGPD; que existen protocolos para prevenir las suplantaciones de identidad; que se han trasladado a los implicados en la tramitación; que se han introducido mejoras tras conocer ciertas vulnerabilidades; que existen penalizaciones por su incumplimiento o que ha actuado diligentemente a la hora de minimizar el impacto implantando nuevas medidas de seguridad).

Por todo lo anterior, no procede declarar la existencia de una infracción del artículo 5.1.f) del RGPD ni, en consecuencia, la imposición de sanción alguna, en tanto se ha acreditado un nivel de diligencia adecuado y no se ha acreditado ninguna quiebra del deber de confidencialidad.

(El subrayado, la cursiva y negrita es de ORANGE).

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, quedan acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: ORANGE es la responsable de los tratamientos de datos referidos en la presente 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 con las finalidades señaladas en su Política de Privacidad, entre otras: la prestación de los servicios de telecomunicaciones, el mantenimiento y la gestión de la relación a efectos de dar cumplimiento a lo dispuesto en el contrato firmado entre las partes (Gestionar el registro del Usuario y permitir el acceso a las actividades y herramientas disponibles a través del Sitio Web www.orage.es; llevar a cabo el alta de Usuario, así como el mantenimiento y la gestión de la relación contractual con ORANGE; gestionar, tramitar y dar respuesta a peticiones, solicitudes, incidencias o consultas del Usuario, cuando éste facilite sus datos a través de los formularios habilitados al efecto en el Sitio Web www.orange.es, etc.)

SEGUNDO: ORANGE presta sus servicios de telefonía móvil a través de tres marcas comerciales que son: ORANGE, AMENA y JAZZTEL. Cada una de ellas dispone de distintas operativas de funcionamiento.

TERCERO: Con fecha 6 de agosto de 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante uno (expediente con núm. de referencia ***E/08994/2019***), dirigida -entre otros- contra ORANGE, tras expedirse en fecha 22 de julio de 2019, un duplicado de la tarjeta SIM de la línea ******TELÉFONO.1***, a favor de una tercera persona distinta a la titular de la línea -la parte reclamante uno-.

Estos hechos fueron denunciados ante la Guardia Civil de Baiona (Pontevedra), en fecha 24 de julio de 2019, con número de atestado ******ATESTADO.1*** en la que la parte reclamante uno manifestó lo siguiente:

'Que la dicente en el día de hoy, sobre las 09:00 horas comprobó que su teléfono móvil XIAOMI Mi A1-con número ******TELÉFONO.1*** *de la compañía ORANGE, con número de IMEI's* ******IMEI.1*** *y* ******IMEI.2****, dejó de funcionar.*

Se dirigió a la tienda de ORANGE para preguntar que habla sucedido, comprobando en la tienda que la tarjeta SIM ******SIM.1*** *que tenía instalada en el teléfono móvil no le funcionaba, por lo que le realizaron una nueva tarjeta SIM* ******SIM.2****.*

La empleada de la tienda se percató que la tarjeta SIM que tenía instalada en su teléfono no correspondía con la que figuraba en la base de datos de ORANGE. Que la tarjeta SIM que constaba en la base de datos de ORANGE es ******SIM.3****.*

Que en el momento que la dicente instaló la nueva tarjeta SIM ******SIM.2*** *recibió dos mensajes de texto (SMS) de SANTEVIÓS, con un código SMS para transferencias de 5000 euros y un SMS de INFOSNET con un código SMS para transferencia de 5000 euros.*

Que la manifestante, una vez le entregan el formulario de solicitud de cambios observa que el correo electrónico ******CUENTA DE CORREO.1****no corresponde con el correo facilitado a ORANGE. Que el correo que les facilitó es* ******CUENTA DE CORREO.2****(…)*

Que la manifestante se pone en contacto telefónico con ORANGE a través del 1470 y le informan que a ORANGE se realizaron dos llamadas, una para cambiar el correo electrónico y otra para solicitar el duplicado de la tarjeta SIM, llamadas que se realizaron el 22/07/20219, una a las 14:00 horas y la otra a las 19:15 horas constando el número de esta última ******NÚMERO.1****.*

Que desde la tienda de ORANGE entran en el perfil de usuario y se observa que figuran cinco llamadas al número de teléfono ******TELÉFONO.2*** *que corresponde a la banca online del Santander (…)*

Que la manifestante examina los movimientos de sus tres cuentas bancarias y de sus dos tarjetas y observa:

Que autor/es desconocidos habían realizado un traspaso de la tarjeta VISA ******VISA.1*** *por las cantidades de 700 y 500 euros a la cuenta* ******CUENTA.1*** *(Banco Popular) siendo la cuenta espejo de la cuenta* ******CUENTA.2*** *(B. Santander).*

La manifestante se percata que el 22 de julio de 2019 autores desconocidos dieron de alta una nueva tarjeta de crédito VISA con numeración ******VISA.2.***

Que autor/es desconocidos realizan un traspaso de la tarjeta ******VISA.2*** *de 5000 euros a la cuenta bancaria numeración* ******CUENTA.3*** *(Banco Popular) siendo la cuenta espejo de la cuenta* ******CUENTA.4*** *(B. Santander).*

Que autor/es desconocidos realizan tres transferencias de su cuenta bancaria ******CUENTA.5,*** *(…) fueron de 1000 euros cada una, enviadas a las cuentas* ******CUENTA.6*** *(EVO BANCO);* ******CUENTA.7*** *(EVO BANCO) y* ******CUENTA.8*** *(OPEN BANK) que por cada una de estas transferencias le cobran la cantidad de 6 euros.*

Que autor/es desconocidos realizan una transferencia de la cuenta ******CUENTA.3****(…) a la cuenta* ******CUENTA.8*** *(OPEN BANK) por la cantidad de 250 euros constando un cargo de 6 euros en concepto de gastos.*

Que autor/es desconocidos de la cuenta con numeración ******CUENTA.1*** *(…) realizaron tres transferencias, siendo la primera por la cantidad de 5000 euros a la*

*cuenta *****CUENTA.6** (EVO BANCO). Una segunda transferencia de 250 euros a la cuenta *****CUENTA.8** (OPEN BANK), una tercera transferencia de 250 euros a la cuenta *****CUENTA.8** (OPEN BANK). (…)*

Consta una "Solicitud de cambios en el servicio Pospago de comunicaciones móviles" con fecha de contacto de 23 de julio de 2019, en la que aparece en los "Datos del Cliente", el email de la persona suplantadora "******CUENTA DE CORREO.1"*** y en los "Datos de los Servicios contratados" el nuevo número de tarjeta SIM asignado ******SIM.2***.

Consta listado de llamadas efectuadas desde dicha SIM a la línea telefónica del Santander ***TELÉFONO.2, y un resumen de las transferencias e ingresos realizados sin su consentimiento.

C.C.C.: ***(…)***		
Concepto	Fecha	Importe
Transferencia inmediata a favor de Juan	22/07/2019	1.006,00
Transferencia inmediata a favor de Juan	23/07/2019	1.006,00
Transferencia inmediata a favor de Juan	23/07/2019	1.006,00

C.C.C.: ***(…)***		
Concepto	Fecha	Importe
Ingreso en cuenta desde tarjetas	23/07/2019	5.000,00
Transferencia inmediata a favor de Lil	23/07/2019	256,00

C.C.C.: ***(…)***		
Concepto	Fecha	Importe
Transferencia inmediata a favor de Juan	22/07/2019	5.006,00
Transferencia inmediata a favor de Hugo	23/07/2019	256,00
Transferencia inmediata a favor de Hugo	23/07/2019	256,00
Ingreso en cuenta desde tarjetas	23/07/2019	700,00
Ingreso en cuenta desde tarjetas	23/07/2019	500,00

En relación con esta reclamación, ORANGE, confirmó a esta Agencia que, la tarjeta SIM fue adquirida (…) y se procedió a su activación a través de (…) el 22 de julio de 2019 a las 18:52 horas. La activación, afirma, se realiza (…) incumpliendo las directrices establecidas por ORANGE para verificar la identidad del cliente.

CUARTO: Con fecha 5 de junio de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante dos (expediente con núm. de referencia ***E/ 05031/2020***), dirigida contra ORANGE, tras expedirse en fecha 8 de enero de 2020, un duplicado de la tarjeta SIM de la línea ******TELÉFONO.3***, a favor de una tercera persona distinta a la titular de la línea -la parte reclamante dos-.

Los hechos fueron denunciados ante la Dirección General de la Policía Nacional en las dependencias de San Andrés (Murcia), en fecha 9 de enero de 2020, con número de atestado ***XXX/YY***, con el siguiente tenor:

"Que en el día de la fecha la mujer del denunciante recibe un SMS el cual le informa de que a través del número del dicente ha solicitado un duplicado de tarje-

ta de su número de teléfono.

Que el dicente manifiesta que no ha autorizado tal operación con su número por lo que se pone en contacto con su compañía de teléfono, ORANGE, confirmándole este la tramitación del duplicado, alegando que puede haber sido un error por parte de ORANGE.

Que el dicente en ese momento se percata de que no dispone de cobertura en su teléfono móvil.

Que decide comprobar sus cuentas bancarias percatándose de que le han sustraído 300 euros desde un cajero automático sito en el lugar del hecho sin autorización. (…)"

En relación con esta reclamación, ORANGE, confirmó a esta Agencia que, el duplicado de tarjeta SIM fue realizado en 08/01/2020 desde (…) y se obtuvo mediante la aportación de documentación manipulada entre la que se encontraba (…). Fue detectado el mismo día de su activación, 08/01/2020, al asociarse la activación de la línea ******TELÉFONO.3*** al IMEI ******IMEI.3***, el cual constaba incluido en (…) empleada por el Grupo de Análisis de Riesgos.

Consta aportado (…) con el que la persona suplantadora se identificó como la parte reclamante dos, y se observa (…) en distintos campos:

- (…).

- (…).

Se verifica que faltan algunos documentos a entregar según el protocolo de ORANGE:

- (…).

- (…).

QUINTO: Las dos reclamaciones presentadas afectan a clientes de la marca ORANGE.

SEXTO: ORANGE cuenta para esta marca con un modelo de gestión de solicitud y activación de duplicados de tarjetas SIM que presta a través (…).

(…):

- (…)
  - .- (…)
  - .- (…)
- (…)

(…):

- (…)

- (…)

- (…)

(…):

- (…)

- (…)

SÉPTIMO: ORANGE dispone de un sistema (…)

(…) (…)	(…) (…)
(…)	(…)
(…)	(…)
(…)	(…)

(…):

- *(…).*

- *(…).*

- *(…):*

  - *(…).*

  - *(…).*

- *(…).*

- *(…).*

(…):

- *(…):*

  - *(…).*
  - *(…).*
  - *(…).*
  - *(…).*
  - *(…).*
  - *(…).*
  - *(…).*

- *(…):*

- *o (…).*
- *o (…).*
- *o (…).*
- *o (…).*

- *(…)*

(…):

- *o (…).*
- *o (…).*
- *o (…).*

(…).

OCTAVO: (…):

- o *(…).*
- *(…).*

Como (…) informa los siguientes:

- *(…).*
- *(…).*
- *(…).*
- *(…).*

En lo relativo a la (…) informa:

- *(…).*

NOVENO: (…), ORANGE recoge la siguiente información:

(…).

(…).

En el punto 1 denominado (…) constan las siguientes especificaciones:

- *(…).*
- *(…).*
- *(…):*
  - *(…):*
    - *(…)*
    - *(…)*
    - *(…)*

- *(…):*

  - *(…)*

  - *(…)*

(…)

- *(…)*

- *(…).*

- *(…).*

- *(…).*

- *(…)*

- *(…).*

- *(…).*

- *(…).*

En cuanto a los (…) ORANGE recoge las siguientes especificaciones:

- *(…)*

- *(…).*

DÉCIMO: (…):

(…).

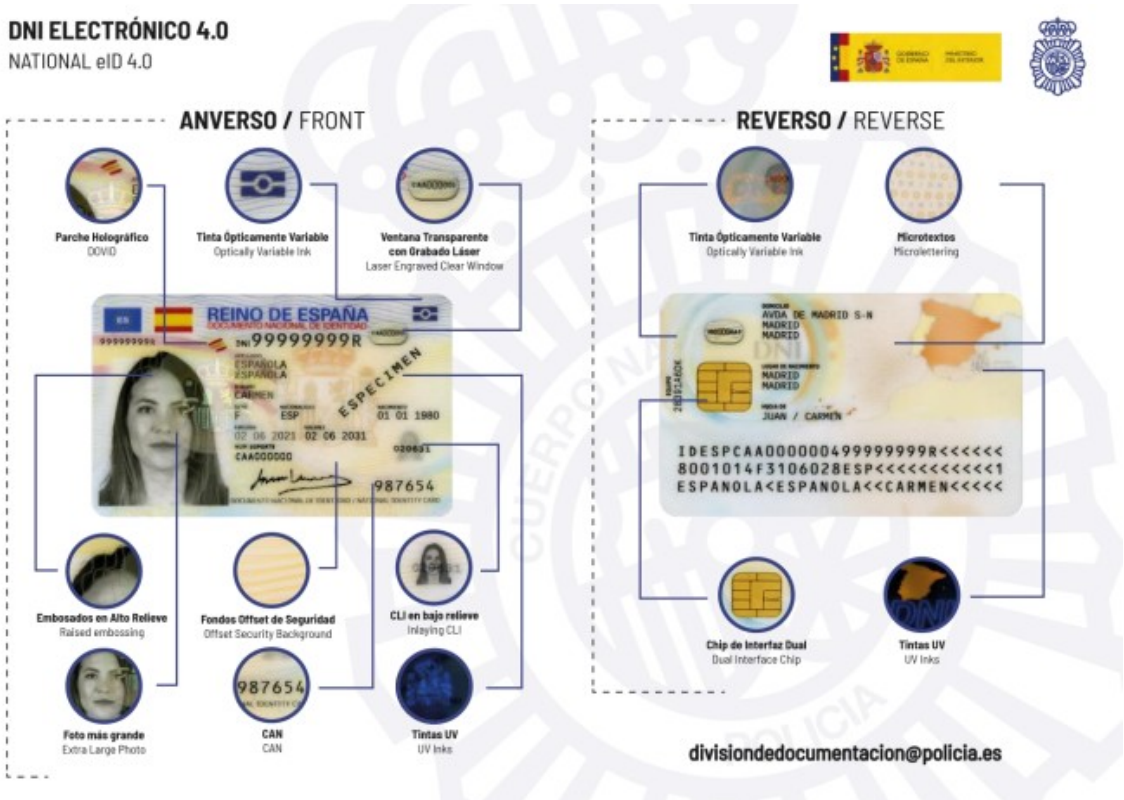
(…).

(…).

(…).

Se constata que no consta incluida la imagen del primer DNIe (expedido desde 2006 hasta finales de 2015) disponible en la página de la Dirección General de la Policía: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_3004&id_menu=51

Se constata que entre los documentos identificativos no consta incluido el nuevo DNIe 4.0, operativo desde la entrada en vigor del Reglamento UE 2019/1157 del Parlamento Europeo y del Consejo de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación, es decir, desde el 2 de agosto de 2021.



UNDÉCIMO: ORANGE forma parte de la Asociación Española para la Digitalización y participa en el proyecto “Identidad Digital Segura (IDS)” que tiene por objeto -entre

otros, proteger frente al fraude y los ciberataques y la defensa de la privacidad de los datos.

Participa activamente en la propuesta de distintos proyectos tractores y en el desarrollo de aplicaciones que garanticen la IDS.

(…)

DUODÉCIMO: ORANGE ha adoptado una serie de acciones para prevenir el SIM Swapping:

- (…).
- (…).
- (…).
- (…).
- (…).
- (…).
- (…).
- (…).
- (…)
- (…).
- (…).

DÉCIMO TERCERO: Consta la difusión de varios "Memorandos internos" emitidos por el Departamento de Fraude:

Fecha	Contenido
11/09/2019	(…)
11/09/2019	(…)
12/09/2019	(…)
9/10/2019	(…)
19/12/2019	(…)

DÉCIMO CUARTO: Consta una grabación relativa a la activación de una solicitud de duplicado de tarjeta SIM sobre la línea ******TELÉFONO.4*** realizada en fecha 22/04/2019. La activación de la tarjeta SIM se solicita a través (…) sin que el agente comercial aplique de forma debida el protocolo (…). No existe constancia del envío del correspondiente (…).

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.

De la participación de las operadoras de telecomunicaciones, y los demás intervinientes, y de las conclusiones o acuerdos a los que se llegó en el GT y que constan en las correspondientes actas, no puede deducirse que por parte de la AEPD se haya validado ningún tipo de actuación de ORANGE en relación con los hechos objeto de análisis en el presente procedimiento.

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 ejercen por los órganos administrativos que las tienen 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 una eventual falta de medidas de seguridad 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 ORANGE, 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 ante-

rior, 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 ORANGE dispone de una política de seguridad en la que se establece el modo de actuar ante los tratamientos de datos personales necesarios para la expedición de los duplicados de tarjeta. Sin embargo, también resultó acreditado 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.

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.

Sentado lo anterior, puede afirmarse que, de la instrucción del procedimiento, tal y como se infiere de los Hechos Probados y considerado el contexto del artículo 24 del RGPD en relación con ORANGE, se constató, entre otras, la implementación de un modelo más eficaz de evitación del riesgo de suplantación de identidad, la revisión, refuerzo y mejora de las medidas de seguridad aplicadas en los distintos canales tendentes a asegurar el procedimiento de identificación y entrega de la tarjeta SIM, con el fin de evitar la materialización de los fraudes. También, la reacción inmediata frente a los hechos descritos y la capacidad de la operadora para demostrar su cumplimiento. Por todo lo expuesto, centramos los hechos en la infracción derivada del artículo 5.1.f) del RGPD.

No obstante lo anterior, conforme al propio principio de responsabilidad proactiva, es el responsable del tratamiento el que debe determinar 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 ORANGE eran 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 los controles existentes en los sistemas de información que no reflejaron la trazabilidad del cambio producido en los datos personales del cliente (dirección de correo electrónico -parte reclamante uno-).

O por ejemplo, el hecho de que se determine la vía presencial como canal prioritario para la solicitud de los duplicados de SIM. Sin embargo, ORANGE (…). Si un operador establece una determinada medida como la expuesta, de prevalencia de un determinado canal, las circunstancias para esquivar la medida deberían ser controladas, ya que en caso contrario se está desvirtuando la política de seguridad implementada.

También, si existen (…), sería deseable que el sistema no permita la continuación con el proceso de cambio de SIM si (…). Aduce ORANGE que en el caso de la parte reclamante dos, al tratarse de (…), cuando anteriormente, en la instrucción del procedimiento ha confirmado lo contrario:

(…):

- (…)

- *(…)*

    - *(…)*

    - *(…)*

    - *(…)*

- *(…)*

    - *(…).*

    - *(…)*

Por otro lado, y en cuanto a los medios utilizados para identificar presencialmente al titular de la línea a los efectos de obtener un duplicado de tarjeta SIM, (…).

Especialmente significativo es el caso de la parte reclamante dos en la que (…).

Además, en la (…) no consta incluida la imagen del primer DNIe (expedido desde 2006 hasta finales de 2015) o del nuevo DNIe 4.0.

Igualmente, ORANGE aportó un (…):

(…).

(…).

Esta información no se corresponde con la que ORANGE aduce en fecha 27 de julio de 2020, en la que confirma (…). Igualmente, la información relativa a la obtención de la SIM (…) no está actualizada, ya que ese canal de acceso fue eliminado en fecha 29 de julio de 2019.

En suma, para mejorar el cumplimiento de las políticas de seguridad las instrucciones que se trasladan deben ser claras y actualizadas.

Asimismo, ORANGE no ha aportado documentación contractual con la empresa, donde consten las condiciones de entrega y las garantías de seguridad en la identificación del cliente. Recordemos que, aunque en el caso de la parte reclamante uno se obtenga la tarjeta SIM (…) y en el caso de la parte reclamante dos, de forma presencial, las actuaciones de la Agencia se han desarrollado para investigar todo el procedimiento de expedición y entrega. Por ello, sería aconsejable incluir en los contratos el compromiso de entrega de la SIM únicamente bajo previa comprobación de la identidad del destinatario y exclusivamente a él.

En cuanto al cambio del tipo infractor que habitualmente venía imputando la AEPD en los casos en los que los defraudadores conseguían suplantar la identidad de los clientes con distintas finalidades (artículo 6.1 RGPD), y la imputación a ORANGE de la responsabilidad del resultado del fraude realizado por un tercero, hemos de indicar que la AEPD tiene atribuidas, en virtud de los artículos 57 y 58 del RGPD, funciones de investigación, en la medida oportuna, respecto de las reclamaciones presentadas al efecto.

En el supuesto ahora examinado, la AEPD, tras la realización de las investigaciones oportunas y en relación con una serie de hechos concretos que considera probados, incardina los mismos en el tipo infractor que considera adecuado, conforme a la aplica-

ción e interpretación de la normativa, motivando de manera prolija y suficiente tal actuación. Y es que la AEPD, al igual que el resto de poderes públicos, está vinculada al principio de legalidad (artículo 9.1 y 9.3 Constitución -CE-) que implica la aplicación e interpretación de las normas atendiendo al supuesto de hecho específico que concurra en cada caso.

Hay que señalar que, ORANGE no explica en qué medida se ven afectados sus derechos de defensa y procedimentales por subsumir los hechos en el artículo 5.1 f) y no en el artículo 6.1 del RGPD.

Aduce que la Agencia no ha justificado el motivo por el que considera que incurre en la infracción del artículo 5.1.f) RGPD.

Sin embargo, la AEPD ha motivado con sucinta referencia de hechos y fundamentos de derecho, conforme exige el artículo 35.1.h) de la LPACAP, el fundamento de su decisión. Asimismo, ha garantizado los derechos previstos en el artículo 64.2.f) y 89.2 de la LPACAP, entre los que se encuentra el derecho a formular alegaciones, sin que, por tanto, pueda aducir indefensión. Ha podido alegar y aportar al procedimiento todo lo que a su derecho ha convenido, sin limitación alguna por parte de la AEPD. Todas las alegaciones formuladas al efecto han sido consideradas y contestadas.

A mayor abundamiento, recordemos que tratar los datos personales sin base jurídica, es decir, sin los supuestos legitimadores previstos en el citado precepto, tiene como consecuencia un tratamiento ilícito, es decir, contrario al apartado 1 del artículo 5 del RGPD. A la sazón, el mismo precepto que se imputa en el caso analizado y, en cualquier caso, ante una hipotética imputación del articulo 6.1 como sostiene ORANGE, también seria de aplicación el articulo 85.3 a) del RGPD.

Por otra parte, 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. Al comienzo de este FD ya indicamos 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.

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 y bajo determinadas circunstancias, podrá realizar

los actos de disposición patrimonial que desee. Por lo tanto, es responsabilidad de la operadora establecer unos requisitos 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 observa 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.

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;*

ORANGE, 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 Probados, 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.

Aduce ORANGE, una serie de matizaciones en cuanto a los datos objeto de tratamiento.

La actividad de tratamiento cuestionada ha sido el modelo de gestión de solicitud y activación de duplicados de tarjetas SIM que presta a través del canal presencial (desde los puntos de venta) y del canal on-line (a través de la App Mi Orange y del área de cliente/e-Care), no los tratamientos efectuados por terceras personas u otras entidades, como las financieras, que invoca en las alegaciones.

Razona que no consta que se haya tratado el IMSI. En este sentido, el IMSI en la medida que permite singularizar a un individuo, y por tanto identificarle, ha de ser considerado dato de carácter personal de acuerdo con el artículo 4.1 del RGPD.

Cabe traer a colación la Sentencia del Tribunal de Justicia de la Unión Europea (STJUE) de 19 de octubre de 2016 Asunto C-582/14, que 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 esto decir 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. En todo caso, la compañía que presta el servicio de telecomunicaciones conoce en todo momento cuál es la IP dinámica a través de la cual se produce la conexión en relación con cada uno de sus clientes.

Si el TJUE considera dato personal dicha dirección IP dinámica, "que cambia cada cierto tiempo" es lógico considerar que el IMSI, 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.

Asimismo, la Sentencia de la Audiencia Provincial (SAP) 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."*

Por lo tanto, 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. (…)"*

De hecho, la cláusula "2.1.2. Tarjeta SIM" de las condiciones generales de los servicios de ORANGE, dispone: *La Tarjeta SIM es una tarjeta que puede ser física o digital "eSIM" y que permite identificar el Servicio suscrito por el Cliente y la línea contratada para poder prestarle el Servicio Móvil. En lo sucesivo, los términos "SIM" o "Tarjeta SIM" podrán entenderse referidos indistintamente a la Tarjeta SIM física o eSIM.*

Asimismo, ORANGE en el documento (…) aportado en fecha 27 de julio de 2020, informa:

> *"(…)."*

En suma, 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.

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

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

PRIMERA: INFRACCIÓN.

En cuanto a esta alegación, nos remitimos a lo dispuesto en el FD Tercero de esta Resolución.

SEGUNDA: TRATAMIENTO DE DATOS PERSONALES Y RESPONSABLE DEL TRATAMIENTO.

Nos remitimos al FD anterior.

TERCERA: ALEGACIONES ADUCIDAS.

1. ALEGACIÓN PREVIA. - EXISTENCIA DE UN GT SOBRE DUPLICIDAD DE LAS TARJETAS SIM LIDERADO POR LA AEPD.

Aduce una quiebra en la confianza legítima depositada en la Agencia por la apertura de este procedimiento.

No cabe apreciar la vulneración del principio de confianza legítima, recogido en el artículo 3.1.e) de la LRJSP, principio que como ha reiterado la jurisprudencia - SSTS de 28 de diciembre 2012 (Rec. 273/2009), 3 de julio 2013 (Rec. 2511/2011), entre otras muchas- *"no puede invocarse para crear, mantener o extender, en el ámbito del Derecho público, situaciones contrarias al ordenamiento jurídico",* siendo la actora presunta responsable de las infracciones apreciadas en el acuerdo de iniciación, a tenor del artículo 28.1 de la LRJSP.

En relación con este principio, la Sentencia de la Audiencia Nacional (SAN), de 29 abril 2019, RJCA 2019\449, indica: Conforme a lo declarado por la antes mencionada sentencia de 6 de julio de 2012 (RJ 2012, 7760) el principio de confianza legítima comporta que *"la autoridad pública no pueda adoptar medidas que resulten contrarias a la esperanza inducida por la razonable estabilidad en las decisiones de aquélla, y en función de las cuales los particulares han adoptado determinadas decisiones. (...) como se declara en la sentencia 3 de julio de 2012 (RJ 2012, 11345) (recurso 6558/2010):"(...) La protección de la confianza legítima no abarca cualquier tipo de convicción psicológica subjetiva en el particular, siendo tan solo susceptible de protección aquella <confianza> sobre aspectos concretos, que se base en signos o hechos externos producidos por la Administración suficientemente concluyentes...". Pero de las propias decisiones de esta Sala, se ha de concluir en un importante y relevante elemento para configurar la confianza legítima, a saber, que la concreta actuación que se espera en esa confianza sea conforme al Ordenamiento (sentencia últimamente citada), es decir, es preciso que la actuación de la Administración, con su conducta, induzca al administrado "a creer que la actuación que él desarrolla es lícita y adecuada en Derecho" (sentencia de 3 de julio de 2012, dictada en el recurso 6558/2010).* En ese mismo sentido se ha declarado que no puede ampararse en la confianza legítima "*la mera expectativa de una invariabilidad de las circunstancias",* como se declara en la sentencia de 22 de marzo de 2012 (recurso 2998/2008), en la que se concluye que no puede mantenerse irreversible un comportamiento que se considera injusto.

Precisamente porque se trata de una problemática generalizada y recurrente, se consideró oportuno la realización de actuaciones previas de investigación.

En el Antecedente Cuarto hicimos referencia a los tres requerimientos de in-

formación dirigidos a ORANGE en distintas fechas.

La SAN de la Sala de lo Contencioso- administrativo, sec 1ª, 17-10-07(rec 180/06) justifica la conveniencia de las actuaciones previas de investigación en relación con los procedimientos sancionadores afirmando que: "*Se trata de que por la gravedad y trascendencia que entraña el ejercicio de la potestad sancionadora, pues el status jurídico de quien se halla sometido a un expediente sancionador, por esta sola circunstancia, puede encontrarse negativamente afectado, resulta necesario que la decisión de incoar el procedimiento sancionador sea fundada y este asentada en sólidas razones que exijan dicha incoación".*

Es decir, con la finalidad de permitir al órgano sancionador conocer los hechos previsiblemente infractores, las circunstancias concurrentes y las personas intervinientes, se le permite practicar dichas actuaciones o indagaciones previas, en cuanto sean necesarias y oportunas para verificar, hasta qué punto, existe base racional para entender producido el hecho infractor, e imputárselo a una persona determinada.

Hay que señalar que el artículo 53 de la LOPDGDD determina el "Alcance de la actividad de investigación":

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación. (…)

Así, la Agencia 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 de la LOPDGDD). No estamos utilizando ningún pretexto, como alude -noticias en prensa-, para justificar nuestra actuación, sino ante la aplicación de los principios generales que rigen el actuar de las administraciones públicas, artículo 3.1. de la LRJSP: *Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.*

Razona ORANGE que existen otros mecanismos correctivos, no obstante, insistimos, la LOPDGDD regula en el Titulo VIII los "*Procedimientos en caso de posible vulneración de la normativa de protección de datos"* y en concreto, el artículo 64.2 dispone que, cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción, se iniciará mediante acuerdo de inicio adoptado por propia iniciativa o como consecuencia de reclamación (en el caso analizado, se han registrado dos reclamaciones de afectados).

Asimismo, el artículo 109.2 de la LRJSP dispone respecto a las Autoridades Administrativas Independientes que actuarán, en el desarrollo de su actividad y para el cumplimiento de sus fines, con independencia de cualquier interés empresarial o comercial.

En definitiva, la participación de ORANGE en el GT no modifica la responsabilidad que ahora se le imputa. Por lo tanto, por el hecho de que haya participado en un GT cuyo objetivo es abordar una actividad delictiva tan específica ("SIM Swapping"), no impide que una vez constatada una infracción, deba sancionarse.

2. ALEGACIÓN PRIMERA. - INCORRECCIÓN Y FALTA DE EXACTITUD EN LAS APRECIACIONES SOBRE EL FRAUDE DE DUPLICADO.

La Agencia en ningún momento ha manifestado que la SIM permita el acceso al IMEI. Tan solo nos remitimos a él a los efectos de aclarar que tanto uno como otro (IME e IMSI) tienen la condición de dato personal conforme a la definición del artículo 4.1 del RGPD.

A juicio de ORANGE no se ha accedido a ninguna información personal distinta de la que han aportado los suplantadores. Discrepa la Agencia sobre este argumento, por cuanto, según afirma la propia ORANGE en el documento "Información y gestiones de SIM", la tarjeta SIM "*almacena toda la información sobre la línea telefónica del cliente; es el elemento que soporta la línea y el número telefónico y permite el acceso del terminal a la Red".*

Según la LGTEL, los servicios de comunicaciones electrónicas tienen la consideración de "servicios de interés general". No olvidemos que mediante estos servicios se garantiza la conectividad a servicios tan importantes como la telefonía fija, móvil o el acceso a Internet. (artículo 2.1 LGTEL)

Asimismo, el obligado respeto a la protección de los datos personales de los usuarios de este sector (artículo 41 LGTEL) figura asimismo dentro de las "obligaciones de carácter público" aplicables al sector de las comunicaciones electrónicas (Título III, capítulo III).

> *41.1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal.*

Considera que la Agencia entremezcla conceptos, en tanto en cuanto, la clave remitida por el banco (factor de posesión) no tiene la condición de dato personal y no puede considerarse una quiebra de seguridad o confidencialidad.

En estos sistemas de autenticación reforzada del cliente, conforme al artículo 4.30 de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior y por la que se mo-

difican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE (en lo sucesivo, Directiva PSD2), la autenticación se basa en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce 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. Ahora bien, si esos elementos no se aplican adecuadamente, la operativa falla.

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.

De hecho, ORANGE, en el documento catalogado como "(…) (SIM Swapping)" dice:

"1(…)."

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. Los sistemas de autenticación son, conforme a legislación europea, procedimientos que permiten al proveedor de servicios de pago comprobar la identidad del usuario de un servicio de pago o la validez de la utilización de determinado instrumento de pago, incluida la utilización de credenciales de seguridad personalizadas del usuario (artículo 4. 29 de la Directiva PSD2).

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 ORANGE.

Alude a una Guía sobre Identidad Digital y a las respuestas de la EBA, que cuestionan la seguridad de los SMS para confirmar operaciones bancarias. No obstante, las medidas de seguridad aplicadas a las operaciones de la banca on line respecto a los tratamientos realizados por las entidades financieras, no son objeto de análisis en este expediente.

3. ALEGACIÓN SEGUNDA. - GENERALIZACIÓN NO FUNDADA DE CONSECUENCIAS NEGATIVAS ASOCIADAS A LA EMISIÓN DEL DUPLICADO.

Reitera ORANGE las alegaciones formuladas con anterioridad, respecto de lo cual la AEPD reproduce lo que ya determinó en la Propuesta de Resolución.

Ya indicábamos que estimábamos la alegación aducida en lo relativo a que el acceso al duplicado no proporciona acceso directo a los contactos almacenados en la tarjeta SIM originaria, ya que, al tratarse de un dispositivo físico, se pierden todos los datos que contiene y no se podrán recuperar los contactos perdidos en la tarjeta SIM reemplazada, a no ser que se hayan almacenado en entornos asociados a Android o Apple, en cuyo caso se deberá sincronizar el dispositivo con una determinada cuenta para poder restaurarlos.

En cuanto al acceso a las cuentas de correo, bancarias y otras.

Para poder cometer la modalidad delictiva de SIM Swapping, con carácter general, 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. Tras ello, 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.

Cuando la modalidad delictiva busca un enriquecimiento patrimonial, es necesario dar los dos pasos que hemos descrito con anterioridad. Sin embargo, cuando la modalidad delictiva pretende otras finalidades como son hacerse pasar por la persona en redes sociales, arrebatar mensajes privados en redes sociales, hacerse con correos electrónicos disponibles en servidores en red, averiguar datos privados de la persona con la finalidad de obligarle a ejecutar determinadas acciones… es decir, acciones delictivas constitutivas de otras conductas delictivas como son coac-

ciones, delitos contra la intimidad, delitos de amenazas, acoso, injurias o calumnias, no es necesaria la primera acción, sino que con la simple obtención del duplicado de la tarjeta SIM es suficiente. Es habitual que las redes sociales o servidores de correo, en caso de olvido de contraseña opten por mecanismos rápidos encaminados a la obtención de un nuevo password, tal cual puede ser el envío de un enlace a la línea de telefonía ofrecida cuando el usuario se dio de alta en ella. Con lo cual, al disponer el delincuente de esa línea de telefonía con el duplicado de la tarjeta SIM, recibirá en el terminal la posibilidad de crear un nuevo password teniendo libre acceso de ese modo a las redes sociales, mensajería instantánea, navegación en la nube, correos electrónicos… de esa persona, ya que el usuario es un dato relativamente sencillo de averiguar.

En definitiva, la rigurosidad de la operadora a la hora de vigilar quién es el titular de la tarjeta SIM o persona por éste autorizada que peticiona el duplicado, debería responder a unos requisitos estrictos. No se trata de que la información a la que se refiere no esté contenida en la tarjeta SIM, sino de que, si en el proceso de expedición de un duplicado de tarjeta SIM no se verifica adecuadamente la identidad del solicitante, la operadora estaría facilitando la suplantación de identidad.

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 de SIM Swapping, que está siendo utilizado con alarmante frecuencia en los últimos años. La técnica consiste en burlar las medidas de seguridad de las entidades bancarias accediendo a los códigos alfanuméricos de confirmación, de uso único, generados con ocasión de las transacciones electrónicas y que ordinariamente se comunican a los/as clientes a través de mensajes SMS. Para ello, los/as delincuentes obtienen previamente un duplicado o una nueva tarjeta SIM a nombre de su víctima, ya sea solicitándola del operador correspondiente, simulando la identidad de aquella, ya sea valiéndose de una metodología más elaborada, como en el supuesto objeto de instrucción judicial en Zamora, en el que se aprovechaba con esa finalidad un establecimiento de reparación de móviles. Una vez tienen la tarjeta SIM a su disposición, los delincuentes se garantizan la recepción en su propio dispositivo del código de confirmación de la transacción fraudulenta y, en definitiva, la posibilidad de hacer efectiva la misma en su 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.”*

Aduce ORANGE que su responsabilidad no puede extenderse más allá de aquellas

cuestiones que quedan bajo su ámbito de actuación y que no concurre falta de diligencia, sino que realiza estas operaciones solicitando datos a quien supuestamente es su titular e incluso aportan falsificaciones de documentos públicos como medio para superar las medidas de control.

Pues bien, en el listado de 20 casos de duplicados de SIM denunciados/reclamados como suplantación de identidad o fraudulentos por los clientes, relativo a la línea ******TELÉFONO.4*** realizado en fecha 22/04/2019, se constata la activación de la tarjeta SIM (…) que se recogen en la Política de Seguridad (…).

En este momento, y contestando a las alegaciones formuladas por ORANGE en relación con el listado de los 20 casos recogidos tenemos que significar que a raíz de las dos reclamaciones por fraude de identidad, que implicaban por parte del responsable del tratamiento la emisión del duplicado de la tarjeta SIM del cliente a un tercero (tras lo cual se han producido gravosos daños económicos a los afectados) investiga en profundidad el origen del problema en aras de averiguar si 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. Por ello los 20 casos relativos a duplicados de tarjetas SIM vienen al caso, mostrando la deficiente aplicación de la política de seguridad.

Igualmente, en el caso de la parte reclamante uno, se cambió la dirección de correo electrónico de forma previa a la solicitud de SIM, sin que ORANGE haya podido acreditar alguna evidencia en sus sistemas de gestión sobre los controles que se pasaron para el cambio de la dirección de correo electrónico del cliente.

En el caso de la parte reclamante dos, la documentación (…). Ni siquiera se le solicitó un requisito adicional de control (alguna pregunta o alguna documentación original) dado que se aportó (…).

De hecho, la operadora reconoce abiertamente que no se cumplieron los protocolos, aludiendo al engaño sufrido por los trabajadores. El factor humano, la evidente posibilidad de cometer errores o ser engañados, es uno de los riesgos más importantes a considerar siempre en relación con la determinación de las medidas de seguridad. El responsable del tratamiento debe contar con el error humano como un riesgo más que probable. Los errores humanos se combaten desde el enfoque de riesgos, el análisis, la planificación, implantación y control de las medidas técnicas y organizativas adecuadas y suficientes.

Un criminal puede intentar engañar y provocar un error humano, pero son las medidas de seguridad adecuadas quienes actúan de freno.

En cuanto a que los delincuentes no han conseguido obtener datos personales de ORANGE, por lo que no puede hablarse de incumplimiento de medidas de protección, señalar que el acceso al duplicado de una tarjeta SIM que hace identificable a su titular, responde a la definición de dato personal del artículo 4.1) del RGPD.

Por todo lo expuesto, se ha considerado que los procedimientos de emisión de duplicados de tarjetas SIM requerían una mejora con el objeto de que se garantizase

la seguridad de los datos personales de los clientes de manera efectiva y en particular, su custodia, con el fin de evitar accesos no autorizados.

4. ALEGACIÓN TERCERA. – IDONEIDAD Y CUMPLIMIENTO DE LAS MEDIDAS PREVENTIVAS IMPLEMENTADAS.

ORANGE informa el número de cambios de SIM realizados en 2019, (…), sin que se haya producido ninguna incidencia en el (…) de los casos. Considera, por tanto, que sus protocolos han demostrado ser efectivos.

No obstante, este procedimiento sancionador ha tenido por objeto el análisis de los procedimientos seguidos para gestionar las solicitudes de cambio de SIM, determinando, en su caso, la vulneración del principio de la confidencialidad de los datos personales (en este caso, la tarjeta SIM) tratados por ORANGE como responsable de tratamiento y si esa vulneración ha sido producto de unas medidas de seguridad insuficientes.

Durante el año 2019, ORANGE informa haber facilitado (…) duplicados de tarjeta SIM.

Como hemos indicado anteriormente, la Agencia se ha centrado, no sólo en el hecho de que terceros han superado las medidas de seguridad implantadas por ORANGE, sino en el por qué las han superado; esto es, se examina la condición, características y adecuación de las medidas citadas a la normativa de protección de datos y la actuación del responsable del tratamiento al respecto.

Respecto al enfoque de riesgo, hay que señalar que, la Agencia no pretende exigir en ningún momento un riesgo cero. Pero el mismo RGPD indica que las medidas deben ser adecuadas, de acuerdo con el riesgo previsible. Y el RGPD tampoco hace referencia alguna a los porcentajes de materialización del riesgo a partir del cual pueden considerarse o no como desdeñables a los efectos de no considerarlo infracción ni falta de diligencia.

Se considera que está más que demostrado que la práctica de este tipo de fraudes, como el aquí analizado, es una práctica frecuente y que, por tanto, las operadoras deben contar con medidas apropiadas que garanticen que no se facilite indebidamente una tarjeta SIM a quien no sea el legítimo titular. De ahí que, del análisis de la documentación, se concluya que las medidas adoptadas no han sido las adecuadas a tal fin.

ORANGE invoca una quiebra del principio de responsabilidad objetiva en el ámbito sancionador vetado por nuestro Ordenamiento Jurídico.

Al respecto, esta Agencia ya informó en los Antecedentes del Acuerdo de Inicio y en la Propuesta de Resolución, que además de las dos reclamaciones, la SGID investigó las “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”)” como consecuencia de “las noticias aparecidas en medios de comunicación”, tal y como se desprende de la nota interior de la directora que consta en el expediente.

Por tanto, se ha investigado en profundidad el origen del problema en aras de averiguar si podía existir un fallo en el modelo de protección de la privacidad.

No es cierto, como pretende hacer ver ORANGE, que se hayan evaluado las circunstancias -en exclusiva-, de dos casos concretos, puesto que, al margen de estas reclamaciones, se ha dirigido a analizar si las medidas técnicas y organizativas adoptadas por ORANGE para la expedición de duplicados de tarjetas SIM a los titulares de las líneas telefónicas eran las apropiadas para asegurar la mitigación de los posibles riesgos para los derechos y libertades fundamentales de los titulares de las líneas.

Las circunstancias de los dos casos en los que se ha presentado reclamación ante la AEPD han puesto de manifiesto la insuficiencia de las medidas de seguridad adoptadas por ORANGE, que además, reconoce que tales medidas han sido insuficientes en un total de (…) casos durante el año 2019.

Además, hay que tener en cuenta que la gravedad de los hechos probados se plasma en la alarma social generada por la realización de estas prácticas fraudulentas, sin que sea determinante el número de reclamaciones presentadas.

Alega ORANGE que la superación por un tercero de las medidas de seguridad no puede determinar por sí sola que las mismas no sean adecuadas o suficientes. Y cita el expediente E/05168/2021, en el que se archivó una reclamación tras comprobarse que, a pesar de haberse producido un acceso a datos personales por un tercero no autorizado, se había desplegado un nivel de diligencia suficiente y adecuado, aunque se hubieran superado las medidas de seguridad implantadas.

En dicho expediente, las circunstancias eran otras. Se trataba de un tercero que estaba realizando una serie de consultas y peticiones sobre la línea de la titular, debido a que contaba con la información personal de la reclamante por el vínculo que les había unido. No resulta comparable, a juicio de esta Agencia, la información que se puede obtener debido a un vínculo con la información que puede obtener un ciberdelincuente. Por su parte, la operadora implantó no solo medidas para evitar que se produjeran dichas situaciones en general, sino también para el caso concreto. Y, por último, esa reclamación se archivó en aplicación del principio de presunción de inocencia, que impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se derive la existencia de infracción. El expediente que ahora se resuelve es distinto, en el que -además de las dos reclamaciones-, se han constatado una serie de casos informados por la propia ORANGE, en los que se ha materializado el acceso a (…) duplicados de tarjetas SIM de forma indebida, como consecuencia de carecer de las medidas de seguridad apropiadas para evitarlo.

ORANGE también cita el expediente E/00536/2016 en el que se suplanta la identidad para modificar los datos del reclamante en la intranet de ORANGE. Y añade que la Agencia consideró que “el mal uso o el uso indebido mediante suplantación de identidad por parte de un tercero no es imputable a Orange, ya que cumplió con las oportunas medidas de seguridad” y que “pese a que se produjo un acceso ilícito, la Agencia concluye que: “No se han acreditado elementos probatorios que permi-

tan atribuir a Orange una vulneración de la normativa en materia de protección de datos, en la medida en que actuó con diligencia" y, consiguientemente, archiva el procedimiento".

En este expediente, un tercero había accedido de forma indebida a los servicios ofrecidos por ORANGE a través de la página web y había realizado una serie de pedidos fraudulentos de terminales móviles. Por consiguiente, su objeto fue analizar si las medidas con que contaba ORANGE para identificar a la persona que realizaba la solicitud de los terminales habían sido suficientes para entender que había actuado con razonable diligencia. En este sentido, se consideró que ORANGE empleó una razonable diligencia ya que -precisamente-, adoptó las medidas necesarias para identificar a la persona que realizaba la solicitud de los terminales (al solicitar usuario y clave para el trámite) y que, en cuanto tuvo conocimiento de la reclamación, canceló los pedidos solicitados.

No obstante, estamos ante supuestos distintos, dado que en el expediente E/00536/2016 únicamente el fraude se concreta en la realización de pedidos fraudulentos de terminales móviles, mientras que en este procedimiento se trata de facilitar un duplicado de una tarjeta SIM (dato personal) a quien no es su titular, lo que conduce, como se ha explicado de forma reiterada, a una pérdida de control de los datos personales.

Cita también el expediente E/2723/2020, en el que asegura que se considera que ORANGE adoptó las medidas adecuadas. No obstante, la resolución del citado expediente en ningún momento afirma que las medidas adoptadas por ORANGE fueran adecuadas. Lo que afirma es que: "se ha constatado la falta de indicios racionales de la existencia de una infracción (…), no procediendo, en consecuencia, la apertura de un procedimiento sancionador". Y ello en virtud del principio de presunción de inocencia, según el cual no se puede imputar una infracción administrativa cuando no se hubieran obtenido evidencias o indicios de los que se derive la existencia de una infracción. El hecho de afirmar que no se han constatado evidencias de infracción por parte de ORANGE es muy distinto a afirmar que las medidas adoptadas por ORANGE eran adecuadas, lo que no se produce en este expediente.

ORANGE también menciona el expediente E/06963/2020. En este, la Agencia no admite a trámite la reclamación sobre reclamación de pago de facturas de líneas telefónicas contratadas utilizando sus datos personales sin consentimiento, por entender que la reclamación en cuestión había sido atendida, al bloquear ORANGE los servicios contratados y cancelar la deuda reclamada.

Tampoco se afirma en ese expediente que las medidas con que contaba ORANGE fueran adecuadas. De hecho, ni siquiera se analizan las citadas medidas.

En cualquier caso, la mencionada resolución también dispone "Todo ello sin perjuicio de que la Agencia, aplicando los poderes de investigación y correctivos que ostenta, pueda llevar a cabo posteriores actuaciones relativas al tratamiento de datos referido en la reclamación". Esto es, sin perjuicio de lo cual, esta Agencia puede investigar sobre el procedimiento seguido en general para este tipo de hechos. Por tanto, aunque en ese supuesto concreto se hubiera inadmitido la reclamación en cuestión, ello no obsta a que la Agencia pueda examinar las medidas de seguridad

con que cuenta ORANGE con el fin de evitar que un tercero contrate líneas de teléfono a su nombre sin su consentimiento.

Por su parte, ORANGE también menciona el expediente E/05272/2018, en el cual diversos trabajadores difundieron imágenes de clientes sospechosos de haber sustraído objetos vía WhatsApp y, no existiendo indicios de que la entidad hubiera incumplido sus obligaciones en cumplimiento de los principios de integridad y confidencialidad, procedió a acordar el archivo de las actuaciones.

Al respecto, esta Agencia quiere señalar que el supuesto de hecho es considerablemente distinto al analizado en este procedimiento sancionador. Y que, el hecho de que en dicho expediente no se hubieran obtenido indicios razonables de la existencia de una brecha de seguridad en el tratamiento que realizada el responsable de tratamiento respecto de los datos de sus clientes, ello no obsta a que en este procedimiento sancionador se hubiera comprobado que ORANGE ha facilitado el acceso a unos duplicados de tarjeta SIM solicitados de forma fraudulenta, como consecuencia de contar con unas medidas de seguridad que no resultan adecuadas a tal fin.

También menciona ORANGE el expediente E/07129/2014, en el que la AEPD archiva el procedimiento en base a, que no siendo posible determinar la identidad del infractor, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan la imputación.

Al respecto, hay que señalar que, en dicho expediente se reclama por la realización de una compra en un sitio web realizada, en su nombre, sin el consentimiento del reclamante. En primer lugar, el supuesto de hecho es considerablemente distinto al analizado ahora. Y en cuanto al principio de presunción de inocencia, reiteramos que este principio impide imputar una infracción administrativa cuando no se hubieran obtenido evidencias o indicios de los que se derive la existencia de infracción, cuestión esta que si concurre en el caso analizado.

Cita ORANGE el expediente E/08205/2019, en el que se produjo una brecha de seguridad, en la que se filtraron nombres, apellidos y otros datos personales de clientes, alcanzando más de 1.300.000 afectados. La Agencia consideró que la entidad demandada disponía de las medidas técnicas y organizativas necesarias para afrontar una brecha como la ocurrida y que adoptó las medidas adicionales necesarias para paliar el impacto y evitar que el suceso se repitiera en el futuro.

Hay que señalar, que dicho supuesto versaba sobre un hacker que había obtenido la base de datos de usuarios registrados en una página web y comercializada a través de la *deep web*. Y que durante la investigación realizada, se comprobó que las medidas de seguridad con que contaba la responsable de tratamiento eran adecuadas para afrontar un incidente de esas características y que había reaccionado de forma diligente al objeto de notificar, comunicar y minimizar el impacto e implementar las medidas razonables oportunas para evitar que se repita en el futuro un incidente similar. No obstante, además de que el supuesto de hecho es considerablemente distinto al supuesto aquí analizado, el hecho de que en dicho expediente se hubiera apreciado que el responsable de tratamiento contaba con las medidas de

seguridad apropiadas, ello no obsta a que en este procedimiento sancionador se haya comprobado que ORANGE facilitó el acceso a duplicados de tarjeta SIM, sin asegurar la identidad de sus titulares.

Por último, menciona ORANGE el expediente E/05441/2018, en el que la empresa reclamada sufre una brecha de seguridad, donde el atacante consigue acceder de forma no autorizada a una base de datos del reclamado. La Agencia indica que la brecha ha vulnerado el artículo 32 del RGPD. Sin embargo, se señala que el reclamado tenía implementadas medidas de seguridad que eran, en principio, adecuadas. Se considera así, que la actuación del reclamado como responsable del tratamiento es acorde con la normativa de protección de datos, archivando, consiguientemente, las actuaciones.

En dicho supuesto, el atacante consiguió acceder de forma no autorizada a una base de datos del reclamado. No obstante, se comprobó que el reclamado "tenía implementadas medidas de seguridad que, en principio, eran las adecuadas para garantizar que los datos personales no fueran accesibles por terceros y, como consta en los hechos, en cuanto el ataque fue detectado y confirmado por la entidad se adoptaron de manera inmediata una serie de medidas de seguridad adicionales con el fin de minimizar los riesgos y extremando las dificultades para el acceso y extracción de la información". Como se ha indicado anteriormente, además de que el supuesto de hecho es considerablemente distinto al supuesto de fraude analizado, el hecho de que en dicho expediente se hubiera apreciado que el responsable de tratamiento contaba con las medidas de seguridad apropiadas para el caso concreto, no obsta que en este procedimiento se haya comprobado que ORANGE disponía de vías de acceso a la obtención de los duplicados (quioscos expendedores o activaciones telefónicas) que favorecían las suplantaciones de identidad.

ORANGE aduce que, no puede vincularse el hecho de permitir en determinadas situaciones el uso de canales no presenciales con ninguna falta de diligencia, en tanto que cualquier vía es susceptible de ser objeto de intentos de fraude.

Ante esto, hay que insistir en que la seguridad de un procedimiento es, como la de una cadena, la de su eslabón más débil, y en el caso de establecer medidas de seguridad estrictas en un canal, si no se establecen también medidas equivalentes en el resto de los canales, se está reduciendo la seguridad global a la del canal de seguridad menor.

En cuanto a la libertad de los gestores para cumplir con las medidas de seguridad y el incumplimiento puntual en estos casos aislados, la imposición de penalizaciones por importe de 300'00 euros, no exime a la operadora de sus obligaciones con los encargados del tratamiento.

De las afirmaciones de ORANGE parece extraerse la conclusión de que no tiene ningún poder de actuación para evitar estos fraudes o suplantaciones, ya que atribuye toda la responsabilidad a terceros intervinientes (encargados o suplantadores). No estamos de acuerdo con este convencimiento.

Los conceptos de responsable y encargado de tratamiento no son formales, sino funcionales y deben atender al caso concreto. El responsable del tratamiento lo es

desde el momento que decide los fines y los medios del tratamiento, no perdiendo tal condición el hecho de dejar cierto margen de actuación al encargado del tratamiento. Así se expresa indubitadamente en las Directrices 07/2020 del CEPD -la traducción es nuestra-:

> *"Un responsable del tratamiento es quien determina los propósitos y los medios del tratamiento, es decir, el porqué y el cómo del tratamiento. El responsable del tratamiento debe decidir sobre ambos propósitos y medios. Sin embargo, algunos aspectos más prácticos de la implementación ("medios no esenciales") se pueden dejar en manos del encargado del tratamiento. No es necesario que el responsable tenga realmente acceso a los datos que se están tratando para calificarse como responsable".*

Asimismo, en el punto 6 se dice (la traducción es nuestra):

> *El responsable del tratamiento será responsable del cumplimiento de los principios establecidos en el artículo 5, apartado 1, del RGPD; y eso*
>
> *El responsable del tratamiento deberá poder demostrar el cumplimiento de los principios establecidos en el artículo 5, apartado 1, del RGPD*

También en su punto 8 establecen:

> *El principio de responsabilidad se ha desarrollado más detalladamente en el artículo 24, que establece que el responsable del tratamiento aplicará las medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento se realiza de conformidad con el RGPD. Dichas medidas se revisarán y actualizarán en caso necesario. (…)*

ORANGE debe evaluar la posibilidad (real) de que tal situación se produzca y es su obligación implementar medidas que eviten este tipo de situaciones o, al menos, las detecten rápidamente. Considerar todas estas supuestas desviaciones de los protocolos establecidos por ORANGE como meros hechos puntuales ante los cuales no se realizan actuaciones adicionales para evitarlos, supone no actuar con la debida diligencia y es por ello, por lo que se considera que ORANGE ha infringido la obligación de asegurar la confidencialidad de los datos personales en el supuesto aquí analizado, como consecuencia de carecer, precisamente, de las medidas de seguridad adecuadas para tal fin.

Tampoco esta Agencia ha exigido la "monitorización total de los empleados", tal y como afirma ORANGE. Simplemente se exige que se implementen unas medidas de seguridad acordes al riesgo que existe de que los agentes no cumplan con las medidas previstas por ORANGE, entre otras.

ORANGE afirma que (…). No obstante, el mero hecho (…) para comprobar la actividad efectiva de los usuarios y adoptar nuevas medidas, no se puede considerar como una medida suficiente y adecuada a los fines reseñados. Por último, hay que

recordar que esta no es la única medida de seguridad que se analiza ni la única que podría emplearse para asegurar la confidencialidad de los datos personales en cuestión.

Por tanto, amén de las medidas de seguridad implementadas con posterioridad a la comisión de los Hechos Probados y que se valoran de forma positiva por la Agencia, la infracción se considera probada. Por todo lo expuesto, la infracción que se imputa es la prevista en el artículo 5.1.f) del RGPD.

Por último, indica ORANGE que "el carácter de derecho fundamental del derecho a la protección de datos no elimina la necesidad de examinar la diligencia desplegada por ORANGE, ni la consideración del porcentaje ínfimo de incidencias que se han producido en los procesos de duplicado de tarjeta SIM. **Toda la actividad de la AEPD versa sobre un derecho fundamental**, por lo que dicho argumento no es válido para sostener la sanción propuesta.

A este respecto, efectuar varios matices.

En primer término, la AEPD también ejerce funciones relacionadas con los derechos digitales (artículos 89 a 94 de la LOPDGDD).

En segundo término, el ejercicio de la potestad sancionadora se ha llevado a cabo previo procedimiento administrativo, acompañado de las debidas garantías, y ha llevado a determinar los Hechos, probar la culpa y graduar la respuesta administrativa. Esta graduación no se ha hecho al margen de las circunstancias concurrentes, sino que como manifestación y exigencia del principio de transparencia (artículo 3.1.c) LRJSP) y derecho a una buena administración (artículo 41 de la Carta de los Derechos Fundamentales de la UE), los hechos se han tratado de forma imparcial y equitativamente, motivando en todo momento la decisión final.

Por lo tanto, la Agencia se ha limitado a analizar las circunstancias del caso concreto con el fin de identificar la existencia de indicios o evidencias (o no) de infracción en su ámbito competencial. Y consecuencia de ello, ha considerado probado que ORANGE ha vulnerado uno de los principios relativos al tratamiento (artículo 5.1.f) RGPD).

5. ALEGACIÓN CUARTA. – ACTUACIÓN DILIGENTE DE ORANGE.

Invoca una total indefensión, por cuanto a pesar de que ha conseguido acreditar el cumplimiento de su deber de diligencia y ser este reconocido, es objeto de una sanción por un motivo indeterminado.

La Agencia ha respetado escrupulosamente el procedimiento, permitiendo a ORANGE el ejercicio de su derecho a una tutela efectiva, toda vez que en este procedimiento se han respetado los principios de bilateralidad, contradicción e igualdad de armas como exige la reiterada doctrina del Tribunal Constitucional señala sobre el derecho a la tutela judicial efectiva que (Valga por todas la Sentencia 220/2002 de 25 Nov. 2002, Rec. 5497/1999) "3. Este Tribunal ha declarado reiteradamente que *el derecho a la tutela judicial efectiva sin indefensión, que se reconoce en el* art. 24.1 CE*, garantiza el derecho a acceder al proceso y a los recursos legal-*

mente establecidos en condiciones de poder ser oído y ejercer la defensa de los derechos e intereses legítimos en un procedimiento en el que se respeten los principios de bilateralidad, contradicción e igualdad de armas procesales, (…) (SSTC 167/1992, de 26 Oct.; 103/1993, de 22 Mar.; 316/1993, de 25 Oct.; 317/1993, de 25 Oct.; 334/1993, de 15 Nov.; 108/1994, de 11 Abr.; 186/1997, de 10 Nov.; 153/2001, de 2 Jul.; 158/2001, de 2 Jul.).

La STC 86/1997, de 22 Abr., FJ 1, dice: *«la indefensión ha de ser material, y no meramente formal, lo que implica que ese defecto formal haya supuesto* un perjuicio real y efectivo para el demandado en sus posibilidades de defensa *(STC 43/1989, 101/1990, 6/1992 y 105/1995, entre otras)»;* en este sentido, ORANGE, en todo momento ha tenido conocimiento de los hechos que se le imputan, las posibles infracciones de los que los hechos son constitutivos, ha podido alegar cuanto a su derecho ha considerado oportuno y ha podido solicitar las pruebas y aportar los documentos que ha considerado en su defensa a lo largo de la instrucción del procedimiento sancionador y, que han sido analizados y tomados en consideración como se refleja en la Propuesta de Resolución contra la cual también ha presentado las alegaciones oportunas que están siendo objeto de análisis en esta Resolución, por lo que, desestimamos la alegación aducida.

Asimismo, lejos de la pretensión de ORANGE, de que los párrafos transcritos en la Propuesta de Resolución pongan de manifiesto una contradicción no solucionable, acreditan que la Agencia ha respetado escrupulosamente los principios del procedimiento sancionador y más en concreto el derecho a la defensa de ORANGE.

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 constituye el elemento de la culpabilidad.

Recordemos que los clientes -personas físicas o jurídicas- suscriben contratos privados con ORANGE para la prestación de determinados servicios que se someten a unas cláusulas de privacidad recogidas en el Anexo de Privacidad conforme dispone la cláusula 13.1 de las “Condiciones Generales de los Servicios de ORANGE”.

Por ejemplo, la cláusula 8 de la vigente Política de Privacidad dice:

> *“8. Medidas de seguridad*
>
> *La seguridad de la información es uno de nuestros firmes compromisos y en cumplimiento de la legislación vigente <u>ORANGE tratará los datos del Usuario en todo momento de forma absolutamente confidencial</u> y guardan-*

do el preceptivo deber de secreto respecto de los mismos, adoptando al efecto las medidas de seguridad de índole técnica y organizativas necesarias que garanticen la seguridad de sus datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos."

Por lo tanto, al igual que a los clientes se les exige el cumplimiento de las obligaciones estipuladas en los contratos suscritos con la operadora, de esta, se espera el cumplimiento de las obligaciones que en materia de seguridad y confidencialidad le competen.

En cuanto a la diligencia debida, reconocemos que ORANGE ha actuado posteriormente de forma diligente a la hora de minimizar el impacto a los posibles afectados implantando nuevas medidas de seguridad para evitar la repetición de incidentes similares en un futuro.

Ciertamente, el principio de responsabilidad previsto en el artículo 28 de la LRJSP, dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."*

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".

Por consiguiente, se desestima la falta de culpabilidad. La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, 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 (…).

En este sentido, ORANGE cuenta con una red de comerciales, puntos de venta y distribuidores homologados a través de un contrato de distribución para ofrecer los servicios de ORANGE. Entre estos servicios ofrecidos desde sus puntos de venta, está la realización de duplicados de tarjetas SIM correspondientes a una línea de telefonía móvil.

Recordemos, que en el caso de la parte reclamante uno, se modificó en la ficha de cliente el email de contacto que constaba previamente (…). Posteriormente, se obtuvo la expedición de un duplicado de la tarjeta SIM, aun habiendo informado (…) en cualquier trámite con la operadora. Y por último, se produce la activación telefónica de la tarjeta SIM sin enviar un (…) a alguna de las líneas asociadas al contrato de la parte reclamante, (…).

En cuanto a que la emisión de duplicado no es suficiente para realizar operaciones bancarias en nombre de los titulares, ciertamente, para completar la estafa, 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.

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

En definitiva, la vulneración de la infracción administrativa imputada responde a un precepto incluido dentro de “Principios relativos al tratamiento” que exige una seguridad adecuada en el tratamiento de los datos personales, seguridad que no se ha garantizado de acuerdo con los Hechos Probados. Y ello es así, porque ha facilitado duplicados de tarjetas SIM a terceras personas distintas a las legítimas titulares de las líneas móviles, tras la superación por estas de la política de seguridad existente, lo que evidencia un incumplimiento del principio de confidencialidad.

La antijuridicidad es la cualidad que tiene una conducta previamente típica de vulnerar el ordenamiento jurídico y los fines que este persigue. De este modo, para ser susceptible de sanción no basta con que la conducta encaje en la descripción contenida en el tipo, sino que con ello se estén vulnerando los objetivos perseguidos por la ley. A este respecto, la conducta será antijurídica si se lesiona el bien jurídico protegido por el precepto vulnerado.

En este supuesto, la legislación sobre protección de datos personales persigue la finalidad de que los responsables y encargados de los datos realicen un tratamiento

de estos disponiendo de medidas de seguridad que impidan el uso ilícito o fraudulento de los mismos. Y este bien jurídico ha quedado lesionado en los hechos objeto de este procedimiento.

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).

Por estos motivos, se desestima la alegación aducida.

6. ALEGACIÓN QUINTA. – FALTA DE PROPORCIONALIDAD 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. Si bien, este aspecto será objeto de análisis en el FD Séptimo.

Aduce ORANGE que la imposición de una multa con finalidad disuasoria no está justificada en el presente supuesto, puesto que no ha sido su voluntad ni intención que estas situaciones se produzcan.

Desde luego que no dudamos de que la operadora tenga intención o voluntad en que estas situaciones se produzcan. Pero confunde la intencionalidad con la negligencia, siendo esta segunda la determinante de la comisión de la infracción.

Lo cierto es que se ha producido una infracción del artículo 5.1.f) del RGPD que debe ser sancionada con una multa en atención a las graves circunstancias individuales concurrentes. Dicha multa debe reunir las características impuestas por el artículo 83.1 del RGPD, esto es, debe individualizarse y ser efectiva, proporcionada y disuasoria.

La multa ha de ser disuasoria, a los efectos de que la conducta infractora no se reitere en el futuro.

Recordemos que, en cuanto a la imposición de una advertencia, apercibimiento, o la adopción de medidas correctivas conforme al artículo 58 del RGPD, 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 aparta-*

do 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)."

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

La multa debe generar un efecto disuasorio respecto del incumplimiento y vulneración de la normativa de protección de datos y nunca resultar más beneficioso para el infractor que el cumplimiento de la norma infringida.

Por otro lado, asevera ORANGE que ha de considerarse para determinar la cuantía de la multa y su proporcionalidad que no ha obtenido beneficio, sino que ha sufrido perjuicio por la comisión del delito.

Además de que, la producción de un eventual perjuicio en el responsable del tratamiento no es considerado como un factor atenuante por la normativa de protección de datos y así se observa de la simple lectura de los artículos 83.2 del RGPD y 76.2 de la LOPDGDD, volvemos a recordar que el objeto del presente procedimiento se centra en la ausencia de garantías de seguridad que ha permitido el acceso no autorizado o ilícito de terceros a los datos personales de los interesados.

Los posibles perjuicios que señala que sufre -ataque a sus sistemas y activos- son provocados por su propia negligencia, puesto que, si hubiera dispuesto de medidas de seguridad adecuadas, tal acceso por terceros no se hubiera producido y el delito posterior no se habría materializado.

Asimismo, en sus alegaciones fija como perjuicios el haber tenido que realizar *"in-*

vestigaciones internas, realizar compensaciones a los reclamantes y reevaluar procedimientos y protocolos". Todos esos perjuicios relativos a investigaciones internas y reevaluación de procedimientos y protocolos no dejan de ser obligaciones propias de la responsabilidad proactiva que impone desde la gestión del riesgo, entre otros muchos deberes, el mantenimiento, actualización y control y auditoría de las políticas de protección de datos en una organización.

Las compensaciones a los reclamantes derivan, asimismo, de la cesión de los datos personales de los afectados a terceros -posibilitando la comisión posterior de delitos- lo que constituye una falta atribuible también a ORANGE, consecuencia de la infracción del artículo 5.1.f) del RGPD.

Igualmente, la multa administrativa será efectiva porque conducirá a la compañía a aplicar las medidas técnicas y organizativas que garanticen un grado de seguridad correspondiente a la categorización del tipo de transacción.

También es proporcional a la vulneración identificada, en particular a su gravedad, a los riesgos en los que se ha incurrido y a la situación financiera de la compañía.

Asimismo, la participación de ORANGE en el GT no modifica la responsabilidad que ahora se le imputa una vez constatada la infracción.

CUARTA. - PRINCIPIOS RELATIVOS AL TRATAMIENTO.

Alude a la compensación que recibieron las personas afectadas por parte de ORANGE. A este respecto, consta una comunicación dirigida a la parte reclamante uno, de fecha 20 de enero de 2020, con el siguiente tenor:

(…).

La medida adoptada se considera que tiene la consideración de mínimo imprescindible después de que la persona afectada perdiera la línea telefónica.

Alude al descarte de lo que califica como "supuestos hipotéticos" o "elucubraciones" de la Agencia, no denunciadas por ningún reclamante: acceso a aplicaciones, uso de redes sociales, etc. Pues bien, estos hechos no se han considerado como circunstancias individuales en la infracción que se imputa a ORANGE, sino que ofrecen una perspectiva de posibles riesgos derivados del tratamiento en cuestión. La gestión del riesgo supone un ejercicio de reflexión que hay que llevar a cabo antes de realizar una actividad de tratamiento de datos personales. Su objetivo es el de identificar y poder anticiparse a los posibles efectos adversos, o no previstos, que el tratamiento podría tener sobre los interesados. Ha de permitir que el responsable tome las decisiones y acciones necesarias para conseguir que el tratamiento cumpla los requisitos del RGPD y la LOPDGDD, garantizando y pudiendo demostrar la protección de los derechos de los interesados.

Tampoco confunde la Agencia el acceso individual a la tarjeta SIM con el acceso al terminal móvil ni está exigiendo responsabilidad administrativa alguna en este sentido.

En cuanto a las operaciones bancarias realizadas y sobre la seguridad de los tratamientos que efectúan las entidades financieras, hay que señalar que, estas entidades

son responsables del tratamiento de los datos de sus clientes, y les competen idénticas obligaciones que las señaladas hasta ahora para las operadoras referidas al cumplimiento del RGPD y la LOPDGDD, y además las derivadas del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

También invoca el artículo 28.10 del RGPD, pues bien, desde un principio debe descartarse que este precepto permita la atribución de responsabilidad sancionadora al encargado del tratamiento. En primer lugar, porque aclara que lo dispuesto en el mismo lo es "sin perjuicio de lo dispuesto en los artículos 82, 83 y 84" (régimen sancionador RGPD). Y, sobre todo, porque la consecuencia jurídica prevista en el artículo 28.10 no es la sancionadora, sino la de considerar al encargado como responsable del tratamiento. La conclusión es lógica, toda vez que, si aquel infringe el Reglamento "al determinar los medios y fines del tratamiento", debe ser considerado como responsable.

No es eso lo que ha ocurrido en este expediente. De hecho, no ha quedado acreditado que se hayan realizado actuaciones que supusieran una "determinación de los fines y medios", sino que, según la propia ORANGE, habrían incumplido alguna de las instrucciones emanadas por esta en los procesos de identificación de clientes.

En consecuencia, en ningún caso procede invocar el artículo 28.10 RGPD para una presunta atribución de responsabilidad a los encargados, que, además, implique la exoneración del responsable del tratamiento (ORANGE conforme ha quedado probado en este expediente).

ORANGE no puede eludir la responsabilidad que le corresponde respecto a la seguridad del tratamiento, escudándose en los incumplimientos de los implicados en la gestión de las solicitudes de duplicados.

Respecto a las dos reclamaciones ya hemos aclarado con anterioridad que este procedimiento abarca una investigación más amplia.

En cuanto a que no ha facilitado datos a terceras personas, la Oficina de Seguridad del Internauta nos dice que el *"Duplicado de tarjeta SIM o intercambio de tarjeta SIM - SIM Swapping-" "se basa en la duplicación de nuestra tarjeta SIM, y para ello, los atacantes necesitan algunos datos personales, como nombre y apellidos, DNI, fecha de nacimiento, los 4 últimos dígitos de nuestra cuenta bancaria, etc., que han podido obtener por otras vías, como el phishing o comprando en tiendas online fraudulentas. Con estos datos, los atacantes solicitan un duplicado de nuestra SIM, suplantando nuestra identidad con los datos anteriores ante la operadora. Mientras, lo único que notamos es que nuestro dispositivo se queda sin cobertura móvil, y cuando nos conectemos a una red wifi, comenzaremos a recibir notificaciones de movimientos realizados desde nuestro móvil sin nuestro consentimiento, como transferencias bancarias o compras online, entre otras".*

No se exige una obligación de resultado, sino de actividad, pero para evaluar dicha actividad e implementación de medidas y su consideración como "adecuadas" es inevitable analizar los métodos utilizados por el tercero para acceder ilícitamente al proceso de duplicado, las salvaguardas implementadas por ORANGE e inevitablemente, el resultado.

En cuanto a la relevancia especial de la tarjeta SIM, nos remitimos a la graduación motivada en el FD Séptimo.

Por último, en cuanto al despliegue de medidas de seguridad, que duda cabe, que ORANGE ha revisado los protocolos para prevenir las suplantaciones de identidad en estos procesos; ha trasladado la información a los implicados en la tramitación; ha introducido mejoras tras conocer ciertas vulnerabilidades; incluidas las penalizaciones por su incumplimiento. Sin embargo, no compartimos el hecho de que se haya llevado a cabo un despliegue de medidas de seguridad apropiado y adecuado, en los términos del artículo 32 del RGPD.

No basta con disponer de una política de seguridad, sino de adecuarla 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.

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.

QUINTA. - SEGURIDAD DEL TRATAMIENTO.

No se imputa una infracción del artículo 32 del RGPD.

SEXTA. - CONDICIONES GENERALES PARA LA IMPOSICIÓN DE LA MULTA ADMINISTRATIVA.

Objeto de análisis en el FD Séptimo de esta Resolución.

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 consonancia con estas previsiones, el considerando 75 del RGPD establece: *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 técnica 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, el teléfono de la víctima se queda sin servicio pasando el control de la línea a las personas suplantadoras. En consecuencia, 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 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 tras facilitar ORANGE duplicados de la tarjeta SIM a terceras personas que no son las legítimas titulares de las líneas móviles e incluso modificar los datos personales -correo electrónico o el número de SIM- (parte reclamante uno), 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 la tarjeta SIM resulta determinante para las actuaciones posteriores desarrolladas por las personas suplantadoras que tienen por objeto obtener un beneficio económico (constan hasta cinco llamadas al Banco Santander y la realización de diez operaciones bancarias en el caso de la parte reclamante uno y una operación, en el caso de la parte reclamante dos), ya que el suplantador aprovecha 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 tras acceder a las claves de banca on-line del legítimo abonado.

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 ORANGE tienen el deber legal de garantizar su seguridad, tal como lo haría con cualquier otro activo de la empresa.

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 funda-

mentales 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 comportamientos 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:
  - Naturaleza y gravedad 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. Permite 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 pasa a tener 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.

Frente a lo que alega ORANGE, la gravedad de la infracción se centra en la pérdida de disposición y control sobre los datos personales de los clientes de la operadora por ausencia de garantías de seguridad apropiadas. La AEPD no focaliza en actuaciones anteriores o posteriores de terceros, sino en las acciones u omisiones de ORANGE que han posibilitado el acceso no autorizado o ilícito de datos personales de sus clientes a terceros por ausencia de garantías de seguridad apropiadas, cuestión que ha quedado debidamente probada.

Con toda probabilidad, si ORANGE hubiera dispuesto de medidas de seguridad apropiadas esta cesión de datos personales a terceros no se hubiera producido.

Es cierto que los terceros no han accedido a los teléfonos móviles de los interesados, pero sí a sus datos personales, tal y como se pone de manifiesto en el presente procedimiento sancionador.

Asimismo, no corresponde a la AEPD determinar cuáles son las concretas medidas de seguridad a implementar, sino al responsable del tratamiento, conocedor en profundidad de su organización, tratamientos, vulnerabilidades y de las medidas de seguridad precisas para hacer efectivo el principio de integridad y confidencialidad.

· Duración de la infracción:

Si bien los hechos denunciados por las partes reclamantes acontecen en fechas determinadas, ORANGE declaró en el ejercicio 2019, (…) casos junto a ORANGE VIRTUAL ESPAÑA, S.A.U (SIMYO).

ORANGE asevera que las infracciones fueron puntuales y rápidamente solventadas y que los (…) casos son atribuibles a otra sociedad jurídicamente diferenciada.

El expediente sancionador tiene su origen en dos reclamaciones presentadas ante la Agencia, si bien ésta no sólo ha tenido en cuenta los hechos concretos y especificidades acaecidos en esos casos, sino que ha cuestionado las medidas de seguridad adoptadas por ORANGE con carácter general. Así, debe tomar en consideración todos los casos de fraude declarados por la propia ORANGE junto a ORANGE VIRTUAL ESPAÑA, S.A.U (SIMYO) que muestran un continuo devenir de casos de fraude.

Sobre este particular, llamar la atención que junto con las alegaciones a la Propuesta de Resolución se aporte un Documento 1 relativo a la denuncia presentada ante la Jefatura Superior de Policía, Brigada provincial de policía judicial, Gº 7, de Madrid, por ORANGE ESPAÑA, S.A.U. como perjudicada por los hechos descritos en la denuncia (suplantación de identidad, duplicación fraudulenta de tarjeta SIM y fraude bancario) de clientes de ORANGE y de SYMIO indistintamente, cuando afirma en sus alegaciones que son dos personas jurídicas distintas.

· Núm. de interesados afectados:

La Resolución recoge las reclamaciones formuladas por las dos partes reclamantes.

Además, ORANGE informa un porcentaje de casos declarados en el ejercicio 2019 (…) respecto al número total de clientes (…) que alcanza un (…) %.

Informa sobre la realización de aproximadamente (…) cambios de SIM, alcanzando los casos de fraude un (…) % del total de cambios de tarjetas SIM realizados.

Dado que, tal y como se ha explicitado, el objeto del procedimiento sancionador no se circunscribe a las dos reclamaciones presentadas, sino a la ausencia de garantías de seguridad y al acceso no autorizado o ilícito de los datos, se considera la cifra global referida.

· Nivel de los daños y perjuicios sufridos:

Alto.

Aduce que la práctica totalidad de las operaciones no han dado lugar a ninguna contingencia, ni se ha producido daño o perjuicio alguno y que la realización de operaciones bancarias es totalmente ajena a la duplicación de la tarjeta SIM.

Sin embargo, los hechos probados constatan que tras la emisión de los duplicados se han efectuado 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.

ORANGE no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias. No obstante, también es cierto, que si ORANGE asegurase el procedimiento de identificación y entrega del duplicado de tarjeta SIM, 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 como confirmación de las operaciones que ejecutan. 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 al 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.

Respecto de las alegaciones formuladas por ORANGE relativas a que no cabe imputar los daños y perjuicios a ORANGE ni considerarlos como agravantes, hemos de significar a mayor abundamiento que es un

daño en sí mismo el acceso no autorizado o ilícito de los datos personales de un interesado por un tercero al vulnerarse el Derecho Fundamental a la protección de datos de carácter personal.

En suma, la aplicación del agravante del artículo 83.2.a) del RGPD se refiere a todos estos aspectos anteriormente analizados, puestos de manifiesto en los Hechos Probados, 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 es la política de protección de datos implantada por el responsable del tratamiento a raíz de diversas reclamaciones presentadas ante la AEPD.

- Artículo 83.2.b) RGPD:

· Intencionalidad o negligencia en la infracción:

Aduce que su conducta ha de ser considerada diligente y actuar este hecho como atenuante de la sanción.

Si bien la Agencia considera que no hubo intencionalidad por parte de ORANGE, la Agencia concluye que fue negligente al no asegurar un procedimiento que garantizase la protección de los datos personales de sus clientes. De manera que, se produce un resultado socialmente dañoso que impone la desaprobación de la política de seguridad implantada.

Negar la concurrencia de una actuación negligente por parte de ORANGE 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 recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

Asimismo, en contraposición a las afirmaciones de ORANGE, cuando la AEPD indica que la operadora "*fue negligente al no asegurar un procedimiento que garantizase la protección de los datos personales de sus clientes"*, no impone una responsabilidad objetiva respecto de las medidas de seguridad. Ello es así, porque esta afirmación ha de ponerse en su contexto: en una vulneración del principio de confidencialidad como

consecuencia de una negligencia a la hora de implementar las medidas adecuadas a que hace referencia el artículo 5.1.f) del RGPD para garantizar esa confidencialidad. Es innegable, que el acceso no autorizado o ilícito de los datos personales del afectado se ha producido, derivado, en este caso por una ausencia de medidas de seguridad adecuadas.

- Artículo 83.2.d) RGPD:

· Grado de responsabilidad del responsable:

Alto.

La responsabilidad de las vulnerabilidades en el procedimiento implantado para la expedición de la SIM corresponde a ORANGE. Los encargados del tratamiento -en su caso-, solo pueden tratar los datos siguiendo las instrucciones documentadas del responsable.

Los datos personales que recabe ORANGE tanto para la contratación del servicio como durante su provisión son de su responsabilidad y deben ser tratados de forma que se permita el buen desarrollo de la relación contractual entre las partes, garantizando en todo momento la aplicación de los principios del artículo 5 RGPD. Y ello, es independiente de que el tratamiento lo realice por sí mismo o a través de un encargado de tratamiento.

En este sentido el artículo 28.3.h) del RGPD establece instrumentos de supervisión continua por parte del responsable del tratamiento al indicar que el encargado *"pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*".

Respecto a la realización de auditorías como un medio idóneo para que el responsable del tratamiento supervise de manera continua al encargado del tratamiento, las Directrices 07/2020 del CEPD establecen que: *"99. La obligación de utilizar únicamente a encargados de tratamiento "que proporcionen garantías suficientes" contenidas en el artículo 28, apartado 1, del RGPD es una obligación continua. No termina en el momento en que el controlador y el encargado del tratamiento celebran un contrato u otro acto legal. En su lugar, el controlador debe, a intervalos apropiados, verificar las garantías del procesador, incluso mediante auditorías e inspecciones cuando proceda".*(La traducción es nuestra).

- Artículo 83.2.e) RGPD:

· Toda infracción anterior cometida por el responsable del tratamiento:

Hay que señalar que el considerando 148 del RGPD añade que ha de referirse a *"cualquier infracción anterior pertinente"* o "*relevante*" de la traducción del texto original en inglés "relevant".

Por ello, solo consideramos un procedimiento en el que se ha sancionado a ORANGE (resolución firme en vía administrativa) como consecuencia de los tratamientos efectuados sin legitimación resultantes de un fraude de identidad.

Núm. procedimiento	Fecha resolución sancionadora	Infracción imputada	Sanción
PS/00452/2019	23/06/2020	6.1 RGPD	80.000,00

- Artículo 83.2.g) RGPD:

  · Categorías de datos personales afectados por la infracción:

  ORANGE aduce que sólo se han visto afectados datos básicos de los clientes y que la tarjeta SIM no es un dato de carácter personal, ya rebatimos este argumento en el FD Cuarto.

  La Agencia considera el acceso no autorizado a un duplicado de tarjeta SIM se considera particularmente grave ya que posibilita la suplantación de identidad. De ahí que consideremos los datos sustraídos como de naturaleza sensible.

  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.

  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 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 insertada la tarjeta SIM duplicada.

  En este sentido, traer de nuevo a colación la ya citada SAP de Barcelona núm. 390/2019 de 30 de mayo.

- 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 ORANGE 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 en el “Antecedente OCTAVO”, que posiciona a ORANGE como una de las tres 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:

(…).

Igualmente, prevé compensaciones por los daños sufridos.

- Artículo 83.2.f) RGPD:

· Grado de cooperación con la autoridad de control:

Alto.

La Agencia considera que ORANGE ha cooperado de forma favorable con la investigación, proporcionando respuesta a los requerimientos y formando parte del GT, 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 ORANGE 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 ORANGE, 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.

Pasa a tenerse en cuenta el siguiente atenuante:

- Artículo 83.2. j) RGPD:

En lo relativo a la adhesión a mecanismos de certificación aprobados con arreglo al artículo 42.

ORANGE dispone del Certificado de conformidad con el Esquema Nacional de Seguridad.

Se desestiman las alegaciones aducidas en relación con el artículo 83.2.a), b), d) y g) del RGPD en los términos anteriormente dispuestos.

Asimismo, se descarta como factor atenuante el 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 apre-*

ciarse 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 último, ORANGE solicita que se sustituya la multa por "*la adopción de las medidas correctivas contempladas en el referido artículo 58, consistentes en la advertencia o apercibimiento al responsable del tratamiento y la imposición de la obligación de adopción de medidas para realizar los tratamientos "de una determinada manera y dentro de un plazo especificado".*

Esta petición debe ser asimismo desestimada. La comprensión del sistema correctivo previsto en el RGPD que plantea ORANGE es errónea.

El artículo 83.2 del RGPD 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)".*

Idéntica previsión se comprende en el artículo 58.2 del RGPD relativo a los poderes correctivos de las autoridades de control, en cuyo apartado i) dispone: *"imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular".*

En el mismo sentido, el considerando 148 del RGPD señala que: *"A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas".*

Esto significa que las multas administrativas se imponen a título adicional, esto es, se impone una multa además de una de las medidas correctivas previstas en el artículo 58.2. letras a) a h) y j) del RGPD. O, que las multas administrativas se imponen a título sustitutivo de las medidas correctivas precitadas, o sea, se impone una multa sustituyendo a una o varias de esas medidas. Así, la multa no es sustituida por una de las medidas correctivas, en su caso, sino al contrario.

A mayor abundamiento, el considerando 148 del RGPD prevé que: "*En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento".* Esta previsión conlleva la necesaria imposición de una multa en todo caso, amén de otras medidas correctivas que adicionalmente se pudieran establecer, si la infracción es considerada grave a los efectos del Reglamento en atención a las circunstancias fijadas en el citado considerando y en el artículo 83 del RGPD.

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 ***ORANGE ESPAGNE, S.A.U.***, con NIF ***A82009812***, 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 700.000'00 euros (setecientos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a ***ORANGE ESPAGNE, S.A.U.***

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 Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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 interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la AEPD, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el artículo 16.4 de la 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