Expediente N.º: EXP202305829

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes:

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 21 de marzo de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra TELEFÓNICA MÓVILES ESPAÑA, S.A.U. con NIF A78923125 (en adelante, la parte reclamada o "TME"). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, con fecha 7 de enero de 2023 sobre las 17:00 horas su teléfono móvil de la marca "Movistar" dejó de funcionar, que no le dio más importancia porque lo atribuía a que la tarjeta SIM de su teléfono se habría dañado.

Añade que el día 9 del mismo mes y año se personó en una tienda de la marca "Movistar" para conseguir otra tarjeta SIM y en ese momento recuperó su línea telefónica.

Así las cosas, señala que el día 16 de enero de 2023 comprueba en la aplicación de su banco que entre los días 7 y 9 de enero de 2023 se han realizado seis operaciones bancarias por un tercero.

Posteriormente, el 17 de enero "TME", le informa que el 7 de enero de 2023 se realizó y entregó un duplicado de la tarjeta SIM del reclamante a un tercero.

Y, aporta la siguiente documentación relevante:

Reclamación efectuada a "TME", de fecha 25 de enero de 2023.

Denuncia ante la Comisaria de la Policía Nacional Madrid-Retiro.

Extractos bancarios.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones

Públicas (en adelante, LPACAP), fue recogido en fecha 16 de mayo de 2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 16 de junio de 2023 se recibe en esta Agencia escrito de respuesta indicando:

"Como se evidenciará a través de las alegaciones que se expondrán a lo largo de este escrito, esta parte entiende que la situación que origina la reclamación interpuesta por el reclamante no tiene como origen una inadecuada observancia de las exigencias de la normativa de protección de datos por parte de Telefónica, sino más bien una actuación fraudulenta cometida dolosamente por un tercero con el ánimo de lucrarse ilícitamente a costa del reclamante.

E*n relación a los hechos reclamados, Telefónica informa de que existe una solicitud de cambio de ICC de la tarjeta SIM del Reclamante el día 7 de enero de 2023 a las 17:53 horas a través de uno de nuestros Puntos de Venta.*

El día 9 de enero de 2023, tal como explica el reclamante en su escrito de reclamación, se solicita otro cambio de ICC. Esta solicitud se hace en otro Punto de Venta de Telefónica.

En este sentido, cuando un cliente solicita el duplicado de una tarjeta SIM en una tienda Movistar, el procedimiento a seguir es el denominado "Cambio de tarjeta SIM", que para clientes particulares de la marca comercial Movistar, como es el presente caso, consiste en lo siguiente: En caso de personas físicas la persona habilitada para llevar a cabo la gestión serían el titular de la línea sobre la que se solicita el duplicado, o un representante legal o autorizado por el titular. Para mayor grado de protección, en cuanto a la acreditación de la identidad del cliente, se establece un doble control:

- La identificación del cliente, entendiéndose por identificar la demostración o el reconocimiento de la identidad de la persona tanto verbalmente (cuando el cliente indica su número de DNI) como visualmente (cuando el cliente presenta su documento de identidad, lo que comporta un mayor nivel de seguridad).

- La validación del cliente, que se puede realizar por dos vías (señalando la operativa que en caso de estar disponible el método de validación a través de código QR, ésta será la forma prioritaria de hacerlo):

• Sistema de Verificación de Identidad de Cliente o "SVIC", también conocido como "escáner de documentos de identidad": implica las siguientes acciones:

▪ Verificar que la documentación de identidad aportada por el cliente es auténtica y está en vigor (evitar suplantación de identidad);

▪ Dejar registro de esta verificación en los sistemas (dejar constancia de que el cliente ha estado en la tienda y ha sido identificado con dicha documentación).

• Código QR: Dentro de la App "Mi Movistar", hay un apartado denominado "Identificación en tienda".

Cuando el cliente acuda a la tienda para solicitar el duplicado de tarjeta, el agente comercial le pedirá que acceda a dicho apartado. Para poder acceder, es imprescindible que el usuario conozca el usuario y contraseña asociados a la línea. En ese momento, se generará automáticamente un código QR que el a agente comercial podrá leer con una pistola de lector de código de barras. De esta manera, la información del cliente (ficha del cliente) aparecerá directamente en la pantalla del ordenador del agente que le esté atendiendo.

En caso de representante legal u otra persona autorizada, será necesario aportar la siguiente documentación según la condición que ostenta la persona física que actúa en nombre del titular (autorizado o representante legal): documento identificativo del autorizado o representante legal; autorización o acreditación documental de la condición de representante legal o poder notarial; fotocopia del documento identificativo del titular.

La autorización, que puede venir impresa o ser recibida en la tienda por e-mail, debe contener la siguiente información:
- Nombre completo y NIF del titular de la línea.
- Autorización a la persona que acude al punto de venta (indicando el nombre completo y NIF).
- Mención de la operación que corresponda (de manera concreta, para que no se entienda autorizado a más de lo que se especifique).
- Firma del autorizante (titular).

Por último, la operativa finaliza con la firma del "Contrato cambio de tarjeta SIM", y la entrega de la tarjeta en mano.

En dicho contrato se recoge el detalle del motivo del cambio, el punto de venta en el que se ha gestionado y los datos identificativos del cliente y de la tarjeta".

TERCERO: Con fecha 20 de junio de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (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, teniendo conocimiento de los siguientes extremos:

Para el caso de duplicado de tarjeta SIM del reclamante, los representantes de la entidad alegan que revisados sus sistemas, no consta la documentación almacenada para la solicitud de cambio de ICC de fecha 7 de enero de 2023.

Sí consta registrada la solicitud de fecha 9 de enero de 2023, de la cual se adjuntan copia. Esta solicitud es la que manifiesta haber efectuado el propio reclamante para recuperar su línea.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad TELEFÓNICA MÓVILES ESPAÑA, S.A.U. es una gran empresa constituida en el año 1988, y con un volumen de negocios de 4.406.624.000 euros en el año 2022.

SEXTO: Con fecha 4 de diciembre de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, 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 la presunta infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD.

SÉPTIMO: Notificado el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), la parte reclamada solicitó la concesión de la ampliación del plazo para formular alegaciones y con fecha 3 de enero de 2024 presentó escrito de alegaciones en el que, en síntesis, manifestaba: << *esta parte solicita a la Agencia que suspenda el procedimiento sancionador y requiera al Reclamante a fin de que aporte información acerca del estado en el que se encuentra la denuncia interpuesta, así como el contenido del procedimiento penal que en su caso se encuentre en marcha, pudiendo, llegado el caso, acordar la suspensión de este procedimiento por prejudicialidad penal dada la íntima relación que, como esta parte ya adelanta, es probable que exista entre el procedimiento penal y el administrativo*.

Indicar que, de las contestaciones realizadas por esta parte a los requerimientos de información realizados por la Agencia, en ningún caso se puede inferir que supongan admitir, presuponer o verificar por parte de la Agencia que el agente comercial no siguió la operativa relativa a la identificación del cliente. Es decir, si bien no se ha registrado en los sistemas la copia de la solicitud realizada en la tienda física, no se puede demostrar que el agente no siguió el resto de operativa establecida a tales efectos en todo lo referente a la identificación del cliente. No consta por tanto una prueba de cargo, con entidad suficiente, como para destruir la presunción de inocencia de Telefónica que acredite la ausencia de verificación de la identidad de quien solicitó el duplicado de la tarjeta SIM, ni tampoco para acreditar la ausencia de aplicación de las cautelas previstas, para casos como el que nos ocupa.

Que no exista copia del contrato no es sinónimo de que la identificación no se realizase correctamente.

Debido al volumen de las operaciones de Telefónica y, con la finalidad de garantizar el cumplimiento de sus obligaciones como operadora de telecomunicaciones, así como una correcta prestación de servicios, Telefónica cuenta para la prestación de servicios con varios proveedores de confianza. Tanto en los contratos firmados con los proveedores del canal presencial como los firmados con proveedores del canal telefónico, Telefónica impone una serie de obligaciones que rigen la relación entre Telefónica y éstos, así como la importancia que Telefónica otorga al cumplimiento de las obligaciones establecidas en normativa de protección de datos y, en particular, a la correcta identificación de clientes. Por ello, en cualquier caso, Telefónica no puede ser considerada responsable de los incumplimientos puntuales y excepcionales de la

operativa que se hayan podido llevar a cabo por parte del personal contratado por los encargados del tratamiento que intervienen en este tipo de procesos.
Por lo expuesto, entendemos que no ha lugar la imputación a mi representada de una infracción del artículo 6.1 del RGPD, ya que el tratamiento de esos datos por parte de Telefónica resulta necesario para gestionar la relación contractual con el Reclamante y, por lo tanto, Telefónica contaba con base legitimadora suficiente, no resultando por tanto la acción típica, debiendo procederse al archivo del presente expediente sancionador.
Si el suplantador ha empleado los datos del Reclamante para la solicitud de la tarjeta SIM, esta parte, desconocedora de tal fechoría, gestiona la solicitud del cliente en base a la ejecución del contrato que tiene suscrito con Telefónica.

A este respecto, interesa a esta parte señalar que la consideración de los hechos objeto del procedimiento como ilícitos supone la cualificación de los mismos por el resultado de los actos de engaño, manipulación y uso ilícito de los datos, llevado a cabo por el posible defraudador bancario que haya podido suplantar la identidad del reclamante, no por las acciones de mi representada.

Telefónica tiene establecidas medidas técnicas y organizativas que resultan apropiadas para garantizar una seguridad adecuada de los datos personales de sus clientes, incluida la protección contra el tratamiento no autorizado o ilícito. Asimismo, dichas medidas se revisan y actualizan cuando es necesario a fin de garantizar la seguridad del tratamiento de los datos personales de los clientes y el cumplimiento de las exigencias recogidas en el RGPD.

Todo lo anterior no hace más que evidenciar que la conducta seguida por Telefónica en ningún caso puede ser considerada típica, dado que la conducta realizada por Telefónica no es subsumible en el precepto cuya infracción se imputa.

Pero es que además, tampoco puede ser considerada antijurídica. Telefónica considera que ha actuado en todo momento con buena fe y fundada creencia excluyente de toda culpabilidad. Cabe recordar que la antijuricidad de la conducta, elemento configurador de cualquier ilícito administrativo, exige en su vertiente o aspecto formal que exista una oposición entre el comportamiento y la norma infringida.

En cualquier caso, tampoco concurre el requisito de culpabilidad en la actuación de mi mandante. O, dicho de otro modo, no existe el elemento subjetivo de culpa requerido para la imposición de sanciones administrativas. La actitud de Telefónica revela una inequívoca voluntad de proceder y de actuar conforme a Derecho sin existir en modo alguno intencionalidad de infringir la norma y teniendo en todo caso voluntad de cumplimiento. Por ello, aún en el caso de que la Agencia considere que sí ha existido un tratamiento ilícito de datos por esta parte, considerando que la acción de Telefónica es típica y antijurídica, en ningún caso se puede afirmar que la conducta seguida por Telefónica pueda considerarse culpable.

A este respecto, hay que tener en cuenta que la gestión del duplicado de SIM se habría realizado en todo caso por el resultado de actos de engaño, manipulación y uso ilícito de datos por parte de una tercera persona, quien habría engañado a nuestro comercial haciéndole creer que se trataba de la persona titular de los datos o que

contaba con su consentimiento para efectuar la solicitud al haberse identificado de forma correcta con los datos de cliente que figuran en nuestros sistemas.

Por tanto y en todo caso, la conducta de Telefónica nunca podría ser considerada culpable, al darse en este supuesto un error de tipo invencible. El error de tipo se produce cuando un sujeto comete un delito sin conocer los elementos del tipo objetivo, sea sobre los hechos que lo constituyen o sobre las circunstancias agravantes de la misma o que la cualifican.

En este caso, donde conforme a operativa, el cliente se habría identificado con los datos correctos para la solicitud del duplicado de tarjeta SIM, queda constatado que estaríamos ante un error de tipo invencible, donde se desconocía la antijuricidad de la conducta, debiendo procederse con el archivo del procedimiento, al no poderse determinar la culpabilidad de Telefónica.

Sin perjuicio de las alegaciones precedentes, sobre ausencia de tipicidad, antijuridicidad y culpabilidad, y por si la Agencia no acordase el archivo del presente expediente sancionador, de forma subsidiaria, esta parte quiere manifestar su disconformidad con la cuantía de la sanción propuesta en el Acuerdo, a todas luces desproporcionada si tenemos en cuenta los siguientes aspectos:

-Cuando dispone como circunstancia para agravar la sanción 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.

Pues bien, si nos atenemos al caso concreto y a la responsabilidad de Telefónica, estamos hablando de un caso individual de una solicitud de duplicado de tarjeta SIM en el que el cliente, en todo caso, ha visto afectado su servicio de telecomunicaciones durante dos días.

Por último, también toma en cuenta la Agencia la circunstancia del artículo 83 2.e) RGPD, mencionando de forma expresa los procedimientos sancionadores EXP202207989 y EXP202211479: "Toda infracción anterior cometida por el responsable o el encargado del tratamiento".

En este sentido, y en tanto en cuanto los Tribunales de Justicia están resolviendo sobre ello y no existe un pronunciamiento definitivo sobre los mismos, esta parte considera que no debería de apreciarse esta agravante. De lo contrario y de estimarse el recurso presentado, se causarían enormes perjuicios a esta parte.

Telefónica es completamente congruente con la seguida por la Agencia cuando ante casos similares de SIMSwapping como en los dos expedientes señalados, señala que no existe una vulneración del principio non bis in idem en la imposición de ambas sanciones por separado, con el siguiente argumento en la Resolución sancionadora del Expediente sancionador EXP202211479, dictada en fecha de 13 de junio de 2023 por la Agencia en un caso de SIMSwapping similar al que ahora aquí se discute.

Pues bien, teniendo en cuenta lo anterior, en este caso no debería de apreciarse esta circunstancia agravante al ser cuestionados hechos que, según la Agencia, no serían

similares. En consecuencia, debe ajustarse el importe de la sanción al caso concreto individual.

Por todo lo expuesto, llegado el caso en el que la Agencia decida mantener la sanción, pese a los argumentos esgrimidos por esta parte, estas atenuantes deberán ser tenidas en cuenta para la disminución considerable del importe de esta.

En este sentido, interesa poner de relieve que, la actuación de la Agencia ante un expediente referido a hechos sustancialmente iguales a los que son objeto de reclamación que nos ocupa, ha sido contradictoria, pues así nos lo hizo saber la propia Agencia en el expediente con referencia N.º EXP202104446 de fecha 26 de enero de 2022, en el que se procedió al archivo del mismo al entender que ya había un expediente sancionador en curso por los mismos hechos, cuyo literal fue el siguiente: "Sobre este particular, procede resaltar que hechos similares a los que son objeto de reclamación han sido investigados por esta Agencia y sancionados en el procedimiento sancionador PS/00021/2021, tramitado contra la parte reclamada, por resolución de fecha 8/11/2021, por lo que no procede el inicio de un nuevo procedimiento sancionador".

En consecuencia, la discrepancia de la actuación administrativa entre un expediente y otro supondría la clara vulneración de la doctrina de los actos propios creando una palpable inseguridad jurídica y, por consiguiente, supondría la concurrencia de la causa de anulabilidad del Acuerdo prevista en el artículo 48.1 de la Ley 39/2015 de 1 de octubre, del procedimiento Administrativo Común de las Administraciones Públicas (en adelante, la "Ley 39/2015").

Además, cabe recordar que Telefónica ya ha sido sancionada por los mismos hechos que hoy se desarrollan en este procedimiento, la Agencia impuso la sanción a través del procedimiento con referencia PS/00021/2021, y tal y como conoce la Agencia, actualmente, se ha interpuesto el correspondiente recurso ante los Tribunales de Justicia. Lo anterior nos lleva a considerar que el iniciar un nuevo procedimiento sancionador, de forma sucesiva, sin que haya un pronunciamiento por parte de los Tribunales de Justicia, y sobre los mismos hechos, incumple el principio non bis in idem. Como es sabido, el principio de non bis in idem prohíbe sancionar dos veces un mismo hecho ilícito, pues hacerlo supondría enjuiciar y valorar desde un punto de vista jurídico lo mismo. A juicio de esta parte, esto es lo que pretende la Agencia en el Acuerdo, donde se viene a castigar "lo mismo": el castigo recae sobre el mismo sujeto, por el mismo y para proteger supuestamente el mismo bien jurídico.

Por todo lo expuesto, SOLICITO A LA AGENCIA, que, teniendo por presentando en tiempo y forma, el presente Escrito de Alegaciones, se sirva admitirlo, y previos los trámites oportunos, en su virtud: i. Se declare la inexistencia de responsabilidad por parte de Telefónica por la presunta infracción que se le imputa en este procedimiento, ordenando el archivo del presente expediente sancionador. ii. Subsidiariamente y para el caso de que no se proceda al archivo del presente expediente sancionador, se suspenda el presente procedimiento y se requiera al reclamante a fin de que aporte en qué punto está la denuncia interpuesta, así como el contenido del procedimiento penal que en su caso se encuentre en marcha, con el fin de determinar si existe prejudicialidad penal. iii. Por último, en caso de que no se estimasen ninguna de las

pretensiones anteriores, *que se minore la sanción inicialmente propuesta en virtud de las atenuantes estipuladas en el art. 83 del RGPD>>.*

OCTAVO: Con fecha 15 de enero de 2024, el instructor del procedimiento acordó practicar las siguientes pruebas: <<*1.Se dan por reproducidos a efectos probatorios la reclamación interpuesta por D.* ***A.A.A.*** *y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento AI/00230/2023. 2.Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por* ***TELEFÓNICA MÓVILES ESPAÑA, S.A.U.****, y la documentación que a ellas acompaña>>.*

NOVENO: Con fecha 12 de febrero de 2024 se formuló la propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a la reclamada, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, con una multa de 200.000 euros.

DÉCIMO: Notificada la propuesta de resolución, con fecha 19 de febrero de 2024, la parte reclamada no ha presentado escrito de alegaciones.

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

HECHOS PROBADOS

PRIMERO. Consta que TME con fecha 7 de enero de 2023 realizó y entregó un duplicado de la tarjeta SIM de la parte reclamante a un tercero.

Así, "TME" reconoce en su respuesta de fecha 16 de junio de 2023, al requerimiento de información de esta Agencia: <<*en relación a los hechos reclamados, Telefónica informa de que existe una solicitud de cambio de ICC de la tarjeta SIM del reclamante el día 7 de enero de 2023 a las 17:53 horas a través de uno de nuestros Puntos de Venta>>*.

SEGUNDO. – "TME" reconoce en su respuesta de fecha 29 de agosto de 2023 que no tiene la documentación relativa al cambio de ICC de la tarjeta SIM del reclamante de fecha 7 de enero de 2023.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para

iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

Prejudicialidad Penal

Con carácter previo procede resolver la alegación presentada por "TME", en base a la existencia de una prejudicialidad penal.

Se manifiesta sobre estos hechos que están siendo actualmente objeto de una investigación penal. Considera que, por ello, en aplicación del principio de prejudicialidad penal recogido en el artículo 10 de la Ley Orgánica del Poder Judicial, no debe resolverse el asunto en vía administrativa en tanto en cuanto no se resuelva por la vía penal. Ello, manifiesta, dado que los hechos declarados probados vincularán a la Agencia respecto a un posible procedimiento sancionador, conforme a lo previsto en el artículo 77.4 de la Ley 39/2015, de 1 de octubre.

Debe tenerse en cuenta que el art. 77.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP): *"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".* Sin embargo, hay que indicar, que en el presente caso no existe la triple identidad necesaria para aplicar el artículo 77 de la LPACAP, (de sujeto, hecho y fundamento), entre la infracción administrativa que se valora y la posible infracción o infracciones penales que se pudieran derivar de las presuntas Diligencias Previas practicadas por un órgano jurisdiccional. Esto, porque:

- El sujeto infractor es obvio que no sería el mismo –respecto a las infracciones de la LOPDGDD el responsable es Telefónica, en tanto que el responsable penal de un eventual delito de usurpación de personalidad o estafa sería el tercero que se hubiera hecho pasar por el reclamante.

- Tampoco el fundamento jurídico sería el mismo: mientras el bien jurídico protegido por la LOPDGDD es el derecho fundamental a la protección de datos personales, el bien jurídico que se protege en los tipos penales cuya comisión investigaría, llegado el caso, el Juzgado de Instrucción serían el estado civil, el patrimonio, etc.

En este sentido es muy esclarecedora la Sentencia de la Audiencia Nacional de 27/04/2012 (rec. 78/2010), en cuyo Fundamento Jurídico segundo el Tribunal se pronuncia en los siguiente términos frente al alegato de la recurrente de que la AEPD ha infringido el artículo 7 del R.D. 1398/1993 (norma que estuvo vigente hasta la entrada en vigor de la LPACAP): *"En este sentido el Art. 7 del Real Decreto 1398/1993, de 4 de agosto, del procedimiento para el ejercicio de la potestad*

sancionadora, únicamente prevé la suspensión del procedimiento administrativo cuando se verifique la existencia efectiva y real de un procedimiento penal, si se estima que concurre identidad de sujeto, hecho y fundamento de derecho entre la infracción administrativa y la infracción penal que pudiera corresponder.

No obstante, y para la concurrencia de una prejudicialidad penal, se requiere que ésta condicione directamente la decisión que haya de tomarse o que sea imprescindible para resolver, presupuestos que no concurren en el caso examinado, en el que existe una separación entre los hechos por los que se sanciona en la resolución ahora recurrida y los que la recurrente invoca como posibles ilícitos penales. Así, y aun de haberse iniciado, en el presente supuesto, y por los hechos ahora controvertidos, también actuaciones penales frente a la empresa distribuidora, lo cierto es que tanto la conducta sancionadora como el bien jurídico protegido son distintos en una y otra vía (contencioso-administrativa y penal). En el ámbito penal, el bien jurídico protegido es una posible falsedad documental y estafa, y en el ámbito administrativo, en cambio, la facultad de disposición de sus datos personales por parte de su titular, por lo que tal objeción de la demandada ha de ser rechazada".

En consideración a lo expuesto no puede prosperar la cuestión planteada por la parte reclamada y debe ser rechazada.

III

Respuesta a las alegaciones

En cuanto a la 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), c), e) y f) del RGPD.

Por dicha razón, este es un proceso en donde la diligencia prestada por las operadoras es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que la persona que contrata es quien dice ser y que se implantan y mantienen medidas apropiadas para dar cumplimiento al principio de licitud.

En esta línea, la reciente Sentencia de la Audiencia Nacional de 1 de marzo de 2024 (rec. 1757/2021) señala:

"Así se impone al responsable del tratamiento que verifique la exactitud de los datos del interesado a través de la implementación de las medidas adecuadas cuando se efectúe una contratación. Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento, y a ello obedece la exigencia de documentación identificativa, como viene reiterando la Sala entre otras en Sentencias de 3 de octubre de 2013 (Rec. 5472012), 21 de noviembre 2014 (Rec. 45/2014) etc"

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos

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

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

En cuanto a la conducta de "TME" se considera que responde al título de culpa. 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.

Es el considerando 74 del RGPD el que dice: *Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas*. Asimismo, el considerando 79 dice: *La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.*

La reclamada ha solicitado en su escrito de alegaciones, con carácter subsidiario, que esta Agencia acuerde el archivo del procedimiento por inexistencia de culpabilidad.

Pues bien, la responsabilidad objetiva está proscrita en nuestro ordenamiento jurídico. Rige en el Derecho Administrativo sancionador el principio de culpabilidad (artículo 28 de la Ley 40/2015, de Régimen Jurídico del Sector Público, en adelante LRJSP), por lo que el elemento subjetivo o culpabilístico es una condición indispensable para que surja la responsabilidad sancionadora. El artículo 28 de la LRJSP, "*Responsabilidad*", dice:

> *"1. 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."

A la luz de este precepto la responsabilidad sancionadora puede exigirse a título de dolo o de culpa, siendo suficiente en el último caso la mera inobservancia del deber de cuidado.

A tal efecto se hace necesario traer a colación la Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de diciembre de 2023, recaída en el asunto C-807/21 (Deutsche Wohnen), que indica:

"76 A este respecto, debe precisarse además, por lo que atañe a la cuestión de si una infracción se ha cometido de forma intencionada o negligente y, por ello, puede sancionarse con una multa administrativa con arreglo al artículo 83 del RGPD, que un responsable del tratamiento puede ser sancionado por un comportamiento comprendido en el ámbito de aplicación del RGPD cuando no podía ignorar el carácter infractor de su conducta, tuviera o no conciencia de infringir las disposiciones del RGPD (véanse, por analogía, las sentencias de 18 de junio de 2013, Schenker & Co. y otros, C-681/11, EU:C:2013:404, apartado 37 y jurisprudencia citada; de 25 de marzo de 2021, Lundbeck/Comisión, C-591/16 P, EU:C:2021:243, apartado 156, y de 25 de marzo de 2021, Arrow Group y Arrow Generics/Comisión, C-601/16 P, EU:C:2021:244, apartado 97)." (el subrayado es nuestro).

El Tribunal Constitucional, entre otras, en su STC 76/1999, ha declarado que las sanciones administrativas participan de la misma naturaleza que las penales, al ser una de las manifestaciones del ius puniendi del Estado, y que, como exigencia derivada de los principios de seguridad jurídica y legalidad penal consagrados en los artículos 9.3 y 25.1 de la CE, es imprescindible su existencia para imponerlas.

A propósito de la culpabilidad de la persona jurídica procede citar la STC 246/1991, 19 de diciembre de 1991 (F.J. 2), conforme a la cual, respecto a las personas jurídicas, el elemento subjetivo de la culpa se ha de aplicar necesariamente de forma distinta a como se hace respecto de las personas físicas y añade que "*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 [...]*".

La reclamada ha invocado distintos argumentos para justificar la ausencia de culpabilidad de su conducta.

La decisión de archivar un expediente sancionador podrá fundarse en la ausencia del elemento de la culpabilidad cuando el responsable de la conducta antijurídica hubiera obrado con toda la diligencia que las circunstancias del caso exigen.

En cumplimiento del principio de culpabilidad la AEPD ha acordado en numerosas ocasiones el archivo de procedimientos sancionadores en los que no concurría el

elemento de la culpabilidad del sujeto infractor. Supuestos en los que, pese a existir un comportamiento antijurídico, había quedado acreditado que el responsable había obrado con toda la diligencia que resultaba exigible, por lo que no se apreciaba culpa alguna en su conducta. Ese ha sido el criterio mantenido por la Sala de lo Contencioso Administrativo, sección 1ª, de la Audiencia Nacional. Pueden citarse, por ser muy esclarecedoras, las siguientes sentencias:

- SAN de 26 de abril de 2002 (Rec. 895/2009) que dice:
"En efecto, no cabe afirmar la existencia de culpabilidad desde el resultado y esto es lo que hace la Agencia al sostener que al no haber impedido las medidas de seguridad el resultado existe culpa. Lejos de ello lo que debe hacerse y se echa de menos en la Resolución es analizar la suficiencia de las medidas desde los parámetros de diligencia media exigible en el mercado de tráfico de datos. Pues si se obra con plena diligencia, cumpliendo escrupulosamente los deberes derivados de una actuar diligente, no cabe afirmar ni presumir la existencia de culpa alguna."

- SAN de 29 de abril de 2010, Fundamento Jurídico sexto, que, a propósito de una contratación fraudulenta, indica que "*La cuestión no es dilucidar si la recurrente trató los datos de carácter personal de la denunciante sin su consentimiento, como si empleó o no una diligencia razonable a la hora de tratar de identificar a la persona con la que suscribió el contrato".*

Llegados a este punto, conviene recordar nuevamente lo que la STC 246/1991 ha dicho a propósito de la culpabilidad de la persona jurídica: que no falta en ella la "*capacidad de infringir las normas a las que están sometidos". "Capacidad de infracción [...] que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz [...]".*

En conexión con lo expuesto hay que referirse al artículo 5.2. del RGPD (principio de responsabilidad proactiva), conforme al cual el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1- por lo que aquí interesa, del principio de licitud en relación con el artículo 6.1 del RGPD- y capaz de demostrar su cumplimiento. El principio de proactividad transfiere al responsable del tratamiento la obligación no solo de cumplir con la normativa, sino también la de poder demostrar dicho cumplimiento.

El Dictamen 3/2010, del Grupo de Trabajo del artículo 29 (GT29) -WP 173- emitido durante la vigencia de la derogada Directiva 95/46/CEE, pero cuyas reflexiones son aplicables en la actualidad, afirma que la "*esencia*" de la responsabilidad proactiva es la obligación del responsable del tratamiento de aplicar medidas que, en circunstancias normales, garanticen que en el contexto de las operaciones de tratamiento se cumplen las normas en materia de protección de datos y en tener disponibles documentos que demuestren a los interesados y a las Autoridades de control qué medidas se han adoptado para alcanzar el cumplimiento de las normas en materia de protección de datos.

El artículo 5.2 se desarrolla en el artículo 24 del RGPD que obliga al responsable a adoptar las medidas técnicas y organizativas apropiadas "*para garantizar y poder demostrar"* que el tratamiento es conforme con el RGPD. El precepto establece:

"*Responsabilidad del responsable del tratamiento*"
"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.
3.La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento."

El artículo 25 del RGPD, "*Protección de datos desde el diseño y por defecto*", establece:

"1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2.[...]".

Es plenamente aplicable al caso la SAN de 17 de octubre de 2007 (rec. 63/2006), que, después de referirse a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, dice: *"[...] 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*".

Telefónica cita en su descargo una serie de resoluciones dictadas por la AEPD, manifestando que el EXP20210446 se procedió al archivo del mismo al entender que ya había un expediente sancionador en curso por los mismos hechos y que Telefónica ya ha sido sancionada por los mismos hechos que hoy se desarrollan en este procedimiento, la Agencia impuso la sanción a través del procedimiento con referencia PS/00021/2021y por lo tanto incumple principio *non bis ídem.*

Sobre este particular, procede resaltar que dichos procedimientos tuvieron por objeto analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM

por parte de Telefónica, identificando las vulnerabilidades que puedan existir en los procedimientos operativos implantados, para detectar las causas por las cuales se pueden 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.

En el procedimiento sancionador PS/00021/2021, tramitado contra la parte reclamada se le imputó la violación del artículo 5.1f), 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.

Además, respecto a que esta Agencia archivó otras reclamaciones similares, hay que manifestar que estas se archivaron, pero siempre sin perjuicio de que la Agencia, aplicando los poderes de investigación y correctivos que ostenta, pudiera llevar a cabo posteriores actuaciones relativas al tratamiento de datos tal y como indican las resoluciones invocadas.

Finalmente manifiesta la parte reclamada que la sanción vulnera el principio de proporcionalidad.

Sobre este particular ha de recordarse que el artículo 83.1 del RGPD previene que "Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasoria".

Las multas por tanto, según se deduce del precepto han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD. La cuantía a la que puede ascender la sanción por la infracción del artículo 6.1 del RGPD, de conformidad con el art. 83.5 del RGPD, es de "20.000.000€ como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía". Por ello, independientemente de lo anterior, la multa impuesta a la parte reclamada por la infracción del artículo 6 del RGPD no es desproporcionada, pues incluso si solamente se tuviera en consideración únicamente el volumen de negocios de Telefónica (de acuerdo con el informe recogido de la herramienta AXESOR, su volumen
de negocios es de 4.406.624.000 de euros en el año 2022), la sanción no supera los 20.000.000 de euros ni alcanza el 4% del volumen de negocio total anual del ejercicio financiero anterior, en los términos del art. 83.4 del RGPD.

Por lo expuesto, no se aceptan las alegaciones presentadas al acuerdo de inicio.

IV

Obligación Incumplida

Resulta preciso señalar que el artículo 4.1 del RGPD define: *«datos personales»* como *"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;"

A este respecto, 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.

Por otro lado, 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).

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

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

Pues bien, se imputa a la reclamada la comisión de una infracción por vulneración del artículo 6 del RGPD, "*Licitud del tratamiento*", que señala en su apartado 1 los supuestos en los que el tratamiento de datos de terceros es considerado lícito:

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

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

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

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

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

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

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

En el presente caso, resulta acreditado que "TME" facilitó un duplicado de la tarjeta SIM de la parte reclamante a un tercero, sin su consentimiento y sin verificar la identidad de dicho tercero, el cual, ha accedido a la información contenida en el teléfono móvil. Así pues, la reclamada, no verificó la personalidad del que solicitó el duplicado de la tarjeta SIM, no tomó las cautelas necesarias para que estos hechos no se produjeran.

En base a lo anteriormente expuesto, en el caso analizado, queda en entredicho la diligencia empleada por parte de la reclamada para identificar a la persona que solicitó un duplicado de la tarjeta SIM.

En primer lugar, hay que destacar tal como reconoce "TME" en la respuesta al traslado de la reclamación de fecha 16 de junio de 2023, que "TME" informa que existe una solicitud de cambio de ICC de la tarjeta SIM del reclamante el día 7 de enero de 2023 a las 17:53 horas a través de un Punto de Venta de Telefónica, y señala que la incidencia puesta de manifiesto por la parte reclamante deriva de una actuación fraudulenta cometida dolosamente por un tercero con el ánimo de lucrarse ilícitamente a costa del reclamante.

Y, en segundo lugar, en su respuesta de fecha 29 de agosto de 2023 la parte reclamada reconoce que se produjo el duplicado fraudulento, manifestando que revisados sus sistemas, "*no consta la documentación almacenada para la solicitud de cambio de ICC de fecha 7 de enero de 2023*".

En todo caso, la operadora reconoce que no se siguió el procedimiento implantado por ella misma, ya que, de haberlo hecho, se debió haber producido la denegación del duplicado de la tarjeta SIM.

A la vista de lo anterior, la parte reclamada no logra acreditar que se haya seguido ese procedimiento.

Ahora bien, debe señalarse que el Sim Swapping es un fraude que permite suplantar la identidad mediante el secuestro del número de teléfono al obtener un duplicado de la tarjeta SIM.

Pues bien, el resultado fue que la reclamada expidió la tarjeta SIM a un tercero que no era el titular de la línea, si bien el suplantador conocía las credenciales del reclamante, hubo irregularidades del operador, entregó en un punto de venta la SIM a un tercero, tal como reconoce "TME". Aparte no aportan la documentación de solicitud de cambio de ICC de fecha 7 de enero de 2023.

En base a lo anteriormente expuesto, en el caso analizado, queda en entredicho la diligencia empleada por parte de la reclamada para identificar a la persona que solicitó el duplicado de la tarjeta SIM.

En ese sentido el Considerando 40 del RGPD señala:

"*(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."*

De conformidad con las evidencias de las que se dispone, se estima que la conducta de la parte reclamada vulnera el artículo 6.1 del RGPD siendo constitutiva de la infracción tipificada en el artículo 83.5.a) del citado Reglamento 2016/679.

V

Tipificación y calificación de la infracción

La infracción se tipifica en el artículo 83.5 del RGPD, que considera como tal:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*
a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;".

La LOPGD, a efectos de la prescripción de la infracción, califica en su artículo 72.1 de infracción muy grave, siendo en este caso el plazo de prescripción de tres años, b) *"El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679."*

VI

Sanción

La determinación de la sanción que procede imponer en el presente caso exige observar las previsiones de los artículos 83.1 y 2 del RGPD, preceptos que, respectivamente, disponen lo siguiente:

"1. *Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias."*

"2. *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."

Dentro de este apartado, la LOPDGDD contempla en su artículo 76, titulado "*Sanciones y medidas correctivas*":

"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."

Hay que señalar que la parte reclamada ha obrado con una grave falta de diligencia en el tratamiento efectuado con ocasión del desarrollo de la actividad empresarial que le es propia. A propósito del grado de diligencia que está obligado a desplegar en el cumplimiento de la normativa de protección de datos, cabe citar la SAN de 17/10/2007 (rec. 63/2006), que pese a haberse dictado bajo la vigencia de la anterior normativa resulta plenamente aplicable. Se recoge en ella 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 la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, [...]

Además, conforme al artículo 83.1 del RGPD la imposición de las sanciones de multa está presidida por los siguientes principios: deberán estar individualizadas para cada caso particular, ser efectivas, proporcionadas y disuasorias.

La admisión de que opere como una atenuante que la parte reclamada ha solventado la incidencia objeto de reclamación de forma efectiva, anula en parte la finalidad disuasoria que se cumple a través de la sanción. Aceptar la tesis de "TME" en un supuesto como el que nos ocupa supondría introducir una rebaja artificial en la sanción que verdaderamente procede imponerse; la que resulta de considerar las circunstancias del artículo 83.2 RGPD que sí deben de ser valoradas.

En aras a graduar el importe de la sanción de multa que se propone imponer a "TME" por la infracción del artículo 6.1 del RGPD, estimamos que concurren las circunstancias a las que nos referiremos a continuación, que operan en calidad de agravantes.

Así pues, conforme al apartado e) del artículo 83.2. RGPD, en la determinación del importe de la sanción de multa administrativa no podrán dejar de valorarse todas aquellas infracciones anteriores del responsable o del encargado de tratamiento en aras a calibrar la antijuricidad de la conducta analizada o la culpabilidad del sujeto infractor.

Además, una correcta interpretación de la disposición del artículo 83.2.e) RGPD no puede obviar la finalidad perseguida por la norma: decidir la cuantía de la sanción de multa administrativa en el caso individual planteado atendiendo siempre a que la sanción sea proporcional, efectiva y disuasoria.

Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que la reclamada ha sido sancionada por la infracción del artículo 6.1 del RGPD:

i.EXP 202209359. Resolución dictada el 16 de junio de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.

ii.EXP202211479. Resolución dictada el 13 de junio de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.

- La evidente vinculación entre la actividad empresarial de la reclamada y el tratamiento de datos personales de clientes o de terceros (artículo 83.2.k, del RGPD en relación con el artículo 76.2.b, de la LOPDGDD).

La Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), en la que, respecto 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."*

Procede graduar la sanción a imponer a la reclamada y fijarla en la cuantía de 200.000 € por la por la presunta infracción del artículo 6.1) tipificada en el artículo 83.5.a) del citado RGPD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a TELEFÓNICA MÓVILES ESPAÑA, S.A.U., con NIF A78923125, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de 200.000 euros (doscientos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a TELEFÓNICA MÓVILES ESPAÑA, S.A.U.

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la LPACAP, en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 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 ***IBAN: ES00 0000 0000 0000 0000 0000 (BIC/Código SWIFT: XXXXXXXXXXX)***, abierta a nombre de la Agencia Española de Protección de Datos 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 art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 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 Agencia Española de Protección de Datos, 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 art. 16.4 de la citada Ley 39/2015, de 1 de octubre. 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.

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