- **Procedimiento N.º: PS/00021/2021**

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: 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

SEGUNDO: ***A.A.A.*** (en adelante, la parte reclamante uno), en fecha 12 de diciembre de 2019, interpone una reclamación ante el Registro General del Consell Comarcal de ******LOCALIDAD.1***, que es registrada en la AEPD en fecha 13 de diciembre de 2019, dirigida contra **TELEFÓNICA MÓVILES ESPAÑA, S.A.U.**, con CIF A78923125 (en adelante, TME), por los siguientes motivos:

> *"El 06/03/2019 se hizo un duplicado de la tarjeta SIM* ******TELÉFONO.1*** *en el establecimiento* ***THADER TELECOMUNICACIONES*** *de* ******LOCALIDAD.2****, sin mi consentimiento, a las 18:45:41. Por medio de este duplicado han podido acceder a mi cuenta bancaria, perjudicándome económicamente. Solicito que sancionen esta utilización de datos sin consentimiento."*

Junto a la reclamación aporta la denuncia presentada por estos hechos, en fecha 8 de marzo de 2019, con número de diligencia ******DILIGENCIA.1*** ampliativas de las diligencias ******DILIGENCIA.2*** -relativas a otra denuncia anteriormente presentada por unos hechos similares-, ante los Mossos d'Esquadra USC de ******LOCALIDAD.3*** (Barcelona) en la que denuncia que: *"(…) le han vuelto a duplicar la tarjeta SIM de su móvil* ******TELÉFONO.1*** *y esta vez, han accedido a su banca online del BBVA y han realizado dos transferencias por valor total de 28.000 euros. (…) Que la cuenta corriente final que recibe las transferencias es la* ***ES00 0000 0000 0000 0000 0000*** *del BBVA a nombre*

*de **B.B.B.**. (…) Que precisamente, desde el 6 de marzo de 2019 por la tarde, el denunciante se quedó con el móvil inoperativo. (…) Que presentará una reclamación a Movistar por este motivo también ya que es la segunda vez que le realizan un duplicado de su tarjeta SIM sin su autorización ni DNI físico."*

Asimismo, aporta copia del email enviado desde el correo electrónico ******EMAIL.1*** para TE_SOPORTE COMERCIAL, con el siguiente tenor:

"*Buenas*,

*Este cliente, viene por primera vez el día 07/02, que le habían llamado de *****PROVINCIA.2**, que un hombre iba por las tiendas queriendo hacer un duplicado de su línea. Y que creía que ya no tenía línea en el *****TELÉFONO.2**, evidentemente, entramos en CTC y le habían hecho desde MOVISTAR CARREFOUR *****PROVINCIA.1** UN DUPLICADO EL DIA 5/02/2019.*

*Él vive en *****LOCALIDAD.4**, un pueblo cerca de *****LOCALIDAD.3**, en la provincia de Barcelona.*

*HICIMOS duplicado otra vez del *****TELÉFONO.2** y aparte hicimos un número nuevo, que es el *****TELÉFONO.1**, el cliente fue al banco y a cambio (sic) el número de contacto por el nuevo en todos los sitios, por si acaso. Pero la sorpresa ha sido que ayer a las 18:45 le volvieron hacer lo mismo, un DUPLICADO (sic) pero del número nuevo, el *****TELÉFONO.1** y esta vez lo han usado para vaciarle 28.000 euros de su cuenta bancaria.*

Reclama que se le pida siempre el DNI ORIGINAL Y UNA CLAVE PARA HACER QUALQUIER TRAMITE, POR TELEFONO O EN TIENDA. Que se ponga una nota EN CTC INFORMÁNDOLO. y sobre todo quiere estar tranquilo que si no es el nadie pueda hacer nada a su nombre

Y reclama que se le devuelvan los dos duplicados en factura, ya que es cosa de un trabajador de movistar que está haciendo duplicados sin pedir identidad original.

*El cliente quiere saber esta vez si también ha sido en el Carrefour de *****PROVINCIA.1**, pero como no entraron en CTC, no aparece el HISTÓRICO DE AYER y a mí no me deja ver quien le hizo el duplicado.*

ADJUNTO LA PRIMERA DENUNCIA, EL PRIMER DUPLICADO Y LA ALTA DEL NUMERO NUEVO QUE HICIMOS EL DIA 7/02.

LAS FACTURAS DEL DUPLICADO DEL DIA 7/02 Y DEL DIA 7/03 PARA SU DEVOLUCION Y LOS JUSTIFICANTES DEL BANCO DONDE APARECE EL NOMBRE DE LA PERSONA QUE LE HA HECHO LA SUPLANTACION DE IDENTIDAD. Y LOS IMPORTES QUE LE HAN QUITADO.

DNI I CONTRATOS FIRMADOS."

Asimismo, aporta una impresión de pantalla del duplicado de la tarjeta SIM expedido en fecha 6 de marzo de 2019, respecto al número de abonado ******TELÉFONO.1.***

En fecha 16 de diciembre de 2019, la parte reclamante uno, presenta nuevo escrito ante el Registro General del Consell Comarcal de ******LOCALIDAD.1***, que es registrado en la AEPD en fecha 17 de diciembre de 2019, mediante el cual aporta una denuncia presentada en fecha 7 de febrero, con número de diligencia ******DILIGENCIA.2*** ante los Mossos d'Esquadra USC de ******LOCALIDAD.3*** (Barcelona) en relación, por una parte, a un intento de suplantación de identidad en 5 tiendas de Movistar de ******PROVINCIA.2*** para obtener un duplicado de su tarjeta SIM respecto al número de abonado ******TELÉFONO.2*** y por otra parte, en relación a la expedición de un duplicado de su tarjeta SIM el día 6 de febrero de 2019, en un Carrefour de ******PROVINCIA.1**. Respecto a esta última expedición aporta el código de distribuidor ******CÓDIGO.1*** y el número de agente responsable de dicha expedición: ******AGENTE.1***.

Asimismo, aporta una impresión de pantalla del duplicado de la tarjeta SIM expedido en fecha 5 de febrero de 2019, respecto al número de abonado ******TELÉFONO.2.***

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 22 de enero de 2020, se dio traslado de la reclamación a TME y a THADER TELECOMUNICACIONES, S.L. (en lo sucesivo, THADER), para que procedieran a su análisis y dieran respuesta en el plazo de un mes.

En respuesta a dichos requerimientos, THADER, manifestó -entre otros argumentos- lo siguiente:

> *"(…) 3 — Informe sobre las causas que han motivado la incidencia que ha originado la reclamación:*
>
> *El día 06/03/2019 se persona un cliente en nuestra tienda de Movistar sita en* ******DIRECCIÓN.1*** *de* ******LOCALIDAD.2*** *(*******PROVINCIA.2****), solicitando un cambio de tarjera SIM del número* ******TELÉFONO.1*** *aportando esta documentación:*
>
> - *Fotocopia del DNI del titular de la línea.*
> - *Fotocopia de denuncia por robo de DNI titular de la línea y móvil con el número* ******TELÉFONO.1.***
> - *Autorización firmada para su gestión.*
> - *Fotocopia del pasaporte de la persona autorizada.*
>
> *Dando validez a la documentación aportada se procede al cambio de tarjera SIM según la operativa de Movistar en el apartado Autorizado a tradicional".*
>
> *Según Art. 6 de RGPD Licitud del Tratamiento*
>
> *I.A El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.*

I.B El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

4 — Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares, fechas de implantación V controles efectuados para comprobar su eficacia

En vista de la forma de actuar para producir este tipo de fraude o swapping optamos en acogernos a la identificación del titular sobre la opción de SVIC (escáner), solo siendo válido el DNI original y en vigor y en presencia del titular, dejando el resto de opciones de validación no aptas.

Implantamos dichas medidas con fecha 24/01/2020, por decisión propia, por nuestro DPD y por recomendación de nuestra central sobre fraudes similares detectados a nivel nacional "Anexo 2".

Procedemos al control diario de cambios de tarjetas SIM con documentación escaneada en SVIC.

5 — Cualquier otra que considere relevante

La empresa en sus procedimientos implanta la formación a su dependencia en LOPD y RGPD al personal vía formación.

Petición a la central que nos informe de causas de fraude similares a nivel nacional.

Ponemos a su disposición nuestro registro de actividades, documento de seguridad 2016 respecto a LOPD 15/1999, ficheros inscritos anteriores a entrada en vigor del RGPD y registro de actividades permanentemente actualizado para demostrar desde un principio la colaboración y responsabilidad proactiva desde antes y después de entrada en vigor del reglamento UE 2016/679 por parte de esta dirección.

DOCUMENTACION ADJUNTA

Anexo 1 Extracto boletines identificación duplicados SIM

Anexo 2 Correo Responsable de Movistar sobre fraudes

FICHE DEFI THADER TELECOMUNICACIONES S.L

DOCUMENTO SEGURIDAD THADER TELECOMUNICACIONES

AUDITORIA INTERNA THADER TELECOMUNICACIONES, S.L

MANUAL RGPD THADER TELECOMUNICACIONES, S.L"

Por su parte, TME, no dio respuesta a este requerimiento, notificado en fecha 27 de enero de 2020, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, según certificado que figura en el expediente.

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 30 de marzo de 2020, en el expediente con núm. de referencia E/00560/2020.

TERCERO: ***C.C.C.*** (en adelante, la parte reclamante dos), en fecha 6 de marzo de 2020, interpone una reclamación ante la AEPD dirigida contra TME, por los siguientes

motivos:

"El 13 de febrero del 2020, fui víctima de duplicación fraudulenta de tarjeta SIM en la tienda CATHOME de ******LOCALIDAD.4*** *(Barcelona) que es distribuidora de Telefónica Movistar.*

Esta información (la duplicación de la SIM y el lugar) me la proporciona Telefónica cuando llamé para preguntar qué ocurría con el servicio al darme cuenta que no tenía acceso a la red.

Consecuencia de la duplicación fraudulenta, realizada por medio de suplantación de identidad, fue el robo de 18.000 euros en mis cuentas bancarias del banco Santander.

Llamé varias veces a CATHOME y al servicio de Atención al Cliente de Movistar para recabar más información de los detalles de cómo sucedió el hecho pero todo fueron evasivas. En CATHOME me dijeron que esperara a ver que podían decirme. Unas 5 horas más tarde me mandan un SMS (yo ya había recuperado mi número de teléfono) del que se deduce que reconocen que se ha producido el hecho de la duplicación pero que espere más tiempo, hasta la fecha, no se han vuelto a poner en contacto conmigo. ¿cómo se realizó el proceso de identificación al ladrón? (yo nunca perdí mi DNI ni mis tarjetas de crédito)

¿Hay un protocolo, de obligado cumplimiento, para realizar una duplicación de tarjeta SIM? ¿la tienda siguió el protocolo? ¿Ese protocolo es el adecuado en relación al riesgo que se corre?

En mi opinión, se pueden hacer pequeñas pesquisas para asegurarse que la persona que pide el duplicado es quien dice ser y muchos de los delitos que se pueden cometer con esta clase de métodos quedarían anulados, por lo que creo que existe una clara BRECHA DE SEGURIDAD y esto es una de las razones por las que presento la presente reclamación.

Es importante tener en cuenta que no solo corre riesgo el dinero de las personas.

Mientras la duplicación fraudulenta está activa todas las llamadas, mensajes etc. Le llegan al criminal poniendo en riesgo la seguridad de los contactos de la víctima.

En mi caso, el ladrón cogía las llamadas que se le hacían a mi número de teléfono. Yo mismo, llegué a hablar con él. ¿Si solo quería robar dinero, por qué cogía las llamadas?

También pongo esta reclamación para que, si fuera el caso, sancionen a la tienda CATHOME y/o Telefónica Movistar. (…)."

Junto a la reclamación aportó dos denuncias presentadas ante el Puesto P. de las Rozas de la Comandancia de la Guardia Civil de Madrid, en fecha 13 de febrero de 2020, con número de atestado ******ATESTADO.1*** y en fecha 18 de febrero de 2020, con número de atestado ******ATESTADO.2.***

En la primera de ellas denuncia que:

*"(…) se ha realizado un duplicado de la tarjeta SIM del teléfono *****TELÉFONO.3** no autorizado por el denunciante, que el denunciante sobre las 13:00 al realizar una llamada desde su teléfono este no le permite realizar la misma.*

*Que empieza a realizar gestiones, se pone en contacto con TELEFONICA MOVISTAR los cuales le informan que ha realizado un duplicado de tarjeta EN UNA TIENDA DE MOVISTAR sita en *****DIRECCIÓN.2** de la localidad de *****LOCALIDAD.5**. Que el denunciante le informa que él se encuentra en Madrid y es imposible que haya autorizado ningún duplicado.*

Que al tener sospechas fundadas de que esto no era normal realiza comprobaciones en su cuenta bancaria DEL BANCO SANTANDER la cual se encuentra a su nombre, observando varios cargos en la misma no autorizados, siendo estos los siguientes:

Han realizado una compra en la empresa REVOLUT por valor de 2.500 euros
Han realizado una compra en la empresa REVOLUT por valor de 3.500 euros.

*(…) que recibió un mensaje el lunes 3 de febrero de su banco de (…) su gestor del banco Santander pidiéndole que se pusiera en contacto con el teléfono *****TELÉFONO.4** y que el 10 recibió una llamada del departamento antifraude del Banco Santander informándole que había un intento de manipulación de cuentas desde *****PAÍS.1**, que fue al banco y cambió las claves."*

En la segunda de ellas denuncia que:

"(…) quiere ampliar los datos de los cargos sufridos en su tarjeta ya que le han realizado más cargos de los que no estaba informado el día que hizo la denuncia.

*Que el 13 de febrero de 2020 cuando revisaba sus cuentas observa que le han realizado unos cargos los cuales no ha realizado ni autorizado en su cuenta bancaria *****CUENTA.1** y número de tarjeta asociada *****CUENTA.2**, por un valor de:*

Empresa REVOLUT, 13-02.2020, por valor de 2.500 euros
Empresa REVOLUT, 13-02.2020, por valor de 5.500 euros

*Que ese mismo día le han realizado el mismo procedimiento en otra cuenta que tiene con la entidad bancaria *****ENTIDAD.1** número de tarjeta asociada *****TARJETA.1**, por un valor de:*

Empresa REVOLUT, 13-02.2020, por valor de 2.450 euros
Empresa REVOLUT, 13-02.2020, por valor de 3.500 euros"

En fecha 8 de junio de 2020, se dio traslado de la reclamación a TME, para que procediera a su análisis y diera respuesta en el plazo de un mes.

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

"(…) 3. Informe sobre las causas que han motivado la incidencia que ha originado la
reclamación.

En relación a los hechos reclamados, TME informa de que existe una solicitud de *cambio de ICC de la tarjeta SIM del Reclamante el día 13 de febrero de 2020 a las 11:48 horas a 2 través de uno de nuestros* ***(…)****, y en concreto, de la* ***(…) ***LOCALIDAD.4****".*

Revisado el caso y pese a que TME cuenta con una operativa adecuada y conocida por todos nuestros agentes sobre cómo actuar ante una solicitud de cambio de tarjeta SIM y que se detallará más adelante, en este caso en concreto se ha podido determinar que ***(…).***

Ese mismo día a las 17:12 horas, tal como explica el Reclamante en su escrito de reclamación, se solicita otro cambio de ICC para recuperar su línea. Esta solicitud se hace en el ***(…)****, que se adjunta como Anexo 2. Tal como fue trasladado en el marco del requerimiento de información con ref.* ***REFERENCIA.2*** *de la AEPD, TME cuenta con una operativa adecuada sobre el cambio de tarjetas SIM. (…)*

Por tanto y en conclusión, en este caso en concreto en el que se ha visto afectado tan solo una persona se ha podido determinar que ***(…).***

4. Informe sobre las medidas adoptadas. Indicar que a todo el personal de la marca Movistar se le exige acceso y cumplimiento de todos los procedimientos establecidos para realizar y entregar duplicados de SIM a través de nuestro ***(…)****. Por ello, se han realizado refuerzos y recordatorios de la operativa de cambios de duplicados de SIM, así como la publicación de una comunicación de concienciación y sensibilización sobre los cambios de tarjeta SIM. (…)"*

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 24 de septiembre de 2020, en el expediente con núm. de referencia E/03543/2020.

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 cuatro requerimientos de información dirigidos a TME, en distintas fechas:

Requerimiento	Código Seguro de Verificación	Fecha requerimiento	Fecha notificación requerimiento

Primero	***CSV.1***	13/01/2020	15/01/2020
Segundo	***CSV.2***	06/03/2020	09/03/2020
Tercero	***CSV.3***	29/06/2020	06/07/2020
Cuarto	***CSV.4***	17/09/2020	21/09/2020

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 6 de marzo de 2020, se solicitaba la misma información citada en el requerimiento anterior, de fecha 13 de enero de 2020.

En el tercer requerimiento, de fecha 29 de junio de 2020, se solicitaba la siguiente in-

formación:

PUNTO 1

Se solicita aclaración sobre los siguientes aspectos con relación a la contestación de nuestro requerimiento de fecha 6 de marzo de 2020, en el marco de este mismo expediente:

A). En el caso de la marca MOVISTAR se indica que solo es posible la solicitud presencial en tienda. Se pide información sobre si en algún caso excepcional se tramita de forma telefónica u online, siempre hablando de clientes particulares (residenciales)

Se pide, en caso afirmativo, copia del procedimiento por escrito donde consten todos los casos que se tramitan no presencialmente, incluyendo todos los supuestos o circunstancias.

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

B). En el caso de las autorizaciones o representaciones para tramitaciones presenciales en tienda se pide información sobre los controles que se realizan sobre la copia del documento de identidad (del cliente que autoriza o representado). Información sobre si queda almacenada la imagen del documento de identidad del solicitante, la autorización o acreditación de representación, y la copia del documento del cliente.

C) En las entregas a domicilio, se pide información sobre la posibilidad expresada del cambio de la dirección de entrega de la SIM, tanto durante la solicitud de cambio de SIM, como de forma previa al cambio de SIM en gestión independiente, y sobre los controles establecidos para realizar el cambio de este dato.

D). En O2 y TUENTI Información sobre los controles establecidos para tramitar el cambio de dirección de correo electrónico de un usuario.

Implicaciones que puede tener un cambio de dirección de correo electrónico en la
solicitud o activación fraudulenta de un nuevo duplicado de SIM. Información sobre si la dirección de correo electrónico es coincidente con el código de usuario para las apps/webapps, o si se utiliza durante la tramitación de cambio de SIM.

E). Para los casos de entrega de la SIM por ***(…)***,o empresas de mensajería:

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 o instrucciones al respecto 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 MOVISTAR. 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) Motivo por el cual fue posible el duplicado de SIM para cada caso. Acreditación de los controles que se pasaron, para cada caso, sobre la identidad del solicitante en la solicitud presencial en tienda. Copia del Documento de identidad presentado y controles que se le pasaron, o resultado de la validación con código QR .

B) Motivo por el cual fueron posibles dos duplicados de SIM consecutivos para este cliente. Información sobre el tipo de contrato del cliente.

C) 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 realizado alguna actuación con el distribuidor o tienda.
- Si se ha contactado con el cliente para alertarle de lo sucedido y sobre la resolución de su caso.

En el cuarto y último de los requerimientos, de fecha 17 de septiembre de 2020, se solicitaba la siguiente información:

PUNTO 1

Sobre el listado de 20 casos de duplicados de SIM denunciados/reclamados (que se da por íntegramente reproducido en este acto de trámite):

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

B. Para los casos de solicitud telefónica:

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

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

C. Información general sobre la casuística de "apropiación indebida del SIM":

- Información concreta sobre si los SIM fueron sustraídos de un punto de venta o cómo se produjo esa apropiación indebida.

- Información sobre si es posible adquirir SIMs sin asociarlos a ninguna línea o cliente. Causas por las que se permite que un cliente se lleve de una tienda un SIM sin activar y sin asociar a una línea determinada, y se permite posteriormente activar telefónicamente dicho SIM y asociar a una línea.

  Información si existe esta posibilidad, sin fraude de SIM swapping, consistente en la activación de un SIM que esté en posesión de un cliente, sin haber sido asociado previamente en los sistemas de la entidad a una línea de su titularidad.
- Causas por las que se permite en el procedimiento activar telefónicamente un SIM cualquiera para una línea determinada. (Caso de posibles SIMs sustraídos en una tienda, que se encuentran sin asociar con cliente alguno o línea).

- Política de seguridad que se pasa al solicitante en la recogida del SIM cuando no se asocia a una línea o cliente durante su recogida.

QUINTO: Con fecha 10 de marzo de 2020, TME solicita una ampliación del plazo ante la imposibilidad de recabar y estructurar la información requerida en el plazo establecido.

Con fecha 12 de marzo de 2020, la Subdirectora General de Inspección de Datos acuerda la ampliación del plazo para responder por un periodo de cinco días, a partir del día siguiente a aquel en el que finalice el primer plazo otorgado.

SEXTO: En respuesta a los cuatro requerimientos formulados, TME aporta la siguiente información, que fue objeto de análisis por esta Agencia:

1.- Información sobre las vías de que disponen los clientes para solicitar un duplicado de tarjeta SIM:

Clientes de la marca Movistar

(…).

2.- Información detallada del procedimiento:

(…):

Marca MOVISTAR:

(…).

MARCA O2

(…).

MARCA TUENTI

(…).

3.- Instrucciones giradas al respecto al personal que atiende las solicitudes:

(…).

4.- Información sobre si la realización de los controles queda reflejada:

Marca Movistar.

(…).

Marca O2.

(…).

Marca Tuenti.

(…).

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

(…).

6.- Acciones emprendidas por la entidad cuando se detecta uno de estos casos:

Los representantes de la entidad han manifestado desarrollar las siguientes acciones al respecto:

(…).

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

(…).

El número total de clientes de las marcas Movistar, Tuenti y O2 a cierre enero 2020 era de 8.142.352 clientes.

Respecto a la información solicitada relativa a los casos adicionales no presentados ante esta Agencia, manifiesta lo siguiente:

(…).

para las SIM solicitadas como recogidas presencialmente en tienda, los representantes de TME manifiestan:

(…).

Requerida la grabación de la conversación para los casos telefónicos, en las que el solicitante supera la política de seguridad, no las aportan, manifestando los representantes de la entidad lo siguiente:

(…).

Se ha solicitado a TME el detalle de las circunstancias que concurrieron para acceder a la tramitación de la solicitud telefónica, no respondiendo los representantes de la entidad porqué se tramitó telefónicamente, indicando que en 5 de los casos:

(…).

Se ha solicitado a TME información sobre si es posible adquirir tarjetas SIM sin asociarlas a ninguna línea o cliente así como las causas por las que se permite que un cliente se lleve de una tienda una SIM sin activar y sin asociar a una línea determinada, y se permite posteriormente activar telefónicamente dicha SIM y asociar a una línea. Los representantes de la entidad han contestado aportando la siguiente información:

(…).

Respecto a la información solicitada relativa a los casos presentados ante esta Agencia, manifestó lo siguiente:

- Expediente E/00560/2020:

  El primer duplicado, de la línea ******TELÉFONO.2***, nunca llegó a efectuarse al completo, ya que el distribuidor no llegó a entregar la tarjeta SIM al suplantador. El agente comercial que atendió la solicitud detectó que la documentación aportada por el suplantador no pasaba los ***(…)*** y, la tarjeta SIM que se utilizó para hacer el duplicado continua en la tienda del distribuidor. Aportan fotografía de la tarjeta SIM, indicando que su numeración ICC (***XXXXXXXXXXXXXXX***) coincide con la asignada a la línea. Aportan impresión de pantalla con la ICC asignada.

Según manifestaciones de los representantes de TME en el segundo caso (duplicado de la línea ***TELÉFONO.1**), el duplicado fue posible por la concurrencia de las siguientes circunstancias:

(…).

Sobre el motivo por el cual fueron posibles dos duplicados de SIM consecutivos para este cliente. Información sobre el tipo de contrato del cliente, los representantes de la entidad han manifestado que

(…).

Posteriormente el caso se deriva al ***(…)***, quien investiga el supuesto para aclarar lo sucedido y trasladar las conclusiones de su estudio al ***(…).***

En este caso no se implementaron estas medidas porque ***(…).***

Los representantes de TME indican que en caso ***(…). Los*** estudios de investigación de Prevención del Fraude nos ayudan a definir nuevos modelos o escenarios de fraude, a fin de reforzar nuestras operativas y mejor de manera constante las medidas de seguridad implantadas y los procesos de identificación de clientes.

(…).

Indican respecto a las investigaciones internas para esclarecer los hechos que cuando se ha tenido constancia del caso, internamente se ha consultado en todos los sistemas de TME las distintas actuaciones sobre las líneas del cliente para esclarecer lo ocurrido.

Asimismo, se ha contactado con los interlocutores territoriales habituales para ponerles sobre aviso, recabar más información y reforzar la operativa con las tiendas implicadas.

En cuanto a la realización de alguna actuación con el distribuidor o tienda, manifiestan con carácter general que con toda la red de tiendas se han realizado diversos refuerzos sobre ***(…)***, así como de ***(…)***. Cuando tienen constancia de algún caso de SIM SWAPPING ***(…)***.

En relación con los cambios realizados en el procedimiento para evitar casos futuros, indican que ***(…).***

Por último, respondiendo a la cuestión de si han contactado con el cliente, indican que, ***(…).***

- Expediente E/03543/2020:

No aportan DNI ni documento de solicitud de cambio de SIM. Los representantes de TME han manifestado que, revisado el caso y pese a que TME cuenta con una operativa adecuada y conocida por todos los agentes sobre cómo actuar ante una solicitud de cambio de tarjeta SIM, en este caso en concreto se

ha podido determinar que ***(…).***

En el mismo día, el reclamante solicita otro cambio de ICC para recuperar su línea.

Esta solicitud se hace en ***(…),*** y en este caso sí se siguió la operativa de TME ***(…),*** que adjuntan.

Indican que a todo el personal de la marca Movistar ***(…).***

SÉPTIMO: ***D.D.D.*** (en adelante, la parte reclamante tres), en fecha 23 de octubre de 2020, interpone una reclamación ante la AEPD dirigida contra TME, por los siguientes motivos:

"El 25/09/2020 a las 14:40h recibo un correo electrónico de Movistar indicándome que mi servicio de Movistar Cloud había sido dado de baja a lo que respondí a las 14:53 diciendo que yo no había cancelado nada y que era un error o un uso no autorizado. (…)

El 25/09/2020 a las 14:58h llamo al 1004 de Movistar para intentar aclara la baja, pero como suele ser habitual no logro contactar con nadie y la llamada se corta. Dicha llamada duró 4m 17seg y todos estos datos quedaron registrados en mi móvil.

Ese mismo día y ya por la tarde noté cosas extrañas en mi móvil, tenía un mensaje de que "el móvil estaba perdido" y pasadas las 20:00h ya no tenía señal y no podía efectuar ni recibir llamadas. Entré literalmente en pánico ya que sospeché con fundamento que mi móvil había sido secuestrado (hackeado) o similar. Ayudado por mi esposa con su móvil (que no es de Movistar) y el fijo empezamos una serie de llamadas angustiosas a mis entidades bancarias para bloquear todo. En paralelo y desde el fijo llamé al ***XXXX*** *y aunque me costó varios minutos logré explicar lo que ocurría y solicité a la desespera que anulasen mi nº de móvil ante la confirmación del Banco Santander que ya mi cuenta había sido asaltada y me habían hecho cargos fraudulentos con la tarjeta de crédito. Mi sorpresa e indignación fue indescriptible cuando me dijeron que no podían hacer nada ya que ese número, el mío* ******TELÉFONO.5*** *(y todo el resto del contrato) estaban a nombre de otra persona.*

Cuando conseguí bloquear todas las cuentas bancarias volví a llamar a Movistar y me dijeron igualmente que no podían hacer nada y que para aclarar lo sucedido y recuperar mi señal (desactivar el SIM del impostor y activar el mío) tendría que ir a una tienda de Movistar. (…)

A las 10:00h del 26/09/2020 me presenté en la tienda de Movistar de las Rozas cercana a mi domicilio y aunque me conocían perfectamente como cliente habitual me dijeron que no podían hacer nada ya que mi móvil (y demás servicios) estaba a nombre de otra persona y me proporcionaron un documento como prueba.

Me remitieron a la central de Telefónica en Gran Vía para desbloquear la situación (…)

Estuve en las dependencias de Gran Vía desde las 11:00 hasta las 13:00 aproxi-

madamente y aporté el documento fraudulento mencionado, mis recibos mensuales de Telefónica Movistar en pdf en una llave USB desde 1998, así como copia en papel del último recibo de Movistar. Ante la evidencia de pruebas Movistar decidió anular el SIM fraudulento y activó el mío.

La conclusión de la propia Movistar fue muy clara: el impostor cambió fraudulentamente el contrato a su nombre (posiblemente vía telefónica según Movistar aunque sin confirmar) y después fue a una tienda de Movistar donde pidió un duplicado del SIM. No encontró problemas ya que en el ordenador de la tienda estaba a su nombre y posteriormente anuló el otro, el mío, y ya entró en mis cuentas bancarias. El procedimiento fue relativamente simple: entró en mi cuenta con mi DNI (posiblemente lo obtuvo del contrato mío) pulsó "contraseña perdida u olvidada" y en esos casos el banco envía SMS con códigos de seguridad que una vez introducidos correctamente dan acceso a contraseñas, etc. (…)

*Conclusión: Movistar cambió mi contrato de Movistar Fusión (fijo, móvil y televisión) a nombre de otra persona (…) sin proteger mis datos lo que además dio origen a una estafa de **XXXXX** euros."*

Junto a la reclamación aporta el correo electrónico recibido en fecha 25 de septiembre de 2020 y el de respuesta; copia de la orden de reparación de fecha 26/09/2020; y dos denuncias presentada ante el Puesto P. de las Rozas de la Comandancia de la Guardia Civil de Madrid, en fecha 28 de septiembre de 2020, con número de atestado ***XXX-XXXXXXXX*** y en fecha 2 de octubre de 2020, con número de atestado ***XXXXXXXXX-XXX.***

En la primera de ellas denuncia que:

*"En la tarjeta de debido le han sido realizados un total de tres cargos, sustrayendo un total de **XXXX** euros.*

*En la tarjeta de débito le han realizado un total de seis cargos, sustrayendo un total de **XXXX** euros.*

*También le han realizado una transferencia a través de BIZUM de 500 euros, destinado a un tal **E.E.E.** con número de teléfono ******TELÉFONO.6*** y una recarga bancaria de **XXXX** euros.*

*Todo esto hace un total de **XXXX** euros.*

*El denunciante manifiesta el posible modus operandi del autor: Que a través de un de un cambio de nombre del titular en su contrato, para la línea perteneciente al número *****TELÉFONO.5,** con MOVISTAR vía telefónica, sin su consentimiento, el posible autor realizó el cambio, solicitando una tarjeta SIM a dicha empresa. Anulando la tarjeta SIM del denunciante.*

Que tras obtener dicha tarjeta SIM el autor realizó los movimientos bancarios a través de un teléfono móvil, debido a que tras realizar cualquier operación con la entidad bancaria, necesita la aprobación vía SMS del número de teléfono que realiza la operación.

Tras esto el posible autor se metió en la aplicación de la entidad bancaria Santander y a través de HE OLVIDADO MI CONTRASEÑA, dicho banco le envía SMS al número de teléfono asociado a la cuenta bancaria.

Que el cambio de titular de la cuenta de MOVISTAR, el denunciante aporta datos del posible autor: ***F.F.F. ***NIE.1****.

Además aporta una transferencia bancaria de ***XXXX*** *euros que se anuló, la cual iba dirigida a un tal* ***G.G.G.****(…).*

Que el denunciante aporta el contrato fraudulento de MOVISTAR con nombre y apellidos del presunto autor, copia de la última factura del contrato legal del denunciante, datos de la transferencia abortada y los cargos realizados."

En la segunda de ellas denuncia que:

"(…) Que el día 01-10-2020 jueves el denunciante se personó en su oficina del Banco Sabadell sita en (…) para recuperar las claves previamente bloqueadas para poder operar.

Que el Banco Sabadell informó que lamentablemente se había emitido una transferencia fraudulenta por importe de 7.003'00 euros a nombre de ***H.H.H.*** *a la cuenta* ***ES00 0000 0000 0000 0000 0000*** *de la entidad bancaria ING motivo por el que se ve obligado a denunciar los hechos para poder recuperar la cantidad defraudada.*

El denunciante manifiesta el posible modus operandi del autor", donde reproduce las mismas manifestaciones informadas en la denuncia anterior.

En fecha 25 de noviembre de 2020, se dio traslado de la reclamación a TME, para que procediera a su análisis y diera respuesta en el plazo de un mes.

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

"(…) 3. Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.

El Sr. ***D.D.D.*** *en el escrito presentado ante esta Agencia indica que, es cliente de la marca comercial Movistar con la que mantiene contratadas tres líneas, una fija y dos líneas móviles que son* ******TELÉFONO.6****,* ******TELÉFONO.5****,* ******TELÉFONO.7****.*

Así mismo indica que con fecha 25 de septiembre de 2020, notó que su línea ******TELÉFONO.5*** *se encontraba sin servicio, tras esto, contactó con nuestro servicio de atención al cliente en el número 1004, donde le indicaron que todas sus líneas se encontraban a nombre de otra persona.*

Posteriormente, con fecha 26 de septiembre de 2020, el cliente se personó en una de nuestras tiendas físicas, donde le explicaron que era posible que una tercera persona hubiera cambiado la titularidad de sus líneas solicitando a su vez un dupli-

cado de su tarjeta SIM para las líneas móviles.

En este sentido, tenemos que decir que, en este caso concreto, el 25 de septiembre de 2020 se produjo un cambio de titularidad en las tres líneas mencionadas anteriormente a través ***(…)****; ese mismo día, el suplantador solicita un duplicado de tarjeta SIM para las líneas móviles, pero solo hace efectivo el cambio en la línea* ******TELÉFONO.5****.*

En cuanto a la causa que ha producido la reclamación, tenemos que indicar que ***(…)****.*

A este respecto, informamos de que Telefónica cuenta con un procedimiento consolidado y adecuado de verificación de la identidad de nuestros clientes que reviste de las garantías suficientes para identificar al solicitante del cambio de titular antes de proceder a la tramitación del mismo. En este procedimiento de verificación de identidad se solicitan, además de ***(…)****.*

No obstante, lo anterior, Telefónica trabaja continuamente en la mejora de las medidas de las que dispone con el objetivo de evitar la suplantación de identidad en los distintos procesos de contratación y posteriores gestiones que soliciten los titulares de los servicios a través de los distintos canales de los que dispone. De este modo, se han reforzado los diferentes procesos, que detallaremos en el siguiente punto.

En relación con los hechos descritos, esta compañía informa de que los hechos denunciados ya han sido tratados y solucionados con anterioridad a la entrada de la denuncia ante la Agencia de Protección de Datos.

En cuanto a las actuaciones llevadas a cabo por Telefónica en la resolución de la reclamación planteada, confirmamos que:

- *A fecha de este escrito, las líneas se encuentran regularizadas a nombre del titular original, hoy reclamante, el Sr.* ***D.D.D.***
- *La línea afectada* ******TELÉFONO.5****, cuenta con una nueva tarjeta SIM asociada correctamente al titular de la línea.*
- *Nuestro equipo de prevención del Fraude ha contactado con el titular para informarle sobre el cambio de tarjeta SIM de la línea* ******TELÉFONO.7*** *que resulta necesario llevar a cabo para regularizarla igualmente.*

4. Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.

Durante el año 2020 se han implementado las siguientes medidas específicas que afectan a las operativas de los canales:

(…).

Sobre dicha reclamación recayó resolución de ADMISIÓN A TRÁMITE de fecha 25 de enero de 2021, en el expediente con núm. de referencia E/09638/2020.

OCTAVO: Con fecha 27 de agosto de 2020, se obtiene información de la Comisión

Nacional de los Mercados y la Competencia sobre las líneas de telefonía móvil de voz por tipo de contrato y por segmento siendo los resultados:

OPERADOR	PREPAGO		POSPAGO	
	Residencial	Negocios	Residencial	Negocios
Movistar	1.215.667	0	10.048.727	5.102.197

NOVENO: Con fecha 27 de enero de 2021, se obtiene información comercial sobre el volumen de ventas de TME durante el año 2019 siendo los resultados de 4.340.283.000,00 euros. El capital social asciende a 209.404.687,00 euros.

DÉCIMO: Con fecha 11 de febrero de 2021**,** la directora de la AEPD acuerda iniciar un procedimiento sancionador contra TME, 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 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.

Con fecha 15 de febrero de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, se notifica el Acuerdo de Iniciación.

UNDÉCIMO: Con fecha 17 de febrero de 2021, TME solicita la ampliación del plazo para aducir alegaciones y aportar documentos u otros elementos de juicio, y, la remisión del expediente PS/00021/2021 y del resto de expedientes referenciados.

DUODÉCIMO: Con fecha 17 de febrero de 2021, la instructora del procedimiento acuerda la ampliación de plazo instada hasta un máximo de cinco días y con fecha 23 de febrero de 2021, la remisión de la copia del expediente, de acuerdo con lo dispuesto en los artículos 32.1 y 53.1 a) de la LPACAP.

DÉCIMO TERCERO: Con fecha 22 de febrero de 2021, TME comunica la modificación de la dirección postal para la remisión del expediente sancionador PS/00021/2021 y del resto de expedientes referenciados.

DÉCIMO CUARTO: Con fecha 22 de febrero de 2021, se notifica a TME el Acuerdo de ampliación de plazo y con fecha 25 de febrero de 2021, la remisión de la copia del expediente.

DÉCIMO QUINTO: Con fecha 8 de marzo de 2021, se recibe en esta Agencia, en tiempo y forma, escrito del representante de TME, por el que se procede a formular alegaciones y en el que, tras manifestar lo que a su derecho conviene, solicita:

"i. Se suspenda el presente procedimiento y se requiera a los reclamantes a fin de que aporten en qué punto están las denuncias interpuestas, así como el contenido de los procedimientos penales que en su caso se encuentren en marcha, con el fin de determinar si existe prejudicialidad penal.

ii. Subsidiariamente y para el caso de que no se estimase la solicitud de suspen-

sión, se declare la inexistencia de responsabilidad por parte de TME por las presuntas infracciones que se le imputan en este procedimiento, ordenando el archivo del presente expediente sancionador.

iii. Por último, en caso de que no se estimasen ninguna de las pretensiones anteriores, que se minore la sanción inicialmente propuesta en virtud del art. 83 del RGPD."

En síntesis, en las alegaciones manifestó que:

PREVIA: SOBRE LA INCOACIÓN DEL EXPEDIENTE SANCIONADOR.

Considera que la sanción es desproporcionada en relación con los hechos afectados, lo que vulnera el principio de buena fe y confianza legítima que debe regir la actividad y el ejercicio de las funciones de cualquier entidad pública, según lo estipulado en el artículo 3.1.e) de la Ley 40/2015.

La AEPD convocó el 20 de enero de 2020 un grupo de trabajo (GT) con distintos operadores, así como con otros representantes, con el objetivo de "analizar los problemas de la duplicidad de las tarjetas SIM y estudiar vías y procedimientos para evitar que se produzcan", convocándose la primera reunión el 4 de diciembre de 2020.

No obstante, la AEPD decide incoar un expediente sancionador con una propuesta de sanción sin precedentes.

Además cambia el tipo infractor que habitualmente venía imputando en los casos en los que, quebrantando las medidas técnicas y organizativas establecidas por TME, los defraudadores conseguían suplantar la identidad de los clientes con distintas finalidades (art. 6.1, falta de legitimidad en el tratamiento de los datos de los interesados), y que era el reproche que en todo caso había puesto de manifiesto hasta el momento en relación con el SIM Swapping, sino que, además, imputa a TME la responsabilidad del resultado del fraude realizado por un tercero, es decir, el resultado del robo del dinero de las cuentas bancarias de dichos clientes, así como la alarma social causada por este tipo de prácticas.

I. SOBRE LOS HECHOS QUE MOTIVAN LA INCOACIÓN.

Cuestión de prejudicialidad penal.

Las tres partes reclamantes interpusieron sendas denuncias ante los Cuerpos y Fuerzas de Seguridad del Estado en relación con los mismos hechos que se están tratando en el presente procedimiento. Es indispensable constatar si las denuncias han avanzado llegando a sede de instrucción judicial, lo que supondría que no se podría continuar la vía administrativa hasta saber el resultado final de la vía penal, tal y como establece el art. 77.4 de la LPACAP.

PRIMERA. **De la operativa de identificación de clientes:**

Las medidas de seguridad son el resultado de un minucioso y continuo proce-

so de estudio que abarca múltiples disciplinas y áreas del conocimiento (entre otras, asesoría jurídica, seguridad, prevención del fraude) que ha sido llevado a cabo desde un primer momento con todas las garantías y con el máximo respeto y observancia de los principios del artículo 5 del RGPD.

El eje central de estas medidas de seguridad está constituido por la ***(…)*** que resulte aplicable en función del tipo de gestión solicitada por el cliente.

1.1.- Las medidas técnicas y organizativas implantadas resultan apropiadas en función de las características que reviste cada uno de los tipos de gestión afectados por el fraude:

Las gestiones de las que se valen los suplantadores para perpetrar los fraudes de tipo SIM Swapping son básicamente dos: las solicitudes de duplicado de tarjeta SIM y las solicitudes de cambio de titularidad.

1.1.1.- Garantías que reviste el procedimiento de solicitud de duplicado de tarjeta SIM ***(…)****:*

(…).

1.1.2.- Garantías que reviste el procedimiento de cambio de titular en el ***(…)****:*

(…).

1.2.- Las medidas técnicas y organizativas implementadas se revisan y actualizan de manera continua de conformidad al principio de privacidad desde el diseño y por defecto:

- Medidas adoptadas en el corto plazo

(…).

- Medidas adoptadas en el largo plazo

- Durante el año 2020 TME ha trabajado en el desarrollo ***(…)***.

- Adicionalmente y para el año 2021 ***(…).***

1.3.- Aclaraciones sobre el funcionamiento de los duplicados de Tarjeta:

NO es cierto que:

(…).

SEGUNDA. **Las circunstancias que han hecho posible la superación por**

terceras personas de las políticas de seguridad implantadas y la consecuente suplantación de identidad de los reclamantes uno, dos y tres superan la esfera de responsabilidad de TME.

Los agentes comerciales del ***(…)*** han sido engañados e inducidos a cometer errores humanos a la hora de aplicar la operativa de identificación diseñada y exigida por TME.

2.1.- Del incumplimiento de la operativa por parte de los empleados de distribuidores y otros proveedores:

Aportan los contratos firmados por THADER, CATPHONE y ***(…***

2.2.- De la diligencia debida demostrada por TME a la hora de hacer cumplir la operativa de Identificación:

Demostrada en todo momento, incrementando aún más sus esfuerzos desde que es conocedora de la existencia de esta modalidad de fraude. Insiste en la gran cantidad de ***(…)*** en el sentido de hacer llegar el detalle de la operativa de identificación a todos los canales.

Ha desarrollado numerosas acciones de ***(…)***. En este sentido, con objeto de reforzar el cumplimiento de la operativa diseñada por Movistar, el protocolo incluye ***(…)*** y de ***(…)***.

2.3.- De la continua innovación de las técnicas de fraude y la sofisticación de los suplantadores a la hora de perpetrar y evolucionar este tipo de fraude:

Debe tenerse presente que dichos comerciales se enfrentan a la ***(…)***, se vale de ellos para tramitar una gestión en particular conforme a los trámites establecidos para ello en TME.

2.4.- De la concurrencia de otras operativas bancarias no conocidas por TME necesarias para perpetrar el fraude bancario:

Las obligaciones de autenticación y acceso de terceros impuestas por la Directiva PSD2 no resultan de aplicación a TME y, además, no entraron en vigor hasta el 14 de septiembre de 2019. En consecuencia, TME no es responsable de los resultados de suplantación de identidad.

TERCERA. Las medidas de seguridad implantadas se han demostrado adecuadas, oportunas y eficaces en atención al volumen de contratación y a las obligaciones impuestas por la normativa sectorial aplicable para asegurar la conectividad de sus clientes de forma rápida y sostenible en el tiempo.

3.1.- Adecuación, oportunidad y eficacia de las medidas de seguridad implantadas por TME:

La AEPD únicamente ha identificado tres casos de fraude bancario (partes reclamantes uno, dos y tres).

Las solicitudes fraudulentas identificadas por TME son mínimas y completamente excepcionales si las comparamos con el volumen de operaciones de este tipo gestionadas por TME.

- Porcentaje de solicitudes fraudulentas detectadas en duplicados de tarjeta:

  Es del ***X,XXXX*** %. La imposición de restricciones supondría una rigidez y una carga excesiva que, en última instancia, podría poner en riesgo:

  ▫ La conectividad de los clientes de forma rápida y sostenible en el tiempo conforme a la normativa sectorial que impone a las operadoras un estándar de calidad y de nivel de servicio exigentes en aras de asegurar la conectividad.

  ▫ El cumplimiento de otros principios consagrados en el RGPD, como el principio de minimización de datos.

  Por otra parte, el porcentaje general de solicitudes fraudulentas de las que se valen los suplantadores para cometer los fraudes bancarios ***(…)***.

3.2.- Efectividad de determinados procesos señalados por la agencia:

3.2.1.- La efectividad del check "víctima de fraude"

No existe como tal un procedimiento de este tipo.

- **<u>Restricción por robo</u>:**

  Que consiste en ***(…).***

- **<u>Acciones llevadas a cabo por el departamento de fraude:</u>**

  Detectado un posible fraude, ***(…).***

3.2.2.- La efectividad del ***(…).***

No existe ningún ***(…).***

3.2.3.- La efectividad ***(…)***

Entre sus obligaciones como empresa prestadora de servicios de comunicaciones electrónicas se incluye la necesidad de <u>garantizar la accesibilidad a sus servicios de atención al cliente</u>.

La ***(…)*** responde al conjunto de obligaciones expuestas y, en

atención a estas, considera que no se puede poner en duda su eficacia.

II. SOBRE LOS FUNDAMENTOS DE DERECHO.

PRIMERA. Sobre las presuntas infracciones cometidas por parte de TME: vulneración del principio de tipicidad.

1.1.- Sobre la conducta de TME: en ningún caso podría considerarse subsumible en ninguno de los preceptos que se consideran vulnerados

La conducta realizada no es subsumible en ninguno de los preceptos cuya infracción se imputa, para ello sería necesario que:

- No se aplicasen unas "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

- En general, no se garantizase una "seguridad adecuada" en el tratamiento de datos personales.

- No se fuese capaz de demostrar todo lo anterior.

- Sobre la presunta infracción de los artículos 5.1 f) y 32 del RGPD:

  TME cuenta con unas medidas técnicas y organizativas apropiadas:

  ▫ Resultado de un minucioso y continuado proceso de estudio que abarca múltiples disciplinas y áreas del conocimiento (asesoría jurídica, seguridad, prevención del fraude) que se revisan y actualizan cuando es necesario.

  ▫ En relación con la evaluación de riesgos, debe tenerse en cuenta que la emisión de un duplicado de tarjeta puede resultar necesaria para que un cliente siga disfrutando de su servicio de comunicaciones móviles conforme al artículo 47 de la Ley 9/2014, de 9 de mayo (LGTEL) y el Real Decreto 899/2009, de 22 de mayo.

- Sobre la presunta infracción del artículo 5.2 RGPD:

  La norma exige demostrar el cumplimiento de la implantación de unas medidas de seguridad apropiadas, no su infalibilidad. Infalibilidad que sí parece estar exigiéndose a TME, atendiéndose tan solo al resultado producido en el caso de tres reclamantes, y asumiendo de esa forma la existencia de una responsabilidad objetiva.

- Sobre la presunta infracción del artículo 25 RGPD:

  Se está imputando a TME la infracción de un artículo que protege la privacidad en una doble vertiente: privacidad desde el diseño y por de-

fecto, sin ni siquiera referirse a su alcance total en el Acuerdo de Inicio.

● Sobre la tipificación de la presunta conducta en otros procedimientos sancionadores incoados a TME y Telefónica de España, S.A.U.

La actuación de la Agencia es arbitraria por cuanto en otros expedientes administrativos la tipificación de la conducta ha sido diferente (PS/00114/2019; PS/00453/2019; PS/00235/2020). En todos ellos se ha tipificado la conducta como contraria al artículo 6.1 RGPD.

Con este proceder, la AEPD propicia una proscrita inseguridad jurídica y dificulta una adecuada defensa de TME, vulnerando en consecuencia las previsiones del artículo 9.3 CE.

1.2.- Sobre la redacción de la normativa que resulta de aplicación: conceptos jurídicos indeterminados que contribuyen a incrementar la inseguridad jurídica e indefensión de TME:

Invoca varias sentencias: STS de 26 de junio de 2001 (RJ 2001, 5740); STC 104/2009, de 4 de mayo (RTC 2009, 104); y la STC 145/2013 de 11 julio (RTC 2013\145).

La Agencia colabora con dicha indeterminación de conceptos al hacer referencia a un supuesto "principio de seguridad de los datos" de ahora nueva formulación en varias ocasiones mencionado, pero no recogido en el RGPD.

1.3.- Subsidiariamente: sobre la interpretación y aplicación de la normativa realizada por la agencia. Riesgo de vulneración del principio "non bin in idem" y de especialidad:

El ***(…)*** exige la prioridad en la aplicación del precepto específico sobre el general. Por lo que, no resultaría aplicable a este caso ni el artículo 5.1 f) ni el 5.2 del RGPD, cuya redacción es genérica y procede la aplicación del artículo 32 del RGPD. Dicha especialidad se encuentra también recogida en la LOPDGDD, que en su artículo 73 f), a diferencia del artículo 72.1 a), prevé como infracción grave "f) *La **(…)** que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por **(…)***".

SEGUNDA. La conducta de TME no es antijurídica.

La operativa de identificación de clientes de TME contempla medidas técnicas y organizativas diseñadas para garantizar una seguridad adecuada de los datos personales de sus clientes, incluida la protección contra el tratamiento no autorizado o ilícito. La norma ***(…)*.**

Las medidas de seguridad implantadas por TME se han demostrado ***(…)*** al volumen de contratación y del resto de gestiones, y ***(…)*.**

En relación con la ***(…)***, dichos contratos responden a la realidad mercantil e incluyen todas aquellas previsiones que son necesarias con el objetivo de garantizar su cumplimiento.

TERCERO. Ausencia de culpabilidad.

No existe el elemento subjetivo de culpa requerido para la imposición de sanciones administrativas.

TME revela una inequívoca voluntad de proceder conforme a Derecho sin existir en modo alguno intencionalidad de infringir la norma y teniendo en todo caso voluntad de cumplimiento.

Invoca la STS de 16 de diciembre de 2015. Las conductas en ningún caso son imputables a TME.

3.1.- La actuación diligente, de buena fe y confianza legítima de TME:

Ha actuado con toda la diligencia exigible a la hora de implantar unas medidas técnicas y organizativas (conforme al estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, la probabilidad y gravedad de los riesgos) que resultan apropiadas para garantizar una seguridad adecuada.

Como operador de telecomunicaciones y prestador de servicios de comunicaciones electrónicas tiene la obligación de prestar dichos servicios de manera continuada y atendiendo a las obligaciones derivadas de la normativa que resulta de aplicación.

Invoca el seguimiento del “Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía” y la participación en el GT.

Alega haber actuado conforme al principio de confianza legítima e invoca la STS núm. 64/2017 de 22 de mayo.

3.2.- Circunstancias excepcionales y ajenas a TME:

- Incumplimiento de las operativas establecidas por TME: responsabilidad de los empleados de los distribuidores y proveedores

  La AEPD está exigiendo una ***(…)*** basándose simplemente en el resultado, sin tener en cuenta que ***(…)*** de los distribuidores, que en su caso estarían incumpliendo las operativas. Invoca la STS 1468/2017 de 28 septiembre.

- Posible negligencia en el cuidado de los datos personales por parte de los usuarios:

TME informa a sus clientes en el marco de su relación contractual, lo siguiente:

Condiciones de Movistar Internet: "*Uso y custodia. El CLIENTE se compromete a hacer un* ***(…)****".*

Condiciones particulares de la aplicación móvil Mi Movistar: *"2.7. Movistar no se responsabilizará por la pérdida, sustracción y/o uso no autorizado por terceros de tus credenciales o de la tarjeta SIM de tu/s línea/s vinculada/s, por lo que* ***(…)****. De igual manera,* ***(…)****. Movistar no se responsabiliza por el uso que terceros puedan hacer de Mi Movistar en tu dispositivo".*

Invoca tres Sentencias: de la Audiencia Provincial (AP) de Sevilla, de 26 de mayo de 2014; de la AP de las Palmas de Gran Canaria, de 20 de diciembre de 2012; y de la AP de Valladolid de 10 de marzo.

- Probable responsabilidad de terceros ajenos a TME, como las entidades bancarias:

Corresponde al banco (o resto de proveedores de las aplicaciones mencionadas), ***(…)***, el establecer las medidas que en su caso correspondan, atendiendo a lo establecido en la normativa que resulta de aplicación a las entidades bancarias; y decidir sobre la idoneidad de utilizar determinados mecanismos para autorizar y finalizar la transacción bancaria (en este caso el SMS).

Alude a la SAP de Alicante núm. 107/2018, de 12 marzo (AC 2018\818).

- Acciones intencionadas de terceros para la comisión de un delito

Como indica la propia Agencia, se trata de "*prácticas fraudulentas"* realizadas por terceros, de las que TME es una víctima más.

Por otro lado, también debemos hacer referencia en este punto al **engaño previo por parte del suplantador a los comerciales de TME** para conseguir realizar determinadas gestiones.

Incluso podría considerarse que nos encontramos ante un supuesto de **fuerza mayor**, por encajar las circunstancias descritas en dicho concepto, que determina **la falta de responsabilidad o culpabilidad en la conducta infractora**.

Nos encontramos ante la responsabilidad de los empleados de los distribuidores y proveedores de TME que han incumplido las operativas establecidas, pese a la más que evidente y probada actuación diligente de TME en el marco de dicha relación contractual.

La suplantación de identidad puede producirse por multitud de factores ajenos a la voluntad y capacidad de actuación de TME, tales como

que:

i).- Hay terceros que tienen la voluntad de cometer un delito, acción que resulta inevitable para Telefónica.

ii).- Los datos que permiten la suplantación de identidad no son obtenidos de TME. Los suplantadores **deben tener en su poder otros datos** (en concreto los bancos con los que operan estas personas y las credenciales de acceso a la banca on-line) ya **que el acceso a los mensajes SMS por sí solo no permite la ejecución de operaciones bancarias**.

iii).- Las entidades bancarias son las responsables de determinar las medidas de seguridad necesarias para garantizar el consentimiento del titular de la cuenta ante cualquier operación bancaria, y la acreditación de su identidad.

Por lo tanto, resulta de extraordinario interés reiterar que no hay nexo causal por acción u omisión, entre TME y el resultado final, debido a la intervención de terceros con entidad suficiente para alterarlo.

CUARTO. Incumplimiento del principio de proporcionalidad.

En el hipotético caso de que la AEPD, carente del adecuado soporte legal y con el único objetivo de imponer una multa, considere idóneo e indispensable sancionar económicamente a TME, el importe de tal sanción deberá ser estimado atendiendo en todo caso al principio de proporcionalidad.

Invoca la **STS de 2 de junio de 2003** y los **Considerandos 4, 129 y 148** y artículo **83** del RGPD.

La sanción económica que correspondería resulta de todo punto ineficaz y desproporcionada. No se han tenido en consideración las previsiones de los artículos 83.1 y 83.2 del RGPD.

4.1.- De las agravantes apreciadas:

1. Gravedad de la infracción

Alude a la **Sentencia de la Audiencia Nacional (SAN) 00496/2017**, en la que no se considera justificada ni motivada la valoración de la conducta como grave por parte de la SESIAD, en la medida en que no se apreciaba que el incumplimiento fuese generalizado.

En consecuencia, no se puede considerar que la naturaleza de la infracción sea grave.

2. Duración de los hechos.

La duración del tratamiento supuestamente irregular no podría exce-

der del momento en el que se perfeccionó el duplicado de tarjeta SIM de los tres reclamantes.

No deja de sorprender que la Agencia aprecie la agravante de duración, al entender que los hechos abarcan un periodo superior al año, y al mismo tiempo se estime como atenuante la falta de carácter continuado de la infracción.

3. Número de interesados afectados

Falta de congruencia debida en relación entre el ilícito cometido y la sanción propuesta -solo 3 casos-.

4. Nivel de daños y perjuicios sufridos

En modo alguno se puede atribuir a TME responsabilidad sobre la materialización del fraude bancario, ya que su responsabilidad termina con el resultado del duplicado de tarjeta, pero no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias.

La apreciación de la agravante contemplada en el artículo 83.2.a) no puede fundarse en la perpetración de este tipo de delitos.

5. Intencionalidad o negligencia

Los sucesos ocurridos con los tres reclamantes no pueden ser considerados como una muestra representativa del nivel de compromiso demostrado por TME y, mucho menos, del grado de eficacia que revisten unas políticas de seguridad que están diseñadas para atender a un volumen de clientes que supera los 8 millones.

6. Responsabilidad del responsable

Parece que la AEPD mezcla en su argumento a las entidades bancarias con los distribuidores.

7. Categoría de datos personales afectados

TME trata solamente datos identificativos (Nombre, apellidos, DNI).

En ese sentido, resulta evidente que la categoría de datos afectados por el fraude, no sólo no entran en la categoría de datos sensibles recogida en el art. 9 del RGPD, si no que la propia AEPD los clasifica como “datos de escaso riesgo”, según la categoría de datos personales realizada en el apartado 6.2.3 de la “Guía para la gestión y notificación de brechas de seguridad.

4.2.- De las atenuantes apreciadas:

La Agencia no ha tenido en cuenta algunas circunstancias que redundan en la aplicación de dichas atenuantes. Por otro lado, ha olvidado incluir en ese listado de atenuantes, otras que también aplican y que resultan fundamentales.

En relación con las circunstancias no tenidas en cuenta:

En relación con el artículo 83.2.c) RGPD. **Medidas tomadas por el responsable para paliar los daños y perjuicios sufridos por los interesados**: la AEPD no hace referencia a ***(…).***

En relación con el artículo 83.2.f) RGPD. **Grado de cooperación con la autoridad de control**: la AEPD tampoco hace referencia a la colaboración realizada por esta parte en el seno del GT.

En relación con el artículo 76.2.a) LOPDGDD. **El carácter continuado de la infracción**: la AEPD no tiene en cuenta el porcentaje ínfimo que suponen los casos de solicitudes fraudulentas de duplicado de SIM en relación con el volumen de transacciones que gestiona TME, y que apenas supera el 0%.

Esta parte entiende que la atenuante que contempla el artículo 76.2.d) resulta determinante a efectos de valorar una posible sanción económica. Las suplantaciones de identidad producidas en los casos de los tres reclamantes no habrían sido posibles si el suplantador no hubiese realizado una previa captación ilegítima de los datos personales de dichos clientes. (El subrayado, la cursiva y negrita es de TME).

Estas alegaciones ya fueron contestadas en la Propuesta de Resolución y se reiteran, en parte, en los FD de esta Resolución.

DÉCIMO SEXTO: Transcurrido el plazo de alegaciones concedido en el Acuerdo de iniciación y presentadas alegaciones, con fecha 4 de mayo de 2021, por la instructora del procedimiento se acuerda la apertura de un período de prueba en los siguientes términos:

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

2. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio PS/00021/2021 *presentadas por TELEFÓNICA MÓVILES ESPAÑA, 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:*

(…).

*3. Practicar con fecha de hoy, un requerimiento a: **A.A.A., C.C.C.** y **D.D.D.,** a fin de que se facilite en un plazo de 10 días hábiles, información sobre el curso de las denuncias interpuestas por estos hechos, así como información de los procedimientos penales que en su caso se encuentren en trámite."*

DÉCIMO SÉPTIMO: En respuesta a este último requerimiento:

Con fecha 25 de mayo de 2021, la parte reclamante uno aporta certificado del Juzgado de Instrucción 2 de ******LOCALIDAD.3***, en el que se sigue procedimiento de Diligencias Previas nº ***XXXXX*** por estafa, en el que figura en condición de perjudicada.

Con fecha 7 de mayo de 2021, la parte reclamante dos manifiesta no tener conocimiento de ningún dato acerca de las posibles pesquisas que se hayan podido dar a partir de la denuncia presentada.

Con fecha 21 de mayo de 2021, la parte reclamante tres manifiesta que el pasado 11 de febrero de 2021, declaró en el Juzgado de 1ª Instancia e Instrucción nº 01 de Majadahonda en el procedimiento de Diligencias Previas ***XXXXX*** en su condición de perjudicado/ofendido, en el que figura como investigado ***F.F.F.*** Añade, que amplió la denuncia inicial presentada ante la Guardia Civil en fecha 28 de septiembre de 2020. Aporta un fichero mp3, facilitado por la Oficina Municipal de Consumidores, en el que consta la grabación del cambio de titularidad del servicio a favor de este último.

DÉCIMO OCTAVO: Con fecha 21 de julio de 2021, se solicita al Juzgado de Instrucción núm. 2 de ******LOCALIDAD.3***, por correo electrónico, información sobre el procedimiento de Diligencias Previas nº ***XXXXX***, y sobre el criterio del órgano judicial respecto a la concurrencia de identidad de sujeto, hecho y fundamento entre la presunta infracción administrativa y la infracción penal que pudiera corresponder, para proceder, en su caso, a la inmediata suspensión del procedimiento iniciado, en virtud de lo preceptuado en el artículo 22 de la LPACAP.

DÉCIMO NOVENO: Con fecha 28 de julio de 2021, se recibe correo electrónico del Juzgado de Instrucción núm. 2 de ******LOCALIDAD.3***, en el que la juez informa lo siguiente:

*"En relación a la petición solicitada les informo que la denuncia presentada por el Sr. **A.A.A.** no se interpuso contra la companyia (sic) TELEFONICA MOVILES ESPAÑA SAU a pesar que en la denuncia relató que se hizo un duplicado de su targeta (sic) SIM núm. ******TELÉFONO.2** y el no lo había solicitado. En este sentido y en contestación a la petición no hay, por este motivo, identidad de sujetos que conduzca a la suspensión del procedimiento."*

VIGÉSIMO: Con fecha 16 de septiembre de 2021, la instructora del procedimiento formula Propuesta de Resolución, en la que propone que por la directora de la AEPD se sancione a **TELEFÓNICA MÓVILES ESPAÑA, S.A.U.**, con CIF A78923125, 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 1.000.000'00 (un millón de euros).

Con fecha 20 de septiembre de 2021, a través del Servicio de Notificaciones Electrónicas y Dirección Electrónica Habilitada, se notifica la Propuesta de Resolución.

VIGÉSIMO PRIMERO: Con fecha 22 de septiembre de 2021, TME solicita la ampliación del plazo para formular alegaciones a la Propuesta de Resolución.

VIGÉSIMO SEGUNDO: Con fecha 23 de septiembre de 2021, la Agencia concede la ampliación instada.

VIGÉSIMO TERCERO: Con fecha 11 de octubre de 2021, TME, formula alegaciones a la Propuesta de Resolución en las que se reitera en todas y cada una de las alegaciones realizadas al Acuerdo de inicio (antecedente DÉCIMO QUINTO) y añade otras:

PREVIA: SOBRE LA INCOACIÓN DEL EXPEDIENTE SANCIONADOR.

La AEPD estaba realizando una investigación independiente de la que, al menos los Operadores que participaban en el GT, y concretamente, TME, no estaba al tanto.

Efectivamente la normativa aplicable establece que la autoridad de control tendrá una serie de competencias, a cuyos efectos otorga hasta 22 tipos de funciones y hasta 10 poderes correctivos, pero todos ellos deben ejercerse siguiendo los principios del ordenamiento jurídico, y en ese sentido, la pretensión de estar utilizando alguna de esas otras herramientas previstas en la ley, cuando en realidad lo que estaba era investigando para dirimir la responsabilidad de los operadores y sancionarlos con multas económicas sin precedentes, no puede ser interpretado de otra manera que como falta de transparencia y discrecionalidad.

Las imputaciones que realiza la AEPD convierten a TME en una suerte de cooperador necesario para la consecución de este tipo de fraudes, cuando en realidad es otra víctima de los defraudadores.

La garantía de un resultado de fraude cero no es exigible a la vista de los principios establecidos en el RGPD, ni de las obligaciones correspondientes al Responsable del tratamiento.

I. SOBRE LOS HECHOS QUE MOTIVAN LA INCOACIÓN.

Se solicitó que se suspendiera el procedimiento y la AEPD se ha limitado a indicar que tales procedimientos no están dirigidos contra TME, aludiendo a que no existe identidad de sujeto para desestimar la alegación de prejudicialidad penal.

Ha ignorado el contenido de las investigaciones que se hayan realizado hasta ahora, lo cual, es relevante para determinar si lo que se estaba tratando en los procedimientos penales son cuestiones similares o trascendentes para este procedimiento, de tal forma que este no pudiese continuar hasta saber el resultado final de la vía penal.

Invoca las Sentencias nº 2249/2016 y núm. 1907/2017 de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de fechas 18 de octubre de

2016 y 5 de diciembre de 2017, respectivamente y aduce que existe prejudicialidad penal cuando **"la decisión a dictar en el proceso penal condiciona la sentencia del recurso contencioso-administrativo, de suerte que no puede pronunciarse éste sin conocer el resultado de aquél",** que es precisamente lo que podría ocurrir en este caso al ser ambos procedimientos una extensión el uno del otro.

Y, si bien no hay identidad de sujetos, los resultados de las actuaciones de investigación de los procesos penales afectan directamente al procedimiento sancionador, no solo para determinar qué ocurrió realmente a la hora de cometerse el fraude, sino también para el caso de que finalmente se impusiese una sanción, determinar el importe adecuado.

Por ello, se solicita que se requiera directamente a los diferentes Juzgados a fin de que aporten en qué punto están las denuncias interpuestas, así como el contenido de los procedimientos penales, para poder, acordar la suspensión de este procedimiento por prejudicialidad penal.

PRIMERA. DE LA CONDICIÓN DE TME COMO RESPONSABLE DEL TRATAMIENTO Y DELIMITACIÓN DE LAS OPERACIONES DE TRATAMIENTO OBJETO DEL PROCEDIMIENTO SANCIONADOR.

En ningún momento ha delimitado la AEPD a qué operaciones o actividades de tratamiento de datos está haciendo referencia concretamente, remitiéndose a éste con carácter general y de manera absolutamente arbitraria y partidista.

No identifica cuáles son los procesos o actividades responsabilidad de TME, de tal manera que se puedan separar de los que entran en el ámbito de responsabilidad de terceros (las entidades bancarias).

Es necesario aclarar que los procesos o actividades de tratamiento que se cuestionan no son otros que el **tratamiento de los datos identificativos** (nombre, apellidos, DNI), con la **finalidad de identificar al cliente** como paso previo a la gestión de una determinada solicitud (en este caso dos solicitudes concretas, el duplicado de tarjeta SIM y el cambio de titularidad), siendo la base legitimadora de dicho tratamiento el de la **ejecución del contrato** existente entre TME y su cliente. Es decir, las operaciones de tratamiento de datos consistirían en **contrastar la información que nos proporciona el solicitante con la información que consta en nuestros sistemas**.

Alude a las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD), en concreto: **"(…) En la práctica, esto puede significar que el control ejercido por una entidad en particular puede extenderse a la totalidad del procesamiento en cuestión, pero también puede estar limitado a una etapa particular del procesamiento**" y a la Sentencia del TJUE de 29 de julio de 2019: **"(…) Por el contrario, [...] esa persona física o jurídica no puede considerarse responsable del tratamiento, en el sentido de dicha disposición, en el contexto de operaciones que preceden o son posteriores en la cadena general de tratamiento para las que esa persona no de-**

termina los fines o los medios".

Considera que la Agencia vincula erróneamente a TME con una serie de operaciones o actividades de tratamiento que deberían quedar fuera del objeto del procedimiento. La Agencia intenta responsabilizarla de unas operaciones o actividades de tratamiento efectuadas por terceros, aunque ciertamente vinculadas con otras operaciones de tratamiento que sí son responsabilidad de TME. No se puede responsabilizar a TME de que se haya cometido un determinado tipo de fraude bancario porque, si esto fuese así, **se la podría responsabilizar de todos los accesos ilegítimos acaecidos en el marco de la prestación de servicios de cualquier empresa que verificase la identidad de sus clientes a través del teléfono móvil**.

Lo que la Agencia cuestiona no es el cumplimiento de los principios del RGPD o la diligencia de TME a la hora de ejecutar el duplicado de tarjeta. **Lo que se ha puesto en tela de juicio es si las políticas de identificación que TME tiene implantadas son lo suficientemente robustas** como para acreditar que el solicitante de una determinada gestión sea quien dice ser.

TME es el primer interesado en que dicho proceso de identificación se lleve a cabo sin fisuras y con las mayores garantías posibles y ha implementado medidas de seguridad adecuadas en atención a los riesgos derivados de la actividad de tratamiento de la que es responsable.

SEGUNDA. DE LA ADOPCIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS.

2.1 MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

Adjunta como **Anexo 1** el documento "***(…)***", que contiene la última versión del documento que ***(…)***. El eje central de estas medidas está constituido por la ***(…)*** que resulte aplicable en función del tipo de gestión solicitada por el cliente.

En relación con ***(…)***:

Se realiza exclusivamente a través *(…).* TME ha adoptado **la medida de seguridad más efectiva y la que más garantías ofrece de cara a identificar a un cliente**, que no es otra que la de verificar presencialmente que alguien es quien dice ser. La Agencia **no ha aclarado en ningún momento en qué sentido considera que dicha operativa es contraria al Reglamento** ni tampoco menciona qué elementos de la política de identificación tendrían que haberse adaptado.

Las medidas no solo **se adecuan a los estándares que han venido aplicando los principales actores del sector de las telecomunicaciones**, sino que en determinados aspectos los superan. Ya se puso de manifiesto que el sistema de validación de identidades que se contempla en la "***(…)***" cuenta con las **mismas garantías que el sistema de autenticación reforzada establecido por la Directiva 2015/2366. La Agencia no ha analizado en ningún mo-**

mento si las medidas dispuestas por TME en su operativa, son o no coherentes con PSD2.

Ya se puso de manifiesto que la "***(…)***" está alineada con las recomendaciones establecidas por la propia Agencia en el informe "**Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía**", **tampoco se ha pronunciado la AEPD en su Propuesta de Resolución a este respecto**.

En relación con ***(…)***:

La ***(…)*** obliga a los agentes de ***(…).***

Además, actualmente este tipo de gestiones se derivan y se tramitan por un ***(…)***. La forma en la que gestiona el ***(…*)** adjuntado como **Anexo 2.** En suma, ***(…).*** Como hace constar en su informe "**Plan de inspección de oficio *(…*)**", esta forma de identificar a los clientes se puede considerar un estándar dentro de las empresas del sector de telecomunicaciones.

TME está en desacuerdo con una de las afirmaciones de la Agencia, en concreto, la contenida en la página 93 de la propuesta, aduce que:

1.- TME **no permite ni solicitar ni gestionar un cambio de tarjeta SIM en el *(…)***, solo es posible solicitarlo presencialmente en tienda.

2.- **La *(…)* son equivalentes**. Ahora bien, aun siendo equivalentes, es evidente que no pueden en ningún caso ser las mismas. **TME no puede adoptar las medidas técnicas y organizativas relativas al tratamiento de identificación sin tener en cuenta el canal, el tipo de gestión para el que se realiza el tratamiento, y el cumplimiento de las obligaciones que tiene como operadora.**

3.- **En ningún caso se ha dicho que sea posible obtener un duplicado de tarjeta SIM sin acudir de forma presencial a una tienda.** No es lo que ha sucedido en los casos de los RECLAMANTES UNO, DOS y TRES.

2.2 REVISIÓN Y ACTUALIZACIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

TME ha probado sobradamente haber llevado a cabo esfuerzos de revisión y refuerzo de la operativa.

Los esfuerzos han sido encauzados en **tres ejes**:

a) **Refuerzo de las operativas existentes:**

- ***(…).*** Adjunta como **Anexo 3** el documento "***(…)***" que contiene:

  -. Extractos de publicaciones realizadas en el ***(…)***, entre los años 2019 al 2021.

.- Extractos de noticias publicadas en ***(…)*** del que forman parte también los ***(…)*** entre 2020 y 2021.

.- Implantación en octubre de 2020 de la nueva ***(…)*** (Anexo 2). ***(…)*** (Anexo 4).

b) **Implantación de proyectos transversales a largo plazo:**

TME ha trabajado en el desarrollo de ***(…).***

c) **Puesta en común de la problemática con esta Agencia y otros interesados:**

.- A fin de estudiar posibles vías de mejora sin haber recibido por parte de la AEPD, ni una sola propuesta de aquellas medidas adicionales que pudiera estar pasando por alto.

.- Ha tratado esta problemática con ***(…)***", con el objetivo de conocer y adaptar, en su caso, medidas efectivas que contribuyan a reducir este tipo de fraudes (Anexo 5 "***(…)***").

.- Ha creado un ***(…)*** cuyo primer encuentro ha tenido lugar en el mes de septiembre de 2021. ***(…).***

No puede decirse, que no haya realizado una labor de adaptación constante en función de los nuevos riesgos identificados.

2.3 VALORACIÓN DE LA ADECUACIÓN, OPORTUNIDAD Y EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

Alude al FD Quinto y que **la AEPD no se ha detenido en ningún momento a valorar dichos aspectos**, pocos esfuerzos se han dedicado al análisis de la proporcionalidad en relación con:

Conocimiento técnico: TME era desconocedora de las obligaciones de autenticación y acceso de terceros impuestas por la Directiva PSD2. Dichas obligaciones no le resultan de aplicación y no entraron en vigor hasta el 14 de septiembre de 2019.

Costos de implementación: son altísimos y también el tiempo de implantación que conlleva la puesta en marcha de medidas de gran calado.

Naturaleza, alcance y propósitos: de verificar la identidad de los clientes en una compañía dedicada a la **prestación de servicios de comunicaciones electrónicas** y, como tal, tiene la obligación de prestar dichos servicios de manera continuada y atendiendo a las obligaciones derivadas de la normativa que resulta de aplicación.

En los Fundamentos la Agencia solo menciona un par de las medidas de

seguridad implantadas por TME. Ni siquiera se ha entrado a hacer un análisis específico de la adecuación, oportunidad y eficacia de todas las medidas que tiene implantadas.

TME tiene **certificados y debidamente auditados los procesos y operativas que se cuestionan** en este expediente. En concreto, la idoneidad y aseguramiento de las políticas de verificación de la identidad de los clientes, es objeto de análisis de la norma **UNE 19601** de **Sistemas de Gestión de Compliance Penal**. En particular, el **control C.047**, relativo a la "**Contratación Verificación identidad cliente**", está específicamente orientado a contrastar la adecuación de las operativas, la forma de verificar la identidad de los clientes y la existencia de mecanismos de seguimiento y control.

Para garantizar el cumplimiento de esta normativa de Compliance Penal es necesario:

-. La obtención del "**Certificado de Sistema de Gestión de Compliance Penal**" (en adelante, SGCP). Este certificado **se renueva cada 3 años** y está sujeto al resultado de las auditorías periódicas de seguimiento practicadas. Aportan:

> Como **Anexo 6.1** y **Anexo 6.2**, los documentos "**Certificación 2017 AENOR 19601**" y "**Certificación 2020 AENOR 19601**", que acreditan la certificación de TME en el cumplimiento de esta normativa desde el año 2017.
>
> Como **Anexo 7.1**, el documento "**Certificación 2020 EQA 19601**", que acredita la certificación de TELEINFORMÁTICA Y COMUNICACIONES, S.A.U. (TELYCO) en el cumplimiento de esta normativa desde el año 2020.

-. La celebración de **auditorías periódicas de seguimiento.** Aportan los documentos:

> "**Auditoría 2021 AENOR 19601**" (Anexo 6.3) y "**Auditoría 2021 EQA 19601**" (Anexo 7.2). En ambas se verifica el **cumplimiento del control C.047**. En concreto, **el resultado de este proceso de auditoría demuestra que TME dispone de**:
>
> ***1.- OPERATIVAS.***
>
> ***2.- VERIFICACIÓN IDENTIDAD Y DOCUMENTACIÓN ASOCIADA.***
>
> ***3.- SEGUIMIENTO y CONTROL.***

El Modelo de Prevención de Delitos utilizado por TME también ha sido auditado por la consultora ***(…)*** a través de su Informe de Control Interno sobre el Modelo de Organización y Gestión para la Prevención de Delitos. Aporta el índice, el objeto, el alcance y las conclusiones de dicho Informe en el documento "**Informe 2020 EY Control Interno Modelo Prevención Delitos**", como

Anexo 8.1 y el documento "**Anexo I Informe 2020 Controles analizados EY**" como **Anexo 8.2.**

Por otro lado, tampoco considera que pueda llevarse a cabo un análisis de la adecuación de las medidas si no se tiene en cuenta su efectividad en términos de volumen de gestiones afectadas:

La Agencia insiste en que estamos ante un derecho fundamental protegido por la CE. Pero, no es menos cierto que, tal y como indica el RGPD "***el derecho a la protección de los datos personales no es un derecho absoluto****, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad*."

Por último, no es admisible que la Agencia aluda en su Propuesta de Resolución a una supuesta vulneración de una política que no es aplicable a TME (Know Your Costumer (KNY)).

TERCERA. DE LA RESPONSABILIDAD DE TME EN LOS CASOS DE SUPLANTACIÓN DE IDENTIDAD DE LOS TRES RECLAMANTES

3.1 RESPONSABILIDAD DEL ENCARGADO DEL TRATAMIENTO

TME encarga parte de las operaciones de tratamiento de datos objeto de este procedimiento a proveedores de confianza. Los proveedores seleccionados pasan por un **riguroso proceso de selección y contratación** que contempla la aplicación de medidas de seguridad específicas, en función del tipo de proveedor contratado. Aporta como **Anexo 9** y **Anexo 10** el ***(…).***

Ambos documentos tienen por objeto, respectivamente:

-. (…).

-. (…).

En última instancia, la aplicación de las citadas normativas internas tiene como resultado la imposición de las medidas de seguridad que se recogen en el ***(…)***, adjuntado como **Anexo 11**.

Alude a lo afirmado por la AEPD en la página 92 y aduce que en ningún momento ha pretendido eludir las responsabilidades que le corresponden respecto a la seguridad del tratamiento, sino **poner de manifiesto el cumplimiento por parte de TME de las obligaciones que la normativa de protección de datos impone al responsable,** en cuanto a:

-. Tener debidamente regularizadas las relaciones de encargo de tratamiento con los proveedores afectados de conformidad con lo dispuesto en el artículo 28 RGPD.

-. Trasladar con la debida diligencia y de manera clara a los encarga-

dos de tratamiento las instrucciones que rigen las operaciones de tratamiento encargadas.

Así, la AEPD considera probado en la Propuesta de Resolución que TME tiene debidamente regularizadas las relaciones con los encargados del tratamiento, he indica que "***se ha constatado en las alegaciones aducidas la existencia de cláusulas contractuales que hacen referencia a "Instrucciones" documentadas por TME (…)****."*

Teniendo en cuenta **que las suplantaciones de las partes reclamantes UNO, DOS y TRES tienen en común la concurrencia de errores puntuales de la operativa** diseñada por TME, y que la Agencia ha constatado la comisión de dichos incumplimientos, entiende que es muy importante remarcar la diferencia que hay entre:

- Que las medidas implantadas sean apropiadas.

- Que las medidas se hayan trasladado correctamente a los encargados.

- Que las medidas se hayan incumplido por los encargados.

Es decir, hay que diferenciar entre que las medidas implantadas sean suficientes y que éstas, aun siendo suficientes, se hayan podido incumplir puntualmente por parte de los encargados.

Aduce que **habiéndose probado en el presente procedimiento que, de no ser por dichos incumplimientos, no se habrían producido dichas suplantaciones**, considera fundamental que se delimiten las responsabilidades que asumen cada una de las partes en relación con las operaciones del tratamiento de datos cuestionadas. Alude a las Directrices 07/2020 donde se dice: ***Tanto los responsables como los encargados pueden ser multados en caso de incumplimiento de las obligaciones del RGPD que son relevantes para ambos, y ambos son directamente responsables ante las autoridades de supervisión (…).***

En relación con este aspecto, TME también afirma que conforme al artículo 28.10 del RGPD, el encargado puede ser considerado como responsable del tratamiento en caso de "determinar los fines y medios del tratamiento". Según indica, las mencionadas Directrices aclararían que ""Determinar los propósitos y los medios equivale a decidir respectivamente el "por qué" y el "cómo" del procesamiento"

En resumen, se alega que no cabe la imputación a TME de la responsabilidad por este incumplimiento, ya que esta empresa habría actuado con toda la diligencia exigible, y que los posibles fallos de seguridad al haberse expedido los duplicados de las tarjetas SIM serían achacables al proveedor, ya que este habría incumplido sus instrucciones.

3.2 RESPONSABILIDAD DE LAS ENTIDADES BANCARIAS

Parece que la AEPD quiere hacer responsable a TME de la comisión de los fraudes bancarios llevados a cabo por los defraudadores en los tres casos.

Las obligaciones de autenticación y acceso de terceros impuestas por la Directiva PSD2 no resultan de aplicación a TME y, además, no entraron en vigor hasta el 14 de septiembre de 2019.

Por todo ello, no se puede hacer a TME responsable de los tratamientos efectuados por otros responsables (entidades bancarias), ni puede atribuirse a TME la responsabilidad de adoptar medidas de seguridad relacionadas con operaciones de tratamiento de datos efectuados con otra finalidad distinta.

II. SOBRE LOS FUNDAMENTOS DE DERECHO

PRIMERA. SOBRE LA PRESUNTA INFRACCIÓN QUE CONTINÚA CONSIDERÁNDOSE COMETIDA POR PARTE DE TME: VULNERACIÓN DEL PRINCIPIO DE TIPICIDAD

Ha quedado probado *"que TME **dispone de políticas documentadas de protección de datos** en las que se establece el modo de actuar de TME y de los encargados*".

1.1 SOBRE LA CONDUCTA DE TME: EN NINGÚN CASO PODRÍA CONSIDERARSE SUBSUMIBLE EN EL ARTÍCULO 5.1 F) RGPD .

La AEPD ha constatado que la conducta no es subsumible en el artículo 5.2 RGPD, es decir, reconoce que TME ha cumplido con lo dispuesto en el artículo 5.1 y ha sido capaz de demostrarlo, constatándose la aplicación de medidas técnicas y organizativas apropiadas que garantizan un nivel de seguridad que es adecuado al riesgo. Estas medidas **se revisan y actualizan** cuando es necesario a fin de garantizar la seguridad del tratamiento.

La Agencia **sí está exigiendo infalibilidad** a TME, **atendiendo tan solo al resultado producido** en el caso de **tan solo tres reclamantes**, y asumiendo de nuevo la existencia de una responsabilidad objetiva (proscrita en nuestro ordenamiento jurídico) como justificación suficiente para considerar que existe una infracción, y que ésta es muy grave. Alude al CIPL *(Centre for Information Policy Leadership*), que en sus comentarios acerca de las directrices sobre la notificación de violaciones de datos personales del GT del Artículo 29 (*"Comments by the Centre for Information Policy Leadership On the Article 29 Working Party's "Directrices on personal data breach notification under Regulation 2016/679" Adopted on 3 October 2017"),* ilustra bien la **diferencia entre mitigación del riesgo e infalibilidad,** al indicar que no puede ser una obligación para las organizaciones garantizar la seguridad absoluta de las operaciones de tratamiento de datos *("**It cannot be an obligation for organisations to guarantee absolute security of data processing activities").***

Asimismo, no se ha tenido en consideración que incluso el GT sobre protección de datos del artículo 29, en las "*Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Regla-*

mento 2016/679" reconoce que, aunque se implementen las medidas de seguridad, pueden existir riesgos, al indicar que:

> *"(…) un elemento clave de cualquier política en materia de seguridad de los datos es poder,* ***en la medida de lo posible****, prevenir una violación y,* ***cuando a pesar de todo se produzca****, reaccionar de forma rápida".*

Alude también a un artículo del INCIBE:

> *"Para* ***reducir*** ***la probabilidad*** *de que este tipo de incidentes ocurran (…)"*
>
> *"De esta forma evitaremos en la* ***medida de lo posible*** *las filtraciones de información y la pérdida de imagen de nuestra compañía".*

Y a la Sentencia de la AP de Valladolid (Sección 1ª) núm. 74/2010 de 10 marzo (AC 2010\368), en relación con el presunto incumplimiento de medidas de seguridad por parte de un banco, expone que:

> *"****En cualquier sistema operativo****, **incluso en el tradicional,** ****existen riesgos**** y lo determinante para atribuir responsabilidades será si en el utilizado se daban garantías suficientes,* ***sin que pueda llegarse a la conclusión contraria por el mero hecho de que posteriormente se hayan mejorado los sistemas de seguridad****, que es de lógica que se vayan modernizando y perfeccionando ante* ***nuevas prácticas defraudatorias*** *que hacen ineficaces los anteriores".*

TME considera que ha quedado probado que las medidas de seguridad no se han visto vulneradas, sino que se ha producido el incumplimiento de las operativas establecidas por TME y que han tenido lugar acciones de terceros ajenos a ella.

Así, **la legalidad o no de una medida de seguridad (es decir su adecuación) viene determinada por su contribución a la reducción de la probabilidad de ocurrencia del incidente, y sin ninguna duda, si la probabilidad de acaecimiento de una solicitud fraudulenta de duplicado SIM (por cualquiera de sus modalidades) es del *X,XXXXX* %,** se trata de un porcentaje mínimo.

En relación con la evaluación de riesgos, debería tenerse en cuenta que la emisión de un duplicado de tarjeta SIM puede resultar necesaria para que un cliente siga disfrutando de su servicio de comunicaciones móviles. Es decir, los datos tratados son identificativos del cliente, con la **finalidad de acreditar la identidad** del solicitante de la gestión y poder **continuar prestando el servicio de telefonía móvil**, conforme a lo exigido en la normativa vigente: artículo 47 de la LGTEL, artículo 3. e) del RD 899/2009, de 22 de mayo y la Orden IET/1090/2014.

1.2 SOBRE LA REDACCIÓN DE LA NORMATIVA QUE RESULTA DE APLICACIÓN: CONCEPTOS JURÍDICOS INDETERMINADOS QUE CONTRIBUYEN A INCREMENTAR LA INSEGURIDAD JURÍDICA E INDEFENSIÓN DE

TME.

Invoca la Sentencia del Tribunal Supremo de 26 de junio de 2001 (RJ 2001, 5740), que recuerda la doctrina del Tribunal Constitucional.

Alude a la importancia de que la norma reguladora no efectúe **formulaciones vagas, abiertas o excesivamente amplias de los ilícitos y sanciones**, que carezcan de la suficiente determinación, ya que "*se permitiría al órgano sancionador actuar con un excesivo arbitrio y no con el prudente y razonable que permitiría una debida especificación normativa" (STC 61/1990, de 29 de marzo).*

La AEPD no ha tenido en cuenta las alegaciones formuladas por TME, limitándose a remitirse a los considerandos 7 y 13 del RGPD, a invocar el derecho a la protección de datos como derecho fundamental, y a las definiciones del artículo 4, entre las que reconoce que **no se incluyen los conceptos jurídicos a los que hicimos referencia en las alegaciones al Acuerdo de Inicio**. Por ello, vuelve a destacarse la **ambigüedad e indeterminación de los conceptos recogidos en el precepto** que esta AEPD considera vulnerado, tales como: "*seguridad adecuada*" o "*medidas técnicas y organizativas apropiadas*".

Invoca el artículo 9.3 de la CE, la STC 104/2009, de 4 de mayo y la STC 145/2013, de 11 de julio y aduce que la Agencia continúa propiciando inseguridad jurídica y dificultando la defensa de TME, pudiendo vulnerarse en consecuencia determinados principios que se encuentran garantizados constitucionalmente (artículo 24, 25 y 9.3 de la CE).

1.3 SUBSIDIARIAMENTE: SOBRE LA INTERPRETACIÓN Y APLICACIÓN DE LA NORMATIVA REALIZADA POR ESTA AGENCIA. RIESGO DE VULNERACIÓN DEL PRINCIPIO DE ESPECIALIDAD.

En relación con el principio de especialidad, la Agencia se limita a recoger los argumentos expresados, sin llegar a pronunciarse sobre este aspecto. En la Propuesta de Resolución se *"reconduce la imputación de las infracciones inicialmente consideradas. La calificación jurídica de los hechos que se imputan pasa a calificarse como una **única infracción derivada de la vulneración del artículo 5.1. f) del RGPD"*** sin tener en cuenta el principio de especialidad, y en concreto el artículo 32 del RGPD.

Una vulneración del **principio de especialidad**, exige la prioridad en la aplicación del precepto específico sobre el general. En definitiva, de los artículos que en su momento fueron referenciados, sería el artículo 32 del RGPD también regulado en la LOPDGDD, que en su artículo 73 f), a diferencia del artículo 72.1 a), prevé como infracción grave "f) *La **falta de adopción de aquellas medidas técnicas y organizativas** que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos p**or el artículo 32.1 del Reglamento (UE) 2016/679**"*. Por lo que, en ningún caso podría calificarse la conducta de TME como muy grave.

SEGUNDA. SOBRE LA TIPIFICACIÓN DE LA PRESUNTA CONDUCTA EN OTROS PROCEDIMIENTOS SANCIONADORES INCOADOS A TME Y TELEFÓNICA DE ESPAÑA, S.A.U (TDE): ERROR EN LA CALIFICACIÓN DE LA INFRACCIÓN.

Debe concretarse que esta parte sí determina cómo puede verse agravada su situación, ya que la actuación de la Agencia es arbitraria. En los PS/ 00114/2019, PS/00453/2019, PS/00235/2020, la tipificación de la conducta ha sido diferente y la sanción impuesta también. En todos ellos se ha tipificado la conducta de TME como contraria al artículo 6.1 RGPD ("*licitud del tratamiento*") por presuntamente haberse tratado los datos de los denunciantes sin existir base legitimadora para ello. Sin embargo, en este caso considera la conducta como contraria al artículo 5.1 f) del RGPD. Asimismo, la sanción impuesta también ha distado mucho de la propuesta en el marco de este expediente, pese a resultar de aplicación el artículo 83.5 a). Es más que evidente que con este proceder, la AEPD propicia una proscrita inseguridad jurídica y dificulta una adecuada defensa de TME, vulnerando en consecuencia las previsiones del artículo 9.3 CE.

TERCERA. LA CONDUCTA DE TME NO ES ANTIJURÍDICA

En cuanto a la antijuricidad de la conducta por la Agencia *"se considera que responde al tipo infractor y al título de culpa",* sin entrar a analizar las alegaciones realizadas por esta parte en este sentido.

Insiste en rechazar la antijuridicidad de la conducta en base a los siguientes argumentos:

-. La operativa de identificación de clientes contempla medidas técnicas y organizativas diseñadas para garantizar una seguridad adecuada de los datos personales de sus clientes, incluida la protección contra el tratamiento no autorizado o ilícito. Aduce que la norma **no exige la infalibilidad de dichas medidas**.

-. Las medidas implantadas se han demostrado **oportunas y eficaces en atención** al volumen de contratación y del resto de gestiones, y **a la obligación de asegurar la conectividad de los clientes de forma rápida y sostenible en el tiempo**. La actuación de TME tampoco ha lesionado o puesto en peligro bien jurídico alguno protegido, sino que responde al **necesario equilibrio entre procurar la seguridad del tratamiento de datos personales y garantizar la prestación de los servicios de comunicaciones electrónicas** conforme al resto de normativa que resulta de aplicación.

-. En relación con la **relación contractual que existe con los distribuidores y resto de proveedores**, dichos contratos responden a la realidad mercantil e incluyen todas aquellas previsiones que son necesarias con el objetivo de garantizar su cumplimiento. En este sentido, la AEPD sí "***ha constatado que TME dispone de políticas documentadas de protección de datos*** *(…)".* Sin embargo, no estima las alegaciones realizadas

por esta parte en ese sentido.

CUARTA. AUSENCIA DE CULPABILIDAD

No existe el elemento subjetivo de culpa requerido para la imposición de sanciones administrativas. Todo lo contrario, ya que la actitud de TME revela una inequívoca voluntad de proceder conforme a Derecho sin existir en modo alguno intencionalidad de infringir la norma, y teniendo en todo caso voluntad de cumplimiento.

No cuestiona TME si las personas jurídicas tienen o no capacidad de infringir las normas a las que están sometidos, sino la ausencia de su culpabilidad, y en consecuencia, la ausencia de infracción de la norma.

Esta falta de culpabilidad se manifiesta en torno a que:

-. La conducta de TME se desempeñó con toda la diligencia profesional exigible, que actuó con buena fe, y que, por ello mismo, no cabe imputársele un actuar culposo.

-. La elección y supervisión de los encargados del tratamiento se ha desempeñado con toda la diligencia profesional exigible. Asimismo, debe insistirse en la propia responsabilidad del encargado del tratamiento.

-. Las conductas que han provocado las consecuencias expuestas en ningún caso son imputables a TME.

4.1 LA ACTUACIÓN DILIGENTE, DE BUENA FE Y CONFIANZA LEGÍTIMA DE TME

En relación con la **diligencia** de TME, resulta llamativo que en la Propuesta de Resolución, por un lado, se indiquen ciertas afirmaciones que incluyan valoraciones positivas y por otra parte, en contraposición se indiquen otras negativas.

En relación con dichos argumentos, conviene hacer una serie de precisiones.

En primer lugar, debe señalarse que TME no se dedica específicamente a la gestión de datos personales, sino que es una compañía dedicada a la **prestación de servicios de comunicaciones electrónicas.**

TME no se ha limitado a invocar la ausencia de culpa, sino que todo lo expuesto en las alegaciones realizadas es plenamente demostrativo del rigor y diligencia con la que ha actuado.

La AEPD mantiene en la Propuesta de Resolución que "*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*** *(…) No basta con disponer de una política de seguridad,* ***sino de adecuarla para mitigar los riesgos****. (…)".* Sin embargo, ha quedado acreditado que TME **tra-**

baja constantemente en la mejora de las medidas de las que dispone con el objetivo de evitar la suplantación de identidad en los distintos procesos de contratación y gestiones que se soliciten, en la formación y en la adaptación de los protocolos de seguridad dentro de la organización. Es decir, ha quedado completamente probado que TME implementa unas medidas de control adecuadas, que se **revisan y refuerzan**. **Invoca la certificación de la UNE 19601 de Sistemas de Gestión de Compliance Penal**, así como **tener debidamente auditado su Modelo de Organización y Gestión para la Prevención de Delitos** incluido el **control C.047** relativo a la "**Contratación Verificación identidad cliente**".

Sin embargo, la Agencia continúa centrándose tan solo en el resultado producido, sin tener en cuenta las circunstancias completamente ajenas a TME que han tenido lugar, exigiendo en consecuencia una responsabilidad objetiva.

La AEPD ha reconocido que TME cuenta con cláusulas contractuales que hacen referencia a instrucciones documentadas, además, como prestador de servicios de comunicaciones electrónica, tiene la obligación de prestarlo de forma continuada y en todo momento ha actuado de buena fe y de forma proactiva y diligente (incluyendo la participación en el GT). Invoca la STS de 17 de diciembre de 1988 que dice: "***no es justo sancionar a quien obra de buena fe*** *procediendo dejar sin efecto la sanción cuando el actuar del inculpado fue debido a una determinada creencia excluyente de la culpabilidad*".

4.2 DILIGENCIA DEBIDA EN LA ELECCIÓN Y SUPERVISIÓN DE LOS ENCARGADOS DEL TRATAMIENTO Y RESPONSABILIDAD DE ESTE:

En la Propuesta de Resolución se señala que *"La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad",* y vuelve a mencionar el contenido del artículo 5 del RGPD

Existe un incumplimiento de las operativas establecidas por TME: responsabilidad de los encargados de tratamiento de TME y de determinadas acciones de terceros ajenos a la esfera de actuación y de responsabilidad de TME.

Invoca que la Agencia ha reconocido la existencia de cláusulas contractuales que hacen referencia a instrucciones documentadas, por lo tanto, reconoce una actuación diligente, sin embargo, desestima la alegación aducida al señalar que *"los tratamientos efectuados por los encargados se harán en nombre del responsable, es decir, TME"*.

Invoca los artículos 1902 y 1903 del Código Civil e insiste en que su conducta ha sido diligente, ya que, por ejemplo:

- Los proveedores seleccionados pasan por un **riguroso proceso de selección y contratación** que contempla de aplicación de medidas de seguridad específicas, en función del tipo de proveedor contratado.

- Cuenta con un procedimiento consolidado y adecuado de verificación de la identidad de los clientes, y con instrucciones debidamente documentadas a sus encargados de tratamiento.

- En los contratos con los encargados se encuentran previstas determinadas **medidas disciplinarias y de penalización**, y, a los efectos de garantizar el cumplimiento de la operativa de identificación en tienda, se ha establecido para todo el canal presencial una penalización adicional por cada gestión realizada y documentada incorrectamente por parte de un comercial. Lleva aparejada la implantación de un **proceso de certificación mensual** del cumplimiento de los distribuidores.

- Se ha aportado certificación de la **UNE 19601 de Sistemas de Gestión de Compliance Penal** y el cumplimiento, tanto por parte de TME como por el resto de las empresas del grupo, del **control C.047** relativo a la "**Contratación Verificación identidad cliente**". Es decir, se acredita, entre otras cosas, la existencia de "***(…)***".

- Se está llevando a cabo la ***(…).***

- Se ha incluido la "***(…)***" para autorizados.

Alude a la STS 1232/2018 de 18 de julio de 2018 y a la STSJ de Madrid 568/2020 de 10 septiembre de 2020. En definitiva, en ningún caso se infringen los deberes de vigilancia que pesan sobre TME en relación con las personas que actúan en su nombre.

La Agencia no ha tenido en cuenta el contenido del artículo 28.10 del RGPD. Por lo que, lo sucedido no se ha debido a vulnerabilidades en los procedimientos establecidos, ni en las instrucciones dadas a los encargados del tratamiento, sino al **incumplimiento de la operativa diseñada por parte de los agentes comerciales** de los canales para la atención de las solicitudes de las diferentes gestiones a las que se refiere este expediente, y en consecuencia al incumplimiento de las instrucciones dadas por TME por parte de los empleados de dichos encargados.

Insiste en que, de lo anterior, puede concluirse que la AEPD está exigiendo una **responsabilidad objetiva**, basándose simplemente en el resultado, sin tener en cuenta que **TME ha actuado con total diligencia en la relación con sus encargados de tratamiento**. Aduce la STS (Sala de lo Contencioso-Administrativo, Sección3ª) núm. 1468/2017 de 28 septiembre (RJ 2017\4422).

Es necesario, por tanto, la constatación de la intervención culpable por parte de TME, que no se ha producido en este caso, sin existir tampoco "*culpa in vigilando".* En tanto no se cumpla con este elemento, no puede imponerse sanción alguna y debería procederse al archivo del procedimiento sancionador.

4.3 CIRCUNSTANCIAS EXCEPCIONALES Y AJENAS A TELEFÓNICA:

• **Posible negligencia en el cuidado de los datos personales por parte de los usuarios: los propios usuarios tienen la responsabilidad de custodiar debidamente sus datos personales.**

Al hacer uso de Internet, estos pueden compartir determinada información personal, lo que puede implicar que sea utilizada por terceros con fines ilícitos. Eso queda fuera del alcance y de la capacidad de actuación de TME, ya que los datos que en ocasiones permiten la suplantación de identidad pueden ser obtenidos de la información que en su caso haya podido divulgar el propio usuario en algún momento, o de una falta de deber de cuidado al custodiar sus contraseñas o información personal.

Alude a la Guía de la AEPD "Protección de datos y prevención de delitos" y las recomendaciones sobre el Phishing. Estas circunstancias no se han tenido en cuenta por la Agencia.

Asimismo, TME informa a sus clientes en el marco de su relación contractual una serie de cláusulas que exigen diligencia sobre las claves de acceso y los dispositivos. Alude a varias sentencias. La Sentencia núm. 107/2018 de la AP de ***PROVINCIA.2 de 12 marzo, que establece que "*Por su parte* ***los clientes tienen un deber de custodia respecto de sus claves de acceso (…);*** Sentencia de la AP de Sevilla, de fecha 26 de mayo de 2014, *al* ***haber hecho caso omiso de las advertencias y avisos de seguridad del banco****;* Sentencia de la AP de Las Palmas de Gran Canaria de fecha 20 de diciembre de 2012, que traslada que si el cliente *incurrió* ***en error provocado por un tercero ajeno*** *al Banco* ***y le facilitó, engañado, las claves a ese delincuente***; y a la Sentencia núm. 74/2010 de la AP de Valladolid de 10 marzo.

En definitiva, y como reproduce la Agencia, "***(…)***", datos que quizá haya podido facilitar el propio afectado sin saberlo, o a los que haya permitido que se acceda, quedando claro que el acceso a los SMS por parte de los suplantadores por sí mismo no permite la ejecución de operaciones bancarias (resultado perseguido por los suplantadores).

• **Probable responsabilidad de terceros ajenos a TME, como las entidades bancarias**

La Agencia reconoce que este tipo de estafas se inician en el ámbito de las entidades bancarias y tienen como finalidad ejecutar operaciones bancarias. Sin embargo, continúa atribuyendo a TME una responsabilidad que no le corresponde, sino que corresponde a estas. TME tan solo trata los datos identificativos del cliente con la finalidad de acreditar la identidad del solicitante de la gestión y poder continuar prestando el servicio de telefonía móvil, atendiendo a las exigencias de la normativa de telecomunicaciones y de consumo). Pero la AEPD está intentando responsabilizarla de unas operaciones de tratamiento de datos personales efectuado por terceros (como son los bancos), que no son de su responsabilidad.

La Agencia reconoce que la Directiva PSD2 no resulta de aplicación a TME e insiste en que el duplicado de tarjeta SIM permite a los suplantadores acceder al código de autenticación de la transacción. Insiste en que no está teniéndo-

se en cuenta que la operación o actividad de tratamiento que realiza, y de la que es responsable del tratamiento, se limita a gestionar el duplicado de una tarjeta SIM en el marco de sus obligaciones como prestador de un servicio de comunicaciones electrónicas. Nada tiene que ver con los mecanismos de autenticación utilizados por terceros.

Insiste, debería la entidad bancaria establecer unas medidas de seguridad adecuadas para el acceso a su entorno privado y comprobar que efectivamente está remitiendo una clave para realizar la transacción al titular de la cuenta y alude a la SAP de Alicante 107/2018 que indica que "Constituye por tanto obligación esencial de las ***entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones (…)*** y a la SAP de Zaragoza que dice: *salvo actuación fraudulenta o negligencia grave del titular de la cuenta,* ***la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático****".*

En conclusión, de todo lo anterior puede extraerse que esta Agencia está imponiendo a TME una serie de obligaciones que no le corresponden, exigiendo de nuevo una responsabilidad objetiva, por el mero hecho de ser la prestadora del servicio de telefonía móvil y en consecuencia ser la encargada de gestionar los duplicados de SIM.

• Acciones intencionadas de terceros para la comisión de un delito

En la Propuesta de Resolución, la Agencia reconoce que:

- *"(…) para completar la estafa,* ***es necesario que un tercero "suplante la identidad" del titular de los datos****, para recibir el duplicado de la tarjeta SIM".*

- *"el 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 inserida la tarjeta SIM duplicada".*

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

Debe tenerse en cuenta que, de la comisión de un delito, tal y como indica el

artículo 27 del Código Penal, los responsables son los "*autores y los cómplices*", siendo autores "***quienes realizan el hecho*** *por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento*" (artículo 28 CP). Y está claro que esos autores son terceros que nada tienen que ver con TME.

Por otro lado, también debemos volver a hacer referencia en este punto al **engaño previo por parte del suplantador a los comerciales de TME** para conseguir realizar determinadas gestiones.

Incluso afirma que podría considerarse un supuesto de **fuerza mayor**, por encajar las circunstancias descritas en dicho concepto, que determina **la falta de responsabilidad o culpabilidad en la conducta infractora**. Alude a 3 sentencias (de la AP de Málaga y de Barcelona).

En resumen, **no concurre en este caso el elemento esencial de culpabilidad en la conducta de TME**, ya que:

- Ha actuado siempre con plena y fundada creencia excluyente de toda responsabilidad y en cumplimiento de la legislación aplicable.

- Nos encontramos ante la responsabilidad de los empleados de los distribuidores y proveedores de TME (encargados del tratamiento) que han incumplido las operativas establecidas por TME, pese a la más que evidente y probada **actuación diligente** de TME en el marco de dicha relación contractual.

- En cualquier caso, y ante una suplantación de identidad, esta puede producirse por multitud de factores que son ajenos a la voluntad y capacidad de actuación de TME, tales como que:

  i) Hay terceros que tienen la voluntad de cometer un delito, acción que resulta inevitable para Telefónica (es decir, no se trata de un error vencible como indica esta Agencia, ya que no podría haber sido evitado).

  ii) Los datos que permiten la suplantación de identidad no son obtenidos de Telefónica. Los usuarios tienen obligación de custodiarlos, y su obtención puede venir derivada de una actuación negligente de dichos usuarios al dar acceso a dichos datos.

  iii) Las entidades bancarias son las responsables de determinar las medidas de seguridad necesarias para garantizar el consentimiento del titular de la cuenta ante cualquier operación bancaria, y la acreditación de su identidad.

Por lo tanto, resulta de extraordinario interés reiterar que en este caso no hay nexo causal por acción u omisión, entre TME y el resultado final, debido a la intervención de terceros con entidad suficiente para alterar ese nexo.

Por lo que, **no existiendo conducta antijurídica, ni típica, ni culpable de TME en los hechos imputados insistimos en que debería haberse orde-**

nado el archivo del presente procedimiento y no imponerse sanción alguna.

QUINTA. INCUMPLIMIENTO DEL PRINCIPIO DE PROPORCIONALIDAD

En el hipotético caso de que la AEPD, carente del adecuado soporte legal y con el único objetivo de imponer una multa, considere idóneo e indispensable sancionar económicamente a TME, el importe deberá ser estimado atendiendo en todo caso al principio de proporcionalidad que rige la potestad sancionadora.

Alude a las STS de 2 de junio de 2003 y a los Considerandos 4, 129 y 148 y al artículo 83.

La sanción económica resulta de todo punto ineficaz y desproporcionada. En concreto, no se han tenido en consideración las previsiones de los artículos 83.1 y 83.2 del RGPD a la hora de determinar el importe de la multa administrativa propuesta.

5.1 DE LAS AGRAVANTES APRECIADAS POR LA AGENCIA

- 83.2.a) RGPD.

Sobre la gravedad: Aduce la **SAN 00496/2017**, en la que no se considera justificada ni motivada la valoración de la conducta como grave por parte de la SESIAD, en la medida en que no se apreciaba que el incumplimiento fuese generalizado.

Sobre la duración: sorprende que la Agencia aprecie la agravante de duración, al entender que los hechos abarcan un periodo superior al año, y al mismo tiempo se estime como atenuante la falta de carácter continuado de la infracción.

Sobre los interesados afectados: la Agencia está utilizando convenientemente la información traslada por TME, dado que, por un lado desestima los argumentos expuestos en la Alegación Tercera de las Alegaciones al Acuerdo de Inicio y por otro, entiende que concurre la agravante de interesados afectados apoyándose en la información trasladada en el marco de los requerimientos de información practicados.

Sobre los daños y perjuicios producidos: en modo alguno se puede atribuir a TME la responsabilidad sobre la materialización del fraude bancario, ya que su responsabilidad termina con el resultado del duplicado de tarjeta, pero no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias.

- 83.2.b) RGPD. **Negligencia**:

Los sucesos ocurridos con las partes reclamantes UNO, DOS y TRES no pueden ser considerados en modo alguno como una muestra representativa del nivel de compromiso demostrado por TME en el cumplimiento de sus obligaciones en materia de protección de datos y, mucho menos, del grado de eficacia que revisten unas políticas de seguridad que están diseñadas para

atender a un volumen de clientes que supera los 8 millones.

- 83.2.d) RGPD. **Responsabilidad:**

TME no entiende el significado de lo expresado en esta agravante ni el criterio que utiliza la Agencia para llegar a dicha conclusión.

- 83.2.e) RGPD. **Otras infracciones cometidas:**

Considera que solo cabe una interpretación restrictiva de dicho precepto, debiendo de tenerse en cuenta en todo caso, únicamente aquellas sanciones que hubieran recaído con anterioridad en relación con el mismo tipo infractor.

- 83.2.g) RGPD**. Categorías de datos afectada:**

La AEPD se está refiriendo una vez más a los perjuicios que provoca el fraude bancario, cuando eso nada tiene que ver con el tipo de categorías de datos tratados por TME que no entran en la categoría de datos sensibles recogida en el artículo 9 del RGPD, si no que la propia AEPD los clasifica como "datos de escaso riesgo", según la categoría de datos personales realizada en el apartado 6.2.3 de la "Guía para la gestión y notificación de brechas de seguridad".

- 76.2.b) LOPDGDD. **Vinculación con la realización de tratamientos.**

Si bien es cierto que TME realiza un alto volumen de operaciones de tratamiento de datos personales, la gran mayoría de éstas progresan sin mayor incidencia. Podría, en su caso, considerarse la vinculación de TME con la realización de tratamiento de datos personales como un atenuante, no como una circunstancia agravante.

5.2 DE LAS ATENUANTES APRECIADAS POR ESTA AGENCIA EN EL ACUERDO DE INICIO

TME considera que la Agencia no ha tenido en consideración las siguientes atenuantes:

- 76.2 d) LOPDGDD. **Negligencia del afectado:**

Las suplantaciones de identidad producidas en los tres casos de las partes reclamantes no habrían sido posibles bajo ningún concepto si el suplantador no hubiese realizado una previa captación ilegítima de los datos personales de dichos clientes.

La Agencia desestima la concurrencia de esta atenuante al entender que el citado precepto "*alude a una actuación voluntaria y activa de los afectados, circunstancia no acreditada en los casos analizados*". No obstante, no es eso lo que dice el citado artículo, que específicamente indica que "*al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción*."

Si entiende la Agencia que el fraude podía haberse evitado en caso de que TME hubiese empleado unos mecanismos de identificación distintos (cuestión que se ha demostrado incierta a lo largo del presente Procedimiento), **no puede arbitrariamente pasarse por alto el hecho de que el fraude no ha-**

bría tenido lugar si los suplantadores no se hubiesen hecho previamente con los datos de carácter personal a través de los interesados.

Lo cierto es que TME no puede hacer establecer sus políticas de identificación cubriendo todos los escenarios en los que los interesados tratan sus propios datos personales.

- 83.2.j) RGPD. **Certificación de los procesos de la compañía cuestionados**:

TME dispone de un SGCP acreditado de conformidad con la norma UNE 19601 que, certifica la validez del sistema de verificación de la identidad de los clientes a los efectos de prevenir posibles delitos de estafa (art. 248, 249, 250, 251 y art. 251 bis del Código Penal).

En el supuesto de que no pueda ser tenida en cuenta para apreciar la atenuante recogida en el artículo 83.2.j) del RGPD, entiende que deberá considerarse como un factor atenuante aplicable a las circunstancias del caso en los términos expuestos en el artículo 83. 2. k) del RGPD.

- 83.2.j) RGPD. **Otros factores atenuantes aplicables a las circunstancias del caso:**

Consideran que no se han tenido en cuenta:

-. Las pérdidas económicas sufridas por TME: La Agencia no ha tenido en cuenta que las operadoras son una víctima más de este tipo de acciones. TME sufre tanto pérdidas económicas directas (devolución del importe de los duplicados, entre otros) como indirectas (grave daño reputacional, alto impacto en la experiencia de clientes).

.- La complejidad de implementar nuevas medidas. TME tiene implementados ***(…)*** que pretenden ser una importante palanca de cambio en los procesos de identificación de clientes. No obstante, este tipo de iniciativas llevan aparejadas grandes cantidades de recursos humanos y económicos, haciendo imposible una implantación inmediata de las mismas.

.- TME tiene debidamente auditado su ***(…)*** para la Prevención de Delitos.

.- La concurrencia de las obligaciones derivadas de la normativa aplicable a las empresas que operan en el sector de las telecomunicaciones.

Por todo lo expuesto, si la AEPD decide mantener la sanción, estas atenuantes deben ser tenidas en cuenta para reducir su importe.

Sobre la base de las anteriores alegaciones TME solicita:

i. Se suspenda el procedimiento y se requiera a los reclamantes a fin de que aporten en qué punto están las denuncias interpuestas con el fin de determinar si existe prejudicialidad penal.

ii. Se declare la inexistencia de responsabilidad por parte de TME por las presuntas infracciones imputadas, ordenando el archivo del expediente sanciona-

dor.

iii. Subsidiariamente, se tenga en consideración que no puede subsumirse la conducta en el precepto que la Agencia continúa considerando vulnerado, y existir un error en la calificación de la infracción.

iv. En caso de entender que las medidas técnicas y de seguridad no son adecuadas, debería atenderse a la especialidad del artículo 32 del RGPD.

v. Por último, que se minore la sanción inicialmente propuesta.

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

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

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

HECHOS PROBADOS

PRIMERO: TME 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 https://www.movistar.es/particulares/centro-de-privacidad/#Para: *En Movistar tratamos los datos del cliente o usuario para la prestación del servicio, así como para otras finalidades que el mismo permita o autorice en los términos informados en la presente Política de Privacidad o en las Condiciones específicas de cada Producto o Servicio Movistar contratado.*

SEGUNDO: TME presta sus servicios de telefonía móvil a través de tres marcas comerciales que son: Movistar, O2 y Tuenti. Cada una de ellas dispone de distintas operativas de funcionamiento.

TERCERO: Con fecha 13 de diciembre 2019, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante uno (expediente con núm. de referencia ***E/00560/2020***), dirigida contra THADER, sita en ******LOCALIDAD.2*** (******PROVINCIA.2***), tras expedirse en fecha 6 de marzo 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 los Mossos d'Esquadra USC de ******LOCALIDAD.3*** (Barcelona) en fecha 8 de marzo de 2019, número de diligencia ***XXXXXXXX,*** en la que la parte reclamante uno manifestó lo siguiente:

"(…) Que quiere denunciar que le han vuelto a duplicar la tarjeta SIM de su móvil ******TELÉFONO.1*** *y esta vez, han accedido a su banca online del BBVA y han realizado dos transferencias por valor total de 28.000 euros.*

Que la primera denuncia con las diligencias arriba indicadas le duplicaron la tar-

jeta SIM del móvil pero no se encontró con ningún cobro ni movimiento fraudulento a través de su móvil.

Que anuló su tarjeta SIM y se hizo otra nueva con un nuevo número de móvil (…)

Que en fecha 7/03/2019 por la mañana, el denunciante recibió una llamada de su entidad para que se personara en la oficina.

Que una vez en la oficina le dijeron si había hecho algún movimiento extraño desde su banca on line y el denunciante dijo que no.

Que desde la oficina del BBVA le dijeron que había habido dos transferencia desde su cuenta corriente a un tercero por valor de 13.000 y 15.000 euros.

Que esas transferencias son realizadas primeramente desde una cuenta corriente en plan fijo del denunciante a la cuenta corriente de ahorro también del denunciante, y de aquí a una tercera persona.

Que la cuenta corriente final que recibe las transferencias es la ***ES00 0000 0000 00000 0000 00000*** *del BBVA a nombre de* ***B.B.B.***

Que la fecha de la transferencia es del día 6/03/2019 por la tarde.

Que precisamente, desde este día por la tarde, el denunciante se quedó con el móvil inoperativo. (…)". (La traducción del catalán es nuestra).

En relación con esta reclamación, THADER, informó a esta Agencia que, en fecha 6 de marzo 2019, se realizó un cambio de tarjeta SIM en la tienda de Movistar de ***LOCALIDAD.2, según la operativa de Movistar "***(…)***" tras dar validez a la documentación aportada: ***(…).***

TME, informó a esta Agencia que, la expedición del duplicado fue posible debido a la concurrencia de varias circunstancias:

1. ***(…):***

2.- (…).

3.- (…).

CUARTO: Con fecha 17 de diciembre de 2019, tuvo entrada en esta Agencia otra reclamación formulada por la parte reclamante uno (expediente con núm. de referencia ***E/00560/2020***), dirigida contra MOVISTAR CARREFOUR ******PROVINCIA.1***, tras expedirse en fecha 5 de febrero de 2019 un duplicado de la tarjeta SIM de la línea ******TELÉFONO.2***, a favor de una tercera persona distinta a la titular de la línea -la parte reclamante uno-.

Estos hechos fueron objeto de una denuncia ante los Mossos d'Esquadra USC de ******LOCALIDAD.3*** (Barcelona) en fecha 7 de febrero de 2019, con número de diligencia ***XXXXXXXXXX***, en la que la parte reclamante uno manifestó lo siguiente*:*

"Que el día 5/02/2019 por la mañana recibió una llamada de una tienda de Movistar de ******PROVINCIA.2*** *con teléfono* ***XXXXXXX*** *en la que se le informaba que una persona estaba solicitando un duplicado de tarjeta SIM del número de teléfono* ******TELÉFONO.2****, que corresponde al declarante.*

Que concretamente le manifestaron que una persona italiana había ido a cinco tiendas de Movistar de ******PROVINCIA.2*** *solicitando un duplicado de tarjeta SIM del número* ******TELÉFONO.2*** *y llevaba una denuncia en la cual decía que había perdido su teléfono móvil con el número de teléfono* ***XXXXXXXXX.***

Que también le manifestaron que en el momento que le solicitaban el DNI este chico se iba de la tienda.

Que los de la misma tienda de Movistar le preguntaron si había autorizado un duplicado de tarjeta.

Que el declarante contestó que no.

Que en fecha de hoy el declarante ha ido a la tienda de Movistar de ******LOCALIDAD.3*** *y le han informado que en fecha de ayer a las 21:48h en un Carrefour de* ******PROVINCIA.1*** *habían hecho un duplicado de la tarjeta con su número de teléfono.*

Que el código de distribuidor donde se hizo es ******CÓDIGO.1*** *y el número de agente que hizo el duplicado es* ******AGENTE.1****.*

Que también le informaron que en el momento que se hizo el duplicado el se quedó sin línea telefónica ya que le dieron de baja." (La traducción del catalán es nuestra).

En relación con esta reclamación, TME, informó a esta Agencia que, el duplicado nunca llegó a efectuarse al completo, ya que el distribuidor no llegó a entregar la tarjeta SIM al suplantador. ***(…).***

QUINTO: Con fecha 6 de marzo de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante dos (expediente con núm. de referencia E/ 03543/2020), dirigida contra CATPHONE y TME, tras expedirse en fecha 13 de febrero 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-.

Estos hechos fueron objeto de dos denuncias ante el Puesto P. de las Rozas de la Comandancia de la Guardia Civil de Madrid en fechas 13 y 18 de febrero de 2020, con números de atestado ******ATESTADO.1***y ******ATESTADO.2*** respectivamente, en las que la parte reclamante dos manifestó lo siguiente:

En la primera denuncia:

"(…) se ha realizado un duplicado de la tarjeta SIM del teléfono ******TELÉFONO.3*** *no autorizado por el denunciante, que el denunciante sobre las 13:00 al realizar una llamada desde su teléfono este no le permite realizar la misma.*

Que empieza a realizar gestiones, se pone en contacto con TELEFONICA MOVISTAR los cuales le informan que ha realizado un duplicado de tarjeta EN UNA TIENDA DE MOVISTAR sita en ******DIRECCIÓN.2*** *de la localidad de* ******LOCALIDAD.4****. Que el denunciante le informa que él se encuentra en Madrid y es imposible que haya autorizado ningún duplicado.*

Que al tener sospechas fundadas de que esto no era normal realiza comprobaciones en su cuenta bancaria DEL BANCO SANTANDER la cual se encuentra a su nombre, observando varios cargos en la misma no autorizados, siendo estos los siguientes:

Han realizado una compra en la empresa REVOLUT por valor de 2.500 euros
Han realizado una compra en la empresa REVOLUT por valor de 3.500 euros.

(…) que recibió un mensaje el lunes 3 de febrero de su banco de (…) su gestor del banco Santander pidiéndole que se pusiera en contacto con el teléfono ******TELÉFONO.4*** *y que el 10 recibió una llamada del departamento antifraude del Banco Santander informándole que había un intento de manipulación de cuentas desde* ******PAÍS.1****, que fue al banco y cambió las claves."*

En la segunda denuncia:

"(…) quiere ampliar los datos de los cargos sufridos en su tarjeta ya que le han realizado más cargos de los que no estaba informado el día que hizo la denuncia.

Que el 13 de febrero de 2020 cuando revisaba sus cuentas observa que le han realizado unos cargos los cuales no ha realizado ni autorizado en su cuenta bancaria ******CUENTA.1*** *y número de tarjeta asociada* ******CUENTA.2****, por un valor de:*

Empresa REVOLUT, 13-02.2020, por valor de 2.500 euros
Empresa REVOLUT, 13-02.2020, por valor de 5.500 euros

Que ese mismo día le han realizado el mismo procedimiento en otra cuenta que tiene con la entidad bancaria ***ES00 0000 0000 0000 0000 0000*** *y número de tarjeta asociada* ******TARJETA.1*** *, por un valor de:*

Empresa REVOLUT, 13-02.2020, por valor de 2.450 euros
Empresa REVOLUT, 13-02.2020, por valor de 3.500 euros"

En relación con esta reclamación, TME, verificó a esta Agencia que, existió una solicitud de ***(…)*** el día 13 de febrero de 2020 a las 11:48 horas a través de ***(…) ***LOCALIDAD.4***" y que ese mismo día a las 17:12 horas, se solicitó ***(…) "(…)".***

SEXTO: Con fecha 23 de octubre de 2020, tuvo entrada en esta Agencia una reclamación formulada por la parte reclamante tres (expediente con núm. de referencia E/ 09638/2020), dirigida contra TME, tras expedirse en fecha 25 de septiembre de 2020, un duplicado de la tarjeta SIM de la línea ******TELÉFONO.5***, a favor de una tercera persona distinta a la titular de la línea -la parte reclamante tres-.

Con fecha 25 de septiembre de 2020, a las 14:40 horas, la parte reclamante tres reci-

bió un correo electrónico remitido por movistarcloud@telefonica.com con el Asunto: Confirmación de la baja en Movistar Cloud.

En esa misma fecha, a las 14:53 horas, la parte reclamante tres, respondió manifestando que: "Yo no he cancelado la suscripción. Ha sido un error o un uso no autorizado de alguien. Por favor póngase en contacto conmigo. ***TELÉFONO.5**"

Con fecha 26 de septiembre de 2020, la parte reclamante tres consultó la aplicación web de TME y constató que como titular de la línea ***TELÉFONO.5** figuraba el Sr. ***F.-F.F.*** con NIE: ***NIE.1.**

Consta la grabación del cambio de titularidad del servicio solicitada en fecha 25 de septiembre de 2020 -con una duración de 02:12 segundos-, por el Sr. ***F.F.F.*** con NIE: ***NIE.1**, en la que facilita sus datos personales (nombre, apellidos y NIE) y los datos personales de la parte reclamante tres (nombre, apellidos, DNI, número de teléfono fijo y número de teléfono de las dos líneas móviles).

Por estos hechos, la parte reclamante tres, presentó tres denuncias ante el Puesto P. de las Rozas de la Comandancia de la Guardia Civil de Madrid en fechas 28, 30 de septiembre de 2020 y 2 de octubre de 2020, con números de atestado ***XXXXXXXXX***, ***XXXXXXXXXX*** y ***XXXXXXXXXX*** respectivamente, en las que manifestó lo siguiente:

En la primera denuncia:

> *"En la tarjeta de debido le han sido realizados un total de tres cargos, sustrayendo un total de 1200 euros.*
>
> *En la tarjeta de débito le han realizado un total de seis cargos, sustrayendo un total de 3899 euros.*
>
> *También le han realizado una transferencia a través de BIZUM de 500 euros, destinado a un tal **E.E.E.** con número de teléfono ***TELÉFONO.6** y una recarga bancaria de 1400 euros.*
>
> *Todo esto hace un total de 6699 euros.*
>
> *El denunciante manifiesta el posible modus operandi del autor: Que a través de un de un cambio de nombre del titular en su contrato, para la línea perteneciente al número ***TELÉFONO.5,** con MOVISTAR vía telefónica, sin su consentimiento, el posible autor realizó el cambio, solicitando una tarjeta SIM a dicha empresa. Anulando la tarjeta SIM del denunciante.*
>
> *Que tras obtener dicha tarjeta SIM el autor realizó los movimientos bancarios a través de un teléfono móvil, debido a que tras realizar cualquier operación con la entidad bancaria, necesita la aprobación vía SMS del número de teléfono que realiza la operación.*
>
> *Tras esto el posible autor se metió en la aplicación de la entidad bancaria Santander y a través de HE OLVIDADO MI CONTRASEÑA, dicho banco le envía SMS al número de teléfono asociado a la cuenta bancaria.*

Que el cambio de titular de la cuenta de MOVISTAR, el denunciante aporta datos del posible autor: ***F.F.F.***NIE.1****.*

Además aporta una transferencia bancaria de 4998 euros que se anuló, la cual iba dirigida a un tal ***XXXXXXXXXX****, siendo el número de cuenta* ***ES00 0000 0000 0000 0000 0000*** *de la entidad bancaria CAIXABANK SA.*

Que el denunciante aporta el contrato fraudulento de MOVISTAR con nombre y apellidos del presunto autor, copia de la última factura del contrato legal del denunciante, datos de la transferencia abortada y los cargos realizados."

En la segunda denuncia:

"Se persona en estas dependencia D. ***D.D.D.*** *para hacer la siguiente corrección sobre la denuncia presentada.*

Que en la diligencia titulada DILIGENCIA DE INICIO POR DENUNCIA DE INFRACCIÓN PENAL MEDIANTE COMPARECENCIA en su párrafo once donde se expresa que todo esto hace un total de 6699 euros debería poner que todo esto hace un total de 6999 euros."

En la tercera denuncia:

"(…) Que el día 01-10-2020 jueves el denunciante se personó en su oficina del Banco Sabadell sita en (…) para recuperar las claves previamente bloqueadas para poder operar.

Que el Banco Sabadell informó que lamentablemente se había emitido una transferencia fraudulenta por importe de 7.003'00 euros a nombre de ***H.H.H.*** *a la cuenta* ***ES00 0000 0000 0000 0000 0000*** *de la entidad bancaria ING motivo por el que se ve obligado a denunciar los hechos para poder recuperar la cantidad defraudada."*

En relación con esta reclamación, TME, informó a esta Agencia que, el 25 de septiembre de 2020, se produjo ***(…)***, pero solo hizo efectivo el cambio en la línea ******TELÉFONO.5***.

SÉPTIMO: Las cuatro reclamaciones presentadas afectan a clientes de la marca Movistar.

OCTAVO: TME cuenta para la marca Movistar con ***(…).***

TME exige ***(…).***

NOVENO: TME cuenta para la marca Movistar con un ***(…).***

DÉCIMO: TME suscribe, ***(…)***

.

UNDÉCIMO: En el contenido del ***"(…)",*** suscrito con ***(…),*** se dispone:

(…).

DUODÉCIMO: TME suscribe,***(…)***.

En la cláusula primera dispone ***(…)***.

En la cláusula segunda dispone ***(…):***

(…).

DÉCIMO TERCERO: En fecha ***(…)*** TME añade una ***(…)",*** que quedan redactados en los siguientes términos:

(…)

DÉCIMO CUARTO: En el contenido del ***(…)*** se dispone:

(…)

RESPONSABILIDAD.

1. (…).
(…).

DÉCIMO QUINTO: TME suscribe con ***(…)***
.

DÉCIMO SEXTO: TME envió un ***(…).***

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.

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

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 TME 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.

Así las cosas, y teniendo en cuenta las consideraciones expuestas, ninguna apariencia de legalidad en la actuación de TME puede inferirse de la participación en el citado GT. Tanto es así que, en las alegaciones se limitó a subrayar su participación, pero no concretó ni determinó en qué medida la AEPD comunicó una cosa y luego hizo otra, en el sentido de qué concreto aspecto extrajo de la participación en el citado grupo, que después se ha visto contradicho por la iniciación de este expediente sancionador.

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 TME, identificando las vulnerabilidades que pudieran existir en los procedimientos operativos implantados, para detectar las causas por las cuales se podrían estar produciendo estos casos, así como encontrar puntos de incumplimiento, mejora o ajuste, para determinar responsabilidades, disminuir los riesgos y elevar la seguridad en el tratamiento de los datos personales de las personas afectadas.

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

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

Asimismo, consta tipificada con sanción de multa administrativa de 20.000.000,00 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

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

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

El artículo 75 de la LPACAP, se refiere a los "Actos de instrucción" como aquellos necesarios para la determinación, conocimiento y comprobación de los hechos en virtud de los cuales deba pronunciarse la resolución. Pues bien, de la instrucción resultó tras el análisis de las pruebas practicadas y de las alegaciones aducidas conforme a lo previsto en los artículos 76 y 77 de la LPACAP, que TME disponía de políticas documentadas de protección de datos en las que se establecía el modo de actuar de TME y de los encargados, ante los tratamientos de datos personales necesarios para la prestación de los servicios contratados y a lo largo de su ciclo de vida. 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 TME, 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 TME 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 ***(…)***, paso previo en muchos casos para obtener un duplicado de la tarjeta SIM.

Así, de la documentación remitida por TME se infiere que los datos personales asociados a la política de seguridad son ***(…)*** sea formulada respecto de algún dato que conozcan únicamente la operadora y su cliente. Ningún requisito suplementario era requerido.

Hemos de significar que, en el caso de la parte reclamante tres bastó con que el suplantador suministrara el ***(…)***, de la parte reclamante tres para procurar el cambio de titularidad. ***(…).***

Asimismo, ***(…).***

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 uno en la que ***(…)*** para obtener el duplicado de la tarjeta SIM. Así, del presunto representante y suplantador se acepta ***(…).***

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 clien-

tes con distintas finalidades (artículo 6.1 RGPD), y la imputación a TME 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 aplicación 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.

TME cita en su descargo una serie de resoluciones dictadas por la AEPD. Pues bien, en el PS/00114/2019 se sancionó por realizar una contratación sin acreditar la representación. Respecto al PS/00453/2019, se sancionó por la contratación fraudulenta de nuevas líneas telefónicas, sin que en ese supuesto se produjese un duplicado de una tarjeta SIM respecto de una línea telefónica preexistente y perteneciente a otro titular (puesto que se trataba de la contratación de una nueva línea que carecía de un titular anterior). Por último, en el PS/00235/2020 se sancionó por falta de diligencia en la aplicación del principio de licitud.

Hay que señalar que, TME 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.

Alega una proscrita inseguridad jurídica o la vulneración del derecho de defensa, sin embargo, la AEPD 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 TME, también seria de aplicación el articulo 85.3 a) del RGPD. En definitiva, TME no determina como puede verse agravada su situación procesal por dicha calificación jurídica, en lugar de la que sostiene, más allá de afirmar que la Agencia incurre en arbitrariedad.

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 puede 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;

TELEFÓNICA MÓVILES ESPAÑA, S.A.U., 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 el que determina la finalidad y medios de los tratamientos

realizados con las finalidades señaladas en su Política de Privacidad: *En Movistar tratamos los datos del cliente o usuario para la prestación del servicio, así como para otras finalidades que el mismo permita o autorice en los términos informados en la presente Política de Privacidad o en las Condiciones específicas de cada Producto o Servicio Movistar contratado.*

(…); CATHPONE-NET, S.L y THADER TELECOMUNICACIONES S.L, actúan en la condición de encargados del tratamiento.

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

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

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

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

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

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

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

PREVIA: SOBRE LA INCOACIÓN DEL EXPEDIENTE SANCIONADOR.

En el Antecedente Cuarto hicimos referencia a los cuatro requerimientos de información dirigidos a TME en distintas fechas que fueron objeto de la correspondiente notificación, en consecuencia, no puede alegar su desconocimiento.

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.

Respecto a la vulneración del principio de buena fe y confianza legítima, no cabe su apreciación.

El 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 responsable de las infracciones apreciadas en la Propuesta de Resolución, a tenor del artículo 28.1 de la LRJSP.

En relación con este principio, la 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.

En definitiva, la participación de TME 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.

Efectivamente las competencias, funciones y poderes que tiene atribuidos la AEPD, se ejercen conforme al ordenamiento jurídico siguiendo los "Principios Generales" del artículo 3 de la LRJSP, entre los que se encuentran la objetividad y transparencia de la actuación administrativa, que aplican a la AEPD, en su condición de entidad de derecho público, en concreto, una autoridad administrativa independiente de ámbito estatal, artículo 109 LRJSP y 44.1 de la LOPDGDD, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

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

I. SOBRE LOS HECHOS QUE MOTIVAN LA INCOACIÓN.

Cuestión de prejudicialidad penal.-

No ha lugar a la petición deducida por cuanto ya se requirió la información durante la instrucción del procedimiento y se constató que no existía identidad de sujeto, hecho y fundamento (artículo 31.1 LRJSP), presupuesto sin el cual no concurre la prejudicialidad penal.

El artículo 31.1 de la LRJSP establece que *"No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento"*.

En el mismo sentido, el artículo 77.4 de la LPACAP dispone: " *En los procedimientos de carácter sancionador, los hechos declarados probados por resoluciones judiciales penales firmes vincularán a las Administraciones Públicas respecto de los procedimientos sancionadores que substancien".*

Así, la SAN de 25 de septiembre de 2019, de la Sala de lo Contencioso-administrativo, Sección 1ª (Rec. 1122/2018) determina que: *"La triple identidad de sujeto, hecho y fundamento entre la infracción administrativa y la infracción penal que pudiera corresponder constituye una exigencia ineludible para que la Administración demandada se encuentre obligada a suspender el procedimiento administrativo sancionador*".

En esta misma sentencia, en la que se desestimaba la pretensión de suspensión del recurso por prejudicialidad penal, se plantea un supuesto idéntico al ahora examinado, donde "*Se funda la sociedad recurrente en la existencia de prejudicialidad penal en la existencia de dos denuncias presentadas ante la*

Policía Nacional. Pues bien, con lo expuesto, en primer lugar, no se acredita si continua la tramitación de dichas denuncias o han sido archivadas, ni siquiera, si se han incoado diligencias previas por algún órgano jurisdiccional, y, por otro lado, no existe identidad de sujeto, pues el sujeto infractor es obvio que no sería el mismo. Así, en relación con las infracciones de la LOPD (LA LEY 4633/1999) el responsable es la entidad AVON, en tanto que el responsable penal de un eventual delito de usurpación de estado civil o estafa sería el tercero que se hubiera hecho pasar por el denunciante, por lo que con lo dicho es suficiente para desestimar el motivo de impugnación que estamos analizando. Cabe decir lo mismo respecto a las diligencias previas que se tramitan en el Juzgado de Instrucción nº. 11 de Madrid, por un ataque a los sistemas informáticos de AVON".

La AEPD no ha ignorado el contenido de las investigaciones que se están llevando a cabo, sino que se ha informado respecto a las personas criminalmente responsables de los delitos denunciados y ha comprobado que no concurren los presupuestos jurídicos para aplicar el precepto invocado. Las Sentencias aducidas (nº 2249/2016 y núm. 1907/2017), se refieren a procedimientos judiciales en distintos órdenes, penal y contencioso administrativo. En este caso, las circunstancias son otras, estamos en la vía administrativa y ante el orden jurisdiccional penal. De hecho, TME reconoce literalmente que *"no hay identidad de sujetos*".

En suma, respecto a los hechos denunciados y los que han sido objeto del expediente sancionador, se advierte con claridad que no concurre entre unos y otros la triple identidad expresada, pues en este expediente sancionador lo que se dilucida es, si TME ha llevado a cabo el tratamiento de los datos de carácter personal respetando los principios relativos al tratamiento (artículo 5.1.f) RGPD), cuestión ajena al objeto de los procesos penales que se sustancien, que por otra parte, protegen bienes jurídicos distintos (por ejemplo: artículo 248.2 del Código Penal en relación con el artículo 249 del mismo texto legal).

PRIMERA. DE LA CONDICIÓN DE TME COMO RESPONSABLE DEL TRATAMIENTO Y DELIMITACIÓN DE LAS OPERACIONES DE TRATAMIENTO.

Sorprende a la Agencia el hecho de que aduzca que no hemos delimitado las operaciones o actividades de tratamiento cuando el Fundamento de Derecho (FD) Cuarto de la Propuesta de Resolución tiene por rúbrica "Tratamiento de datos personales y responsable del tratamiento" que dice: *"(…) la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular"* e identifica al responsable de este *"TELEFÓNICA MÓVILES ESPAÑA, S.A.U, es la responsable de los tratamientos de datos referidos en los antecedentes expuestos".*

En el FD Tercero de esta Resolución se reseñó el objeto de las actuaciones: analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM por parte de TME, no de otras entidades, como las financieras, que invoca.

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 aficione"».*

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. (…)"*

En definitiva, la actividad de tratamiento cuestionada ha sido el procedimiento específico para el cambio de SIM denominado para la marca Movistar "Cambio de tarjeta SIM".

Se remite a las Directrices 07/2020 del CEPD, y a la Sentencia del TJUE de 29 de julio de 2019 para destacar que la condición de responsable del tratamiento puede estar limitada a una etapa particular del procesamiento y que no se le puede responsabilizar de los accesos ilegítimos acaecidos en el marco de la prestación de servicios de cualquier empresa que verifique la identidad de sus clientes a través del teléfono móvil. Pues bien, insistimos, que lo único que se ha cuestionado en este procedimiento, es la adecuación de las medidas de seguridad implementadas por TME para la correcta identificación de los clientes en el momento de expedir el duplicado de la tarjeta SIM.

SEGUNDA. DE LA ADOPCIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS.

2.1 MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

Resultó acreditado en la instrucción del procedimiento que no se había garantizado una seguridad adecuada en el tratamiento de los datos personales, habida cuenta del resultado que produjo la suplantación de identidad. Es decir, un tercero consiguió acceder a los datos personales de los titulares de las líneas sin que las medidas de seguridad que afirmaba TME que existían, hubieran podido impedirlo.

Por consiguiente, y a la vista del resultado producido no estábamos ante una

demostración por parte de TME del cumplimiento de los principios relativos al tratamiento de los datos personales afectados.

Respecto a que la Agencia no aclara en ningún momento porqué considera la operativa contraria al Reglamento, el RGPD se basa en el principio de responsabilidad activa y en relación con la anterior regulación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, donde existía en lo que se refiere a la seguridad un sistema de lista o checklist, ahora es el responsable del tratamiento, y encargado en su caso, el que debe adecuar la implantación de medidas de seguridad al tipo concreto de tratamiento que realice, y precisamente por eso, no por la inexistencia de medidas de seguridad -circunstancia que no concurre en este caso- sino porque de las que disponía TME, no resultaron adecuadas para evitar los hechos producidos.

De igual forma, resultado de la instrucción del procedimiento, se ha constatado la aplicación de nuevas medidas de manera activa y continua para promover y garantizar la protección de los datos en la expedición de los duplicados o incluso en otros tratamientos como es la operativa “Cambio de titular”, cuya última actualización se ha producido en fecha 28 de agosto de 2021.

Se ha constatado que TME ha mejorado la eficacia de los procedimientos tomando acciones, correcciones, introduciendo cambios y refuerzos para mejorar continuamente la prestación de este servicio u otros relacionados con él.

Ha implementado una política de *accountability* y se ha esforzado en demostrar su cumplimiento. Tiene documentadas las decisiones adoptadas en relación con el tratamiento, audita y revisa la seguridad de la información y ha facilitado a la Agencia la información que atañe a la seguridad del tratamiento.

De todo ello, de la documentación anexada y conforme analizamos en el FD Tercero, si bien se concluye el cumplimiento del principio de responsabilidad proactiva, no obstante todo lo anterior, la responsabilidad administrativa es exigible conforme a los Hechos Probados y FD de esta Resolución.

El considerando 78 RGPD declara *“… el responsable del tratamiento debe adoptar políticas internas…”* y el artículo 24.2 establece “*Cuando sean proporcionadas … la aplicación … políticas de protección de datos*”, y que van más allá de la referencia al aspecto formal de la existencia de un documento titulado “Política de protección de datos” donde se realiza la mera reproducción formal del articulado del RGPD y se reduce a una mera declaración de la voluntad de compromiso del responsable con el cumplimiento normativo.

Por consiguiente, la actual política interna de seguridad que aplica TME es coherente con la Directiva PSD2 que obliga adoptar sistemas de “autenticación reforzada de cliente, a pesar no estar incluida en su ámbito de aplicación (artículo 2).

La misma afirmación ha de realizarse respeto al "Plan de inspección de oficio sobre contratación a distancia en operadores de telecomunicaciones y comercializadores de energía" que contiene recomendaciones en materia "*Verificación de la identidad del cliente en procesos posteriores"* y que TME aplica a sus procedimientos:

> *En el Área de Clientes de la web, lo clientes se identifican y autentican a través de código de usuario y contraseña. Debido a que un cliente puede tener contratadas más de una línea, el código de usuario puede ser número de línea (acceso solo a los datos asociados a la línea consultada) o DNI (accesos a todos los datos asociados a las líneas contratadas por el usuario) En los departamentos de Atención al Cliente (canal telefónico) de las diferentes compañías se suele identificar al cliente por nombre completo, DNI y un tercer dato aleatorio como domicilio al que se envían las facturas o número de la cuenta bancaria, aunque muchas compañías proporcionan una contraseña (a solicitud del cliente) que debe ser indicada para proceder al acceso a los datos.*

En cuanto a las siguientes afirmaciones:

> 1.- TME ***(…)***, solo es posible solicitarlo presencialmente en tienda.
>
> Recordemos que en el caso de la parte reclamante tres se produjo ***(…)*** e hizo efectivo el cambio en la línea ******TELÉFONO.5***.
>
> 3.- ***(…).*** Nos remitimos a los hechos probados que han afectado a la parte reclamante tres.

2.2 REVISIÓN Y ACTUALIZACIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

Indudablemente, en la instrucción del expediente se ha puesto de manifiesto la revisión de la medidas técnicas y organizativas.

TME ha reforzado las operativas aplicables a los distintos canales y ha introducido mejoras con el fin de evitar que se reproduzcan hechos similares. Dispone de ***(…).***

Asimismo, reconoce la implantación de sistemas de ***(…).***

Todas estas medidas y esfuerzos de adaptación constante en función de los nuevos riesgos serán objeto de consideración en la condición de "atenuantes".

2.3 VALORACIÓN DE LA ADECUACIÓN, OPORTUNIDAD Y EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS

Los casos declarados por TME durante los ejercicios 2019 y 2020, son un reflejo de la adecuación, oportunidad y eficacia de las medidas adoptadas e implementadas con posterioridad al inicio de las actuaciones realizadas por la

Agencia.

TME reconoce que el fraude ha descendido un 71% en ese periodo. Recordemos que el primer requerimiento de la AEPD es de fecha 13 de enero de 2020.

Si observamos los datos facilitados por TME las cifras por sí mismas expresan la efectividad de las medidas de seguridad adoptadas recientemente, debido precisamente, a la introducción de otras distintas a las preexistentes, que han resultado más adecuadas, oportunas y eficaces.

(…).

Reprocha a la Agencia que no se haya detenido a valorar dichos aspectos.

Precisamente, la imputación que finalmente se efectúa contra TME en la Propuesta de Resolución está referida -únicamente- al artículo 5.1.f) y no al 5.2 RGPD, como inicialmente se consideró en el acuerdo de iniciación. Esta alteración ha tenido un efecto directo en la sanción que inicialmente se consideró y que ascendía a 2.000.000'00. Y ello es así, por lo valoración efectuada (nos remitimos al FD Tercero y al apartado 2.1 de las alegaciones) por la Agencia.

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

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

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

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

dano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

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

En cuanto a la certificación que ostenta por tener implantado un SGCP basado en la Norma UNE 19601, y dado que contiene medidas de vigilancia y control idóneas para prevenir delitos y para reducir de forma significativa el riesgo de cometerlos, la AEPD lo tiene en cuenta en la condición de "atenuante".

Por último, la AEPD no ha dicho que TME aplique una política denominada Know Your Costumer, sino que estas políticas se conocen como tal. El término se refiere a los procesos de identificación o verificación de la identidad que las empresas, especialmente las entidades financieras, pero también las de telecomunicaciones, establecen para garantizar la identidad del cliente.

TERCERA. DE LA RESPONSABILIDAD DE TME EN LOS CASOS DE SUPLANTACIÓN DE IDENTIDAD DE LOS TRES RECLAMANTES

3.1 RESPONSABILIDAD DEL ENCARGADO DEL TRATAMIENTO

Con independencia de las consideraciones que TME realiza acerca de su diligencia en la selección y entrega de instrucciones al proveedor, los preceptos legales mencionados para descartar su responsabilidad son los siguientes:

- En primer lugar, el artículo 28 RGPD. En su apartado 3.c) y 10. Es decir, según TME, el propio RGPD prevé que cuando el encargado del tratamiento trata los datos personales incumpliendo las instrucciones del responsable, se convierte en responsable.

  En relación con este argumento, debe señalarse que en este expediente nunca se ha discutido la posibilidad de que una empresa acuda a técnicas de externalización ("*outsourcing*") para la gestión de determinados procesos. Tampoco se objeta a la consideración de "encargado del tratamiento" de las empresas de las que se vale TME para dicha gestión.

  En efecto, ha quedado acreditado a lo largo de la instrucción que TME ha encomendado la gestión por parte de determinadas empresas de las siguientes actividades:

  - THADER TELECOMUNICACIONES S.L y CATHPONE-NET, S.L, actuarían como distribuidores en establecimientos físicos, para la captación de clientes y realización por estos de determinadas gestiones en su relación contractual con el operador (entre ellas, la expedición de du-

plicados de tarjetas SIM).

- o ***(…)***, como empresa gestora de un centro de atención de llamadas ("*call center*") a través del cual se realizaría la atención telefónica a los clientes del operador. En lo que atañe a este expediente, a través de dicha atención se podrían realizar gestiones de relevancia contractual como el cambio de titularidad de una línea telefónica.

En relación con estos aspectos, y la invocación por parte de TME del artículo 28 RGPD, es preciso señalar inicialmente que deben deslindarse las obligaciones establecidas en el artículo 28.3.d) (adoptar las medidas necesarias por el encargado del tratamiento) de la previsión establecida en el apartado 10 del mismo artículo.

En efecto, este último establece lo siguiente:

> *"Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento"*

Desde un principio debe descartarse que este precepto permita la atribución de responsabilidad sancionadora al encargado. 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 ninguna de las tres empresas haya realizado actuaciones que supusieran una "determinación de los fines y medios", sino que, en palabras de la propia TME, habrían incumplido alguna de las instrucciones emanadas por esta en los procesos de identificación de clientes.

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

- Invoca las Directrices 07/2020 del CEPD. En concreto, el apartado 9:

Este apartado se limita a determinar, de modo genérico, que tanto el responsable como el encargado del tratamiento pueden ser sancionados por el incumplimiento de las disposiciones del RGPD. Nada añade a lo ya establecido en la normativa interna (LOPDGDD), en cuyo artículo 70.1.a) y b) incluye a los responsables y encargados de los tratamientos entre los sujetos sancionables.

La mera existencia de ambas figuras no desplaza al encargado toda la respon-

sabilidad en el tratamiento de los datos personales. Procede ahora, por lo tanto, dilucidar si en este supuesto, si se han vulnerado obligaciones del responsable o del encargado.

A este respecto, ya se indicó en la Propuesta de Resolución que en los tres casos, los encargados actúan por cuenta de TME, en el caso de ***(...).***

Es decir, la intervención instrumental de los encargados tiene como finalidad la iniciación o modificación de las relaciones contractuales entre TME y los usuarios finales de los servicios de comunicaciones electrónicas. A este respecto, conviene acudir a la legislación sectorial, cuya LGTEL establece lo siguiente:

- 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)

- Los canales de comercialización y distribución a que se refiere este expediente (puntos de venta y centro de atención de llamadas) están establecidos para el ejercicio por parte de los usuarios finales de las relaciones contractuales con el operador. Por lo tanto, se refieren al ejercicio de los derechos que como usuarios le corresponden frente a la empresa prestadora del servicio.

- En relación con este aspecto, la LGTEL otorga una naturaleza específica cualificada a los derechos de los usuarios finales de este sector. Tiene la consideración de "obligaciones de carácter público", de acuerdo con lo indicado en el Título III de la Ley, cuyo Capítulo V versa sobre los derechos de los usuarios finales.

- 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" dentro del sector de las comunicaciones electrónicas (Título III, capítulo IV).

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

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

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

Conviene recordar que los hechos enjuiciados en el presente expediente han consistido precisamente en eso, es decir, en la expedición inadecuada de tarjetas SIM que han permitido a terceros ajenos a la línea acceder a ella. Queda afectado, por lo tanto, el derecho del usuario final que tiene la consideración de obligación de carácter público.

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

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

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

Como ha quedado acreditado en este expediente, los puntos de venta y centros de atención de llamadas telefónicas eran utilizados para la expedición de duplicados de tarjetas SIM. A estos efectos sería de aplicación, en la identificación de los clientes, la mencionada Ley 25/2007. Esta Ley, en el momento de su aprobación, era consciente de la posibilidad de uso de entidades externas en los procesos de contratación de líneas, no obstante lo cual, estableció en todo caso a los operadores como sujetos obligados. Un posible fallo en la identificación por parte de un distribuidor sería en todo caso imputable al operador.

Por lo tanto, se encuentran involucrados en la gestión de clientes por parte de los operadores de telecomunicaciones, aspectos directamente relacionados con los servicios de interés general, las obligaciones de carácter público y, sobre todo, la Seguridad pública del Estado. Esto impide considerar que pueda exonerarse al operador de servicios de comunicaciones electrónicas de la responsabilidad por el mero hecho de haber externalizado sus servicios de canal de atención al cliente.

En este sentido, en la prestación de los servicios de comunicaciones electrónicas, el operador siempre habría dispuesto de la opción de prestar por sí mismo el servicio de atención al cliente, en lugar de acudir a técnicas de externalización. El uso de una u otra opción no puede hacer que se derive la responsabilidad cuando se hallan implicados aspectos de tan relevante naturaleza.

Por lo demás, conforme a la documentación aportada por TME, se observa que en los contratos que mantiene con los encargados (tanto THADER y CATPHONE por un lado, como con ***XXXXXX***, por otro) se incluye ***(…).***

En efecto, en ***(…)***, se indica:

(…).

Idéntica cláusula figura en los contratos de distribución suscritos por TME con THADER y CATPHONE.

En función de lo anteriormente expuesto, procede desestimar la alegación aducida y se considera que TME es la responsable de garantizar la seguridad y confidencialidad de los datos personales tratados. Por consiguiente, sin perjuicio de las obligaciones establecidas en otras leyes, los tratamientos que realice TME deben cumplir con la normativa de protección de datos.

3.2 RESPONSABILIDAD DE LAS ENTIDADES BANCARIAS

En tanto que estas entidades son responsables del tratamiento de los datos de sus clientes, 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.

II. SOBRE LOS FUNDAMENTOS DE DERECHO

PRIMERA. SOBRE LA PRESUNTA INFRACCIÓN QUE CONTINÚA CONSIDERÁNDOSE COMETIDA POR PARTE DE TME: VULNERACIÓN DEL PRINCIPIO DE TIPICIDAD

Es cierto que la Agencia reconoció que *"TME **(…)** en las que se establece el modo de actuar de TME y de los encargados*" pero también el hecho de que, a pesar de su existencia, la infracción se produjo.

1.1 SOBRE LA CONDUCTA DE TME: EN NINGÚN CASO PODRÍA CONSIDERARSE SUBSUMIBLE EN EL ARTÍCULO 5.1 F) RGPD.

La incardinación de los hechos en el precepto 5.1.f) RGPD, ha sido objeto de análisis en el FD Tercero.

Sobre la infalibilidad alegada por TME, debe indicarse que 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 TME e inevitablemente, el resultado. Esos tres elementos son los que van a determinar la adecuación al riesgo y no como pretende centrar el debate, TME, sobre si es infalible o no su sistema.

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 ade-

cuación 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.

1.2 SOBRE LA REDACCIÓN DE LA NORMATIVA QUE RESULTA DE APLICACIÓN: CONCEPTOS JURÍDICOS INDETERMINADOS QUE CONTRIBUYEN A INCREMENTAR LA INSEGURIDAD JURÍDICA E INDEFENSIÓN DE TME.

Cabe señalar, que, en el Derecho de la Unión Europea (UE), la protección de datos ha sido reconocida como un derecho fundamental específico. Está recogido en el artículo 16 del Tratado de Funcionamiento de la UE, así como en el artículo 8 de la Carta de los Derechos Fundamentales de la UE. En vista de los rápidos avances tecnológicos, la UE adoptó en 2016 nueva legislación para adaptar la normativa de protección de datos a la era digital. El RGPD entró en vigor en mayo de 2018 y en el artículo 4 dispone una serie de "Definiciones" o conceptos jurídicos determinados entre los que no se incluyen los invocados por TME: seguridad adecuada, medidas técnicas y organizativas apropiadas o nivel de seguridad adecuado al riesgo.

Efectivamente, estamos ante conceptos jurídicos indeterminados, conceptos abstractos, que sólo pueden ser concretados en su aplicación práctica. Para la aplicación de estos conceptos la Agencia ha hecho una valoración fundada en criterios técnicos y razonamientos lógicos desarrollados en los FD que sustentan esta Resolución y que, en ese margen de apreciación, permiten prever, con suficiente seguridad, la conducta sancionada.

Hay que hacer referencia a una precisión efectuada por el Tribunal Constitucional en el Auto 100/2001, de 26 de abril:

> *Conforme a la doctrina de este Tribunal el derecho al principio de legalidad del art. 25.1 CE, en el que se incluye la exigencia de certeza en la predeterminación de las conductas punibles, no es incompatible con la utilización por el legislador de conceptos jurídicos indeterminados, cuyo significado último haya de ser inferido por el intérprete mediante una valoración sistemática de todos los elementos que integran la norma, atendiendo a la finalidad y fundamento de la misma (SSTC 69/1989, de 20 de abril, FJ 1; 305/1993, de 25 de octubre, FJ 5; 26/1994, de 27 de enero, FJ 4; 184/1995, de 12 de diciembre, FJ 3). El lenguaje de la ley no es tan perfecto que permita descartar, en todo caso, la imprecisión o la anfibología. Por ello, lo que el art. 25.1 CE exige al legislador es que la conducta descrita en la norma y objeto de sanción, sea suficientemente recognoscible por sus eventuales destinatarios, debiendo rechazar el aplicador todas aquellas interpretaciones que claramente no encuentren cobertura en la misma. Contrariamente, cuando mediante una elemental inferencia lógica el intérprete pueda concretar sin dificultad la previsión normativa, el precepto sancionador en cuestión cumplirá con los requisitos de tipicidad y certeza requeridos por el art. 25.1 CE, aunque el sancionado recurrente -como ocurre en este caso- alegue una diversa interpretación de la norma en relación con la llevada a cabo por el Consejo General del Poder Judicial*

en el ejercicio de su potestad disciplinaria. En tales supuestos, el control de este Tribunal tiene por objeto evitar que la interpretación del órgano sancionador, ampare aplicaciones de la norma en las que ésta se proyecte sobre conductas que, con arreglo a su contenido, no podrían previsible y razonablemente incardinarse en el tipo o ilícito descrito por aquélla.

1.3 SUBSIDIARIAMENTE: SOBRE LA INTERPRETACIÓN Y APLICACIÓN DE LA NORMATIVA REALIZADA POR ESTA AGENCIA. RIESGO DE VULNERACIÓN DEL PRINCIPIO DE ESPECIALIDAD.

En la fase de instrucción del expediente sancionador, el órgano instructor, ya se planteó la concurrencia de distintos tipos infractores, optándose por la aplicación del artículo 83.5 del RGPD, al ser una infracción más grave, cuya justificación ha sido objeto de aclaración en el FD Tercero.

Hay que destacar, que la Memoria 2021 de la Fiscalía General del Estado dedicado a la "Criminalidad informática" dedica en su punto 8 una mención a las actuaciones fraudulentas online:

"En este breve repaso de las actuaciones fraudulentas online, es obligada la mención de las conductas que afectan al sector de las telecomunicaciones en sus distintas variantes, y muy relacionadas con ellas, aunque el perjuicio se genera en la banca online, el conocido vulgarmente como fraude SIM Swapping, que está siendo utilizado con alarmante frecuencia en los últimos años. La técnica consiste en burlar las medidas de seguridad de las entidades bancarias accediendo a los códigos alfanuméricos de confirmación, de uso único, generados con ocasión de las transacciones electrónicas y que ordinariamente se comunican a los/as clientes a través de mensajes SMS. Para ello, los/as delincuentes obtienen previamente un duplicado o una nueva tarjeta SIM a nombre de su víctima, ya sea solicitándola del operador correspondiente, simulando la identidad de aquella, ya sea valiéndose de una metodología más elaborada, como en el supuesto objeto de instrucción judicial en Zamora, en el que se aprovechaba con esa finalidad un establecimiento de reparación de móviles. Una vez tienen la tarjeta SIM a su disposición, los delincuentes se garantizan la recepción en su propio dispositivo del código de confirmación de la transacción fraudulenta y, en definitiva, la posibilidad de hacer efectiva la misma en su beneficio, evitando que en ese momento sea conocida por el perjudicado o perjudicada. Esta forma de defraudación ha generado en los últimos años múltiples investigaciones policiales y la incoación de procedimientos judiciales en distintos territorios como A Coruña y Valencia. Su efectividad y la facilidad con que los/as delincuentes logran sus ilícitos propósitos ha determinado la adopción por los operadores de telefonía de medidas específicas de prevención y fortalecimiento de las garantías para la emisión de estas tarjetas o de sus duplicados."

Los hechos controvertidos, se consideran de la suficiente relevancia y gravedad, como para, en aplicación del principio de especialidad, subsumirlos en una vulneración del artículo 5.1.f) del RGPD, precisamente, porque no se ha garantizado la seguridad de los datos de los clientes -de for-

ma adecuada-, y en consecuencia, se ha producido un tratamiento no autorizado e ilícito que afecta a la confidencialidad de dato y que ha devenido en otras consecuencias, nada triviales, como son los perjuicios económicos, que no se hubieran producido, si TME, hubiera asegurado la identidad y autentificación correcta de sus clientes.

SEGUNDA. SOBRE LA TIPIFICACIÓN DE LA PRESUNTA CONDUCTA EN OTROS PROCEDIMIENTOS SANCIONADORES INCOADOS A TME Y TELEFÓNICA DE ESPAÑA, S.A.U (TDE): ERROR EN LA CALIFICACIÓN DE LA INFRACCIÓN.

En el FD Tercero ya aclaramos que no se trata de un error en la calificación de la infracción sino de una interpretación que, por razón de los hechos, la Agencia lo califica así.

Es el artículo 27 de la LRJSP bajo el epígrafe de “Principio de tipicidad”, el que dispone:

1. Sólo constituyen infracciones administrativas las vulneraciones del ordenamiento jurídico previstas como tales infracciones por una Ley, sin perjuicio de lo dispuesto para la Administración Local en el Título XI de la Ley 7/1985, de 2 de abril.

Las infracciones administrativas se clasificarán por la Ley en leves, graves y muy graves.

2. Únicamente por la comisión de infracciones administrativas podrán imponerse sanciones que, en todo caso, estarán delimitadas por la Ley.

Integrados los hechos en los artículos 83.5.a) del RGPD y 72.1.a) de la LOPDGDD, se cumple con las exigencias de predeterminación normativa y certeza que se derivan de los principios de legalidad y seguridad jurídica (artículos 9.3 y 25 CE).

TERCERA. LA CONDUCTA DE TME NO ES ANTIJURÍDICA

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.

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 están 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 reali-

cen un tratamiento de los mismos 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 ello, se desestima la alegación aducida. La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable del tratamiento, que es quien determina la existencia del tratamiento y su finalidad. Recordemos que, con carácter general las operadoras tratan los datos de sus clientes al amparo de lo previsto en el artículo 6.1 b) del RGPD, por considerarse un tratamiento necesario para la ejecución de un contrato en el que el interesado es parte (…).

CUARTA. AUSENCIA DE CULPABILIDAD

Alude a la diligencia profesional con la que ha actuado.

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

Así, la infracción devino 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.

No basta con disponer de una política de seguridad, sino que hay que 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. En este contexto, el RGPD exige que los responsables del tratamiento implementen medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los “riesgos de diversa probabilidad y gravedad para los derechos y libertades de

las personas físicas” (artículo 24.1) aplicando las medidas oportunas.

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.

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".*

En el caso de la parte reclamante uno, se produce un intento de duplicado correspondiente al número de teléfono ******TELÉFONO.2,*** en fecha 5 de febrero de 2019, que afortunadamente no fructifica en la entrega a la persona suplantadora. Sin embargo, y a pesar de que cambió de número de teléfono ******TELÉFONO.1***, vuelve a verse afectado por un segundo intento, un mes después -en fecha 6 de marzo de 2019-, que desafortunadamente, sí se materializa y es objeto de entrega a la persona suplantadora, quedándose sin línea y perdiendo el control, en consecuencia, de sus datos personales. Recordemos que es el propio afectado quien manifiesta recibir un aviso mediante una llamada telefónica desde ******PROVINCIA.2*** de un posible intento de suplantación. Destaquemos, además, la existencia de un correo electrónico redactado por personal de TME, de fecha 7 de marzo de 2019, en el que se reconoce que quién expide el segundo duplicado, ***(…)***. A esto hay que añadir, la residencia en ******LOCALIDAD.4***, provincia de Barcelona del afectado, y ***(…)*** ubicado en ******LOCALIDAD.2*** (******PROVINCIA.2***) y la expedición del segundo duplicado en ***(…)*** la ciudad de ******PROVINCIA.1***.

En cuanto a la parte reclamante dos, se expide el duplicado ***(…)*** en ******LOCALIDAD.4*** (Barcelona) cuando el afectado tiene su domicilio en Las Rozas (Madrid).

(…).

En el caso de la parte reclamante tres, se produce ***(…),*** que deviene en la expedición de un duplicado de la línea ******TELÉFONO.5***, aun habiendo contactado con TME trece minutos después de recibir el correo electrónico que le confirma la baja en Movistar Cloud. Asimismo, se ha podido comprobar que en la grabación del cambio de titularidad del servicio aportada por el afectado, ***(…).*** No estaríamos, por lo tanto, ante un engaño de un tercero, sino ante la existencia de unas medidas de seguridad que entonces se manifestaron como insuficientes, devinieron inapropiadas y no garantizaron un nivel de seguridad adecuado en el proceso de verificación de la identidad de los solicitantes de un cambio de servicio. 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.

4.1 LA ACTUACIÓN DILIGENTE, DE BUENA FE Y CONFIANZA LEGÍTIMA DE TME

Aduce lo llamativo que resulta que, en la Propuesta de Resolución, por un lado, se indiquen ciertas afirmaciones que incluyan valoraciones positivas y por otra parte, se indiquen otras en sentido contrario.

Es cierto que como operadora está sujeta a las “Obligaciones de servicio público y derechos y obligaciones de carácter público en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas” de la LGTEL.

Ahora bien, TME no puede negar el hecho de que trata datos de carácter personal a gran escala. Es la propia operadora la que reconoce tener más de ocho millones de clientes.

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.

4.2 DILIGENCIA DEBIDA EN LA ELECCIÓN Y SUPERVISIÓN DE LOS ENCARGADOS DEL TRATAMIENTO Y RESPONSABILIDAD DE ESTE:

Apela también a la existencia de circunstancias excepcionales y ajenas a

TME y a la diligencia debida demostrada, por cuanto no puede ser considerada responsable de los incumplimientos excepcionales de la operativa llevada a cabo por parte de los encargados del tratamiento. Esta alegación debe ser desestimada por cuanto los contratos suscritos, ya prevén que los tratamientos efectuados por los encargados se harán en nombre del responsable, es decir, TME (artículo 29 RGPD).

De las afirmaciones de TME 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. También podríamos rebatir la incongruencia de estas afirmaciones por cuanto, por un lado, aduce una diligencia debida en su elección y supervisión, invoca la STS 1232/2018 para confirmar que ha cumplido con los deberes de vigilancia, y por otro, los responsabiliza de los hechos.

Asimismo, el hecho de que la Agencia haya reconocido que existan ciertas cláusulas que definan los términos de las relaciones con los encargados del tratamiento, no le exime de la gestión del riesgo, que es uno de los pilares de la dirección de cualquier organización. Toda entidad, cuando pretende prestar con garantías un servicio, debe gestionar los elementos de incertidumbre que se derivan de su naturaleza, ámbito, contexto y fines.

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. (…)

4.3 CIRCUNSTANCIAS EXCEPCIONALES Y AJENAS A TELEFÓNICA:

• Posible negligencia en el cuidado de los datos personales por parte de los usuarios: los propios usuarios tienen la responsabilidad de custodiar debidamente sus datos personales.

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".*

Es cierto que queda fuera del ámbito de responsabilidad de TME la información personal que puedan compartir los afectados. Lo que sí está dentro de su esfera de control es la definición de los procedimientos, sistemas, controles y medidas de seguridad aplicables en función de la criticidad del tratamiento que aseguren la correcta identificación del titular de la línea.

• Probable responsabilidad de terceros ajenos a TME, como las entidades bancarias que han operado en cada caso

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

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

car la identidad del usuario, más segura es la transacción.

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

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

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

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

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

• Acciones intencionadas de terceros para la comisión de un delito

En cuanto a la falta de responsabilidad de TME, debe indicarse que, con carácter general TME trata 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 o para la aplicación a petición de este de medidas precontractuales. En otros casos, fundamenta la licitud del tratamiento en las bases previstas en el artículo 6.1.a) y f) del RGPD.

Es cierto, que, para completar la estafa, es necesario que un tercero "suplante la identidad" del titular de los datos, para recibir el duplicado de la tarjeta SIM. 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 dónde 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 cuanto a que los agentes comerciales del canal presencial y telefónico han sido engañados e inducidos a cometer errores humanos a la hora de aplicar la operativa de identificación diseñada, cabe señalar que TME debe estar en disposición de establecer mecanismos que impidan que se produzca la duplicación fraudulenta de las tarjetas SIM, medidas que respeten la integridad y confidencialidad de los datos y que impidan que un tercero acceda a datos que no son de su titularidad, pues precisamente compete a la operadora tratar datos de carácter personal conforme al RGPD (considerandos 76, 77, 78, 79, 81 y 83 RGPD; artículo 32 del RGPD y artículo 28 de la LOPDGDD)

Ya hemos consignado en los Hechos Probados, la existencia de los contratos y clausulas aplicables. Ahora bien, TME no puede eludir la responsabilidad que le corresponde respecto a la seguridad del tratamiento, escudándose en la existencia de cláusulas contractuales que afirma han sido incumplidas por parte de los encargados. Recordemos que en los tres casos, los encargados actúan por cuenta de TME, en el caso de ***(…)*.**

Para mejorar el cumplimiento de las políticas por parte de los distribuidores las instrucciones que se les muestran deben ser claras, siendo recomendable la inclusión de estas en el sistema de información, dentro del proceso de cambio de SIM, incluso con controles en las pantallas del sistema tales como botones de aceptación que impidan la continuidad del proceso si no se acepta haber realizado una determinada acción.

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

Por lo tanto, TME como responsable del tratamiento está obligada a verificar tanto la selección como el nivel de efectividad de los medios técnicos utilizados. La exhaustividad de esta verificación debe evaluarse a través del prisma de adecuación a los riesgos y la proporcionalidad en relación con el estado del conocimiento técnico, los costos de implementación y la naturaleza, el alcance, el contexto y los propósitos del tratamiento.

No se aprecia la concurrencia de fuerza mayor. Tal y como indicaba la instructora en la Propuesta de Resolución, en los casos descritos en el apartado de hechos probados, no se garantizó la seguridad de los datos de forma efec-

tiva, y en particular, su correcta custodia para evitar la pérdida, sustracción o acceso no autorizado.

QUINTA. INCUMPLIMIENTO DEL PRINCIPIO DE PROPORCIONALIDAD

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

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

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

Y por último, es disuasoria. Una multa disuasoria es aquella que tiene un efecto disuasorio genuino. A este respecto, la Sentencia del TJUE, de 13 de junio de 2013, Versalis Spa/Comisión, C-511/11, ECLI:EU:C:2013:386, dice:

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

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

de febrero de 2012, Total y Elf Aquitaine/Comisión, C-421/11 P, apartado 82)."

La Sentencia de fecha 11 de mayo de 2006 dictada en el recurso de casación 7133/2003 establece que: "*Ha de tenerse en cuenta, además, que uno de los criterios rectores de la aplicación de dicho principio régimen sancionador administrativo (criterio recogido bajo la rúbrica de «principio de proporcionalidad» en el apartado 2 del artículo 131 de la citada Ley 30/1992) es que la imposición de sanciones pecuniarias no debe suponer que la comisión de las infracciones tipificadas resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas".*

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

SEXTO: **Principios relativos al tratamiento.**

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

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

1. Los datos personales serán:

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

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

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

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

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

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

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

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

En este sentido, el considerando 75 del RGPD determina: *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*.

Asimismo, el considerando 83 del RGPD establece: *A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la 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 tres 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, los reclamantes ven afectados sus poderes de disposición y control sobre sus datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos según ha señalado el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre de 2000 (FJ 7). De manera que, al conseguir un duplicado de la tarjeta SIM, se posibilita bajo determinadas circunstancias, el acceso a los contactos o a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder modificar las contraseñas. De hecho, la parte reclamante dos denuncia que: "*En mi caso, el ladrón cogía las llamadas que se le hacían a mi número de teléfono. Yo mismo, llegué a hablar con él*". 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 al facilitar TME duplicados de la tarjeta SIM a terceras personas que no son las legítimas titulares de las líneas móviles e incluso modificar la titularidad de los servicios contratados (parte reclamante tres), tras la superación por las personas suplantadoras de las políticas de seguridad implantadas por la operadora, lo que evidencia un incumplimiento del deber de proteger la información de los clientes.

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

La emisión y entrega del duplicado a un tercero no autorizado supone para los afectados la pérdida del control de sus datos personales. Por lo tanto, el valor de ese dato personal, integrado en un soporte físico -tarjeta SIM-, es real e incuestionable, motivo por el cual TME tienen el deber legal de garantizar su seguridad, tal como lo haría con cualquier otro activo.

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

> **"4.** Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.
>
> Ahora bien, con la inclusión del vigente art. 18.4 CE el constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona", pero que es también, "en sí mismo, un derecho o libertad fundamental" (STC 254/1993, de 20 de julio, FJ 6). Preocupación y finalidad del constituyente

que se evidencia, de un lado, si se tiene en cuenta que desde el anteproyecto del texto constitucional ya se incluía un apartado similar al vigente art. 18.4 CE y que éste fue luego ampliado al aceptarse una enmienda para que se incluyera su inciso final. Y más claramente, de otro lado, porque si en el debate en el Senado se suscitaron algunas dudas sobre la necesidad de este apartado del precepto dado el reconocimiento de los derechos a la intimidad y al honor en el apartado inicial, sin embargo, fueron disipadas al ponerse de relieve que estos derechos, en atención a su contenido, no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada. De manera que el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto.

5. ***(…)***

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

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

  · 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:

  No es que la AEPD haya valorado de forma diferente las distintas circunstancias concurrentes del precepto, sino que optó por una valoración independiente para que el análisis de cada una resultara más claro. No obstante, nada impide un análisis conjunto que es el siguiente:

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

  Alude a la SAN 496/2017, si bien, consideramos que las circunstancias a las que se refiere son distintas. En aquel caso, se imputaba una vulneración del artículo 77.37 de la LGTEL. La Audiencia consideró que el incumplimiento o cumplimiento incorrecto de la obligación, en la tramita-

ción de las bajas, no ocasionó una grave vulneración de los derechos de los consumidores y usuarios finales, por lo que resultó ser más favorable la calificación de la infracción como leve.

Con relación al periodo temporal respecto al que acontecen los hechos, si bien los hechos denunciados por las partes reclamantes acontecen en fechas determinadas, TME declaró en el ejercicio 2019 para la marca Movistar un total de ***XXX*** casos y en las actuaciones previas de investigación aportó un listado de ***XX*** casos que van desde el 14 de enero de 2020 hasta el 12 de junio de 2020. Por lo tanto, la aplicación como atenuante de artículo 76.2.a) de la LOPDGDD -carácter continuado de la infracción- como afirma TME, es incompatible con la apreciación de la duración de la infracción como circunstancia agravante, que, mantenemos como tal.

El porcentaje de solicitudes fraudulentas de tarjeta SIM declarado por TME en el ejercicio 2019 asciende al ***X,XXXXX*** % respecto al total de cambios de tarjeta SIM gestionados: ***XXXXXXX*** cambios.

El porcentaje de solicitudes fraudulentas de tarjeta SIM declarado por TME hasta el mes de junio de 2020 asciende al ***X,XXXXX*** % respecto al total de cambios de tarjeta SIM gestionados: ***XXXXXX*** cambios.

En concreto, para la marca Movistar, la cifra correspondiente a 2019 (***XXX*** casos) se desagrega de la siguiente forma:

(…).

Los casos detectados y notificados a la Agencia hasta el mes de junio de 2020 ascienden a ***XX*** casos.

Y si bien, los casos denunciados han sido tres, las actuaciones previas de investigación identificaron la existencia de otros casos (TME declaró para la marca Movistar en el ejercicio 2019 un total de ***XXX*** casos y aportó un listado de ***XX*** casos que van desde el 14/01/2020 al 12/06/2020).

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

Es cierto que TME no es responsable de las políticas de identificación de clientes establecidas por las entidades bancarias ni se le puede atribuir la responsabilidad por e raude bancario. No obstante, también es cierto, que si TME asegurase el procedimiento de identificación y entrega, ni siquiera podría activarse el sistema de verificación de las entidades bancarias. La persona estafadora tras conseguir la activación de la

nueva SIM, toma el control de la línea telefónica, pudiendo así, a continuación, realizar operaciones bancarias fraudulentas accediendo a los SMS que las entidades bancarias envían a sus clientes. Esta secuencia de hechos puesta de manifiesto en las reclamaciones interpuestas genera una serie de daños y perjuicios graves que deberían haberse tenido en cuenta en una evaluación de impacto relativa a la protección de datos (considerando 89, 90, 91 y artículo 35 del RGPD). En definitiva, desde el momento que se entrega un duplicado a una persona distinta a la titular de la línea o persona autorizada, el cliente pierde el control de la línea y los riesgos, daños y perjuicios, se multiplican. Además, los hechos acontecen con una inmediatez abrumadora.

En suma, la aplicación del agravante del artículo 83.2.a) del RGPD se refiere a 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 los sucesos ocurridos con las tres partes reclamantes no pueden ser considerados en modo alguno como una muestra representativa del nivel de compromiso demostrado por TME en el cumplimiento de sus obligaciones en materia de protección de datos y, mucho menos, del grado de eficacia que revisten unas políticas de seguridad que están diseñadas para atender a un volumen de clientes que supera los 8 millones y que el porcentaje de solicitudes fraudulentas es mínimo.

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

Negar la concurrencia de una actuación negligente por parte de TME 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 ilus-

trativa, 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".*

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

- Artículo 83.2.d) RGPD:

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

    Alega no entender la conclusión de la Agencia que califica el grado de responsabilidad como alto.

    La responsabilidad de las vulnerabilidades en el procedimiento para la expedición del duplicado de tarjeta SIM corresponde a TME.

    Los encargados del tratamiento -los distribuidores y proveedores, en su caso- solo tratan los datos siguiendo las instrucciones documentadas del responsable y contractualmente están definidas las consecuencias de su incumplimiento.

    Los datos personales que recaba TME 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).

La Agencia considera que TME ha mitigado los riesgos a raíz de la investigación iniciada y ha incrementado las medidas de seguridad con el fin de poder garantizar la identidad del cliente. Ha presentado documentación para determinar con certeza el momento en que se han tomado las medidas una vez producidos los hechos.

Por consiguiente, es responsable de no haber hecho todo lo que podía esperarse que hiciera, habida cuenta de la naturaleza, los fines o el ámbito de la operación de tratamiento, a la luz de las obligaciones que le impone el RGPD.

- Artículo 83.2.e) RGPD:

  · Toda infracción anterior cometida por el responsable del tratamiento:

  Aduce TME que no se refieren al mismo tipo infractor.

  Se estima, en parte, la alegación aducida y únicamente se consideran como agravante aquellas infracciones anteriores al Acuerdo de Inicio cometidas por TME, que se consideran pertinentes o relevantes.

  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 los dos procedimientos en que se ha sancionado a TME (resoluciones firmes en vía administrativa) consecuencia de tratamientos sin legitimación por fraudes de identidad.

Núm. procedimiento	Fecha resolución sancionadora	Infracción imputada	Sanción
PS/00453/2019	18/03/2020	6.1. RGPD	40.000,00
Contratación fraudulenta de líneas telefónicas sin consentimiento de la persona afectada.			
PS/00235/2020	21/01/2021	6.1.RGPD	75.000,00
Se produce un cambio de titularidad de la línea a favor de un tercero, sin que se hubiese realizado ningún tipo de comprobación de identidad al respecto.			

- Artículo 83.2.g) RGPD:

  · Categorías de datos personales afectados por la infracción:

  El dato personal afectado por el tratamiento tiene una naturaleza especialmente sensible ya que posibilita la suplantación de identidad.

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

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

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

- Artículo 76.2.b) LOPDGDD:

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

  El desarrollo de la actividad empresarial que desempeña TME

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 TME como una de las operadoras de telecomunicaciones más grandes de nuestro país. No procede, como pretende TME, su aplicación como atenuante.

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, teniendo en cuenta la complejidad de implementar nuevas medidas.

    A saber:

    (…).

    Artículo 83.2.f) RGPD:
  - Grado de cooperación con la autoridad de control:

    Alto. La Agencia considera que TME ha cooperado de forma favorable con la investigación, proporcionando respuesta a la mayoría de los requerimientos y formando parte del GT.
- Artículo 76.2.c) LOPDGDD:
  - Los beneficios obtenidos como consecuencia de la comisión de la infracción.

    No considera esta Agencia que TME 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 TME, suscribieron con AUTOCONTROL un Protocolo que, sin perjuicio de las competencias propias de la AEPD, prevé mecanismos para la resolución privada de controversias relativas a la protección de datos en el ámbito de contratación y publicidad de servicios de comunicaciones electrónicas, con fecha 15 de septiembre de 2017. Protocolo cuya aplicación efectiva debe ser considerado como atenuante.

Se estiman las alegaciones aducidas en lo relativo a los siguientes atenuantes, que pasan a tenerse en cuenta:

- Artículo 83.2. j) RGPD:

  En lo relativo a la adhesión a mecanismos de certificación aprobados con arreglo al artículo 42. TME dispone de un Sistema de Gestión de Compliance Penal acreditado de conformidad con la norma UNE 19601.

Se desestiman las alegaciones aducidas en lo relativo al factor atenuante previsto en el artículo 83.2.k) del RGPD. TME no acredita la existencia de las pérdidas económicas sufridas. La complejidad de implementar nuevas medidas, así como la auditoría del Modelo de Organización y Gestión para la Prevención de Delitos ha sido objeto de valoración a través de la atenuante prevista en el artículo 83.2.c) RGPD. Por último, la concurrencia de obligaciones derivadas de la normativa aplicable opera tanto frente a personas físicas como jurídicas.

Asimismo, y siguiendo el criterio expresado por la SAN, Sala de lo Contencioso-administrativo, Sección 1ª, Sentencia de 5 May. 2021, Rec. 1437/2020, finalmente se descarta como factor atenuante el dispuesto en el artículo 76.2.a) LOPDGDD, relativo al carácter continuado de la infracción, que no concurre. Según esta sentencia: "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante".*

También se desestima la alegación relativa a la aplicación del artículo 76.2.d) LOPDGDD: "*La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción*".

TME ha aducido que los duplicados no habrían sido posibles si el suplantador no hubiese realizado una previa captación ilegítima de los datos personales de dichos clientes.

Pues bien, el precepto conecta la conducta del afectado con la comisión de una infracción: la posibilidad de que la conducta del interesado induzca a la comisión de la concreta infracción imputada al reclamado por parte de la AEPD. Recordemos que se imputa a TME la infracción del art. 5.1.f) del RGPD; no se le imputa el fraude, ni el tratamiento de datos sin legitimación, sino una falta de garantías de las medidas de seguridad que produce una cesión de datos a un tercero.

Así, en el supuesto ahora examinado la infracción imputada por falta de garantías de las medidas de seguridad es una obligación impuesta por el ordenamiento jurídico al responsable del tratamiento, de la que es íntegramente responsable, de tal forma que la conducta del interesado (en su caso, suministrar por engaño, descuido o voluntariamente sus datos al tercero que le suplanta, pues debe considerarse que, en este caso, el tercero puede haber obtenido los datos sin la intervención del afectado) es independiente del deficiente establecimiento, mantenimiento o control de las medidas de seguridad fijadas por el responsable del tratamiento. La infracción es ajena a la actuación del interesado y nada de lo que haga este último influiría en su comisión.

Por otro lado, se considera que el precepto se focaliza en la conducta sólo del interesado y no de un tercero interpuesto entre el interesado y aquel

que comete la infracción. Esto es, parece que liga de forma directa una acción u omisión del interesado con esa inducción. La actuación de un tercero, en lo que podríamos denominar una segunda fase -tras una primera de obtención de los datos-, frente al responsable del tratamiento y la conducta del tercero respecto a la inducción de la comisión de la infracción, excedería del ámbito de actuación del afectado. El interesado no controla ni lo que hace el tercero con sus datos ni el comportamiento del tercero. Además, el legislador ha mencionado sólo al afectado y no a un tercero en la literalidad del precepto.

En el caso expuesto, dado que quien ha actuado frente a la operadora es un tercero y no el interesado, no se daría el supuesto de hecho preciso para aplicar este atenuante. Es la conducta del tercero (un delincuente) que se hace pasar por el interesado la que induce al responsable a actuar autorizando un duplicado de tarjeta SIM.

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 **TELEFÓNICA MÓVILES ESPAÑA, S.A.U.**, con CIF A78923125, 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 900.000'00 euros (novecientos mil euros).

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

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

938-131120

Mar España Martí
Directora de la AEPD