- **Expediente N.º: EXP202206350**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Dña. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 11 de mayo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra Vodafone España, S.A.U. con NIF A80907397, anteriormente Vodafone Enabler España (LOWI) (en adelante, la parte reclamada o Vodafone). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 28 de febrero de 2022, Vodafone facilitó a un tercero duplicados de sus dos tarjetas SIM, sin haber realizado ninguna comprobación al respecto, quedándose la parte reclamante sin línea en sus dos terminales.

Añade que dicho tercero modificó los datos de acceso a su área de cliente y que, valiéndose de la información contenida en su teléfono móvil, accedió a su cuenta bancaria, realizando operaciones fraudulentas.

Posteriormente, contactó telefónicamente con la parte reclamada solicitando nuevos duplicados de sus dos tarjetas SIM y además el bloqueo de las líneas y, por otro lado, Vodafone le confirmó que la dirección de su correo electrónico de contacto fue modificada.

Señala que presentó reclamación ante la entidad reclamada sin obtener respuesta.

Documentación relevante aportada por la parte reclamante:

- Correo electrónico de fecha 7 de marzo de 2022 remitido por la reclamante desde la dirección ******USUARIO.1@gmail.com*** *a la dirección* ***(...)@lowi.es*** de la entidad reclamada informando de la activación de dos duplicados fraudulentos de las tarjetas asociadas a los números ******TARJETA.1*** *y* ******TARJETA.2*** y seguidamente se sustrajo dinero de su cuenta bancaria**.** En este correo también informa de que telefónicamente ha solicitado el envío de nuevos duplicados y el bloqueo de las líneas hasta su recepción. Y pone de manifiesto que le han indicado que se ha modificado la dirección de correo electrónico.

- Denuncia interpuesta ante la Policía Nacional de fecha 1 de marzo de 2022 sobre los hechos mencionados*.*

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 28 de junio de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 2 de agosto de 2022 se recibe en esta Agencia escrito de respuesta indicando que: *<<Tras realizar las investigaciones oportunas sobre lo ocurrido y habiendo confirmado mi representada que se han realizado todas las actuaciones pertinentes con anterioridad a la notificación de la presente solicitud de información, se ha procedido a enviar una carta a la reclamante mediante la que se le informa sobre las gestiones que fueron llevadas a cabo por LOWI para solucionar la incidencia y de que lo sucedido ha sido calificado como un fraude por el Departamento de Fraude de LOWI.*

Además, se informa de que la reclamante recuperó el control total sobre las líneas ******TARJETA.1*** *y* ******TARJETA.2*** *afectadas el día 1 de marzo al tramitarse y enviarse las nuevas tarjetas SIM a la reclamante.*

La reclamación tiene su origen en que la reclamante, usuaria de las líneas de telefonía móvil ******TARJETA.1*** *y* ******TARJETA.2*** *contratadas con mi mandante LOWI, alega en su reclamación haber sido víctima de acciones maliciosas por parte de un tercero desconocido mediante las se habría solicitado un duplicado de su tarjeta SIM sin su consentimiento y, tras serle concedido, se habrían realizado operaciones no consentidas a través de su cuenta bancaria.*

Tras analizar la reclamación e investigar lo sucedido, LOWI ha podido comprobar que, el 14 de febrero y el 28 de febrero de 2022, un tercero solicitó, vía telefónica, duplicados de las tarjetas SIM de las líneas ******TARJETA.2*** *y* ******TARJETA.1****, respectivamente, asociadas al ID de cliente de la reclamante. Para ello, la persona que contactó con el servicio de atención al cliente de LOWI aportó los datos necesarios para superar la Política de Seguridad de LOWI.*

Posteriormente, la reclamante indicó haber sufrido una suplantación de identidad y denunció los duplicados SIM, al haber perdido acceso a la red LOWI. Por tal motivo, el propio día 1 de marzo, el servicio de atención al cliente de LOWI procedió a suspender las líneas afectadas, calificar lo sucedido como un fraude y devolver el control sobre su línea a la reclamante, tramitando dos nuevos duplicados SIM y enviando los mismos a la reclamante.

Quiere esta parte señalar que la efectiva gestión de un cambio de tarjeta SIM, ya sea solicitado en tienda física o por vía telefónica, conlleva la superación de las políticas de seguridad que LOWI tiene implementadas a fin de prevenir que se realicen prácticas fraudulentas sobre los datos personales de sus clientes.

En este sentido, y al haberse tramitado dicha gestión sujeta a dicha política de seguridad, mi representada entendió en todo momento que se trataban de gestiones lícitas, reales y veraces.
Sin embargo, en vista de los hechos acontecidos, cuando la reclamante trasladó la pérdida de red, mi representada procedió a realizar las investigaciones y gestiones oportunas a fin de resolver la incidencia acontecida y efectuar los nuevos cambios de SIM que devolvieran el control a la reclamante sobre las líneas.

Así, tras verificar LOWI que estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento, mi representada procedió al bloqueó de las tarjetas SIM de la reclamante para evitar futuros ataques, se devolvió a la reclamante el control sobre sus tarjetas SIM y se tramitaron dos nuevos duplicados SIM.

En paralelo, el Departamento de Fraude procedió a calificar lo sucedido como un fraude y, consecuentemente, aplicó las medidas de seguridad correspondiente en estos casos.

Una vez recibida la presente reclamación, LOWI verificó que lo sucedido se había calificado como un fraude y que las líneas afectadas se encontraban bajo la titularidad de la reclamante.

Asimismo, mi mandante incluyó los datos personales de la reclamante en los ficheros de prevención de fraude de LOWI para evitar que se pueda volver a producir una situación similar en el futuro.

Todo ello se ha notificado a la reclamante mediante en el envío de una carta que se adjunta como Documento número 1.

Por otro lado, a fin de evitar que se produzcan incidencias similares, LOWI trabaja de forma continua en mejorar las Políticas de Seguridad para sus procesos de cambio y duplicados de SIM, así como para cualquier otro proceso que conlleve posibles riesgos de fraudes o actuaciones irregulares para nuestros clientes.

En este sentido, LOWI actúa bajo la Política de Seguridad para la Contratación de Particulares, la cual se ha ido actualizando progresivamente. Mediante dicha Política de Seguridad, mi representada establece qué tipo de información debe requerir al cliente para cada gestión solicitada.

Asimismo, queda incluido cómo proceder en caso de que un usuario no pase la Política de Seguridad, así como las actuaciones preventivas en situaciones de fraude.

La mencionada Política de Seguridad es de obligado cumplimiento para todos los empleados de LOWI, quienes se encargan de aplicarla y respetarla.

Asimismo, en lo que se refiere a la realización de transacciones bancarias de carácter fraudulento como las que pone de manifiesto la reclamante en su reclamación, resulta oportuno expresar que el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta, y no a los datos bancarios del titular.

Por tanto, no parece posible que exista una correlación entre los hechos ocurridos en relación con mi representada y lo ocurrido con la entidad bancaria de la que es cliente la reclamante.

En este sentido, los movimientos bancarios que alega en su reclamación no tienen su origen, ni han sido ocasionados en concepto de facturas por servicios de LOWI que tuviese contratados, sino que se deben a accesos efectuados a través de la cuenta de su entidad bancaria.

Por ello, LOWI no puede ser responsable de los accesos y movimientos bancarios que pudiesen haberse realizado de forma fraudulenta. Con todo ello, podemos confirmar que actualmente mi representada ha realizado todas las actuaciones pertinentes para dar solución a la reclamación, estimando que ha quedado correctamente solventada con anterioridad a la recepción del presente escrito>>.

TERCERO: De conformidad con el artículo 65 de la LOPDGDD, cuando se presentase ante la Agencia Española de Protección de Datos (en adelante, AEPD) una reclamación, ésta deberá evaluar su admisibilidad a trámite, debiendo notificar a la parte reclamante la decisión sobre la admisión o inadmisión a trámite, en el plazo de tres meses desde que la reclamación tuvo entrada en esta Agencia. Si, transcurrido este plazo, no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en el Título VIII de la Ley. Dicha disposición también resulta de aplicación a los procedimientos que la AEPD hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

En este caso, teniendo en cuenta lo anteriormente expuesto y que la reclamación se presentó en esta Agencia, en fecha 11 de mayo de 2022, se comunica que su reclamación ha sido admitida a trámite el 11 de agosto de 2022 al haber transcurrido tres meses desde que la misma tuvo entrada en la AEPD.

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:

Respecto de la reclamación

La parte reclamada manifiesta que ha procedido a la investigación de los hechos puestos de manifiesto en la reclamación ante la Agencia y ha comprobado que la solicitud se inició a consecuencia de una petición telefónica efectuada por un establecimiento distribuidor autorizado. Y declara que no se puede aportar documentación en relación con la superación de la política de Seguridad ya que el distribuidor no ha podido localizarlas.

La entidad ha aportado informes con las modificaciones efectuadas en los sistemas informáticos respecto de la reclamante y los contactos mantenidos con ella.

En dichos informes figura:

- Con fecha 28/02/2022 consta un cambio de mail a ******USUARIO.2@OUTLOOK.ES*** solicitado mediante llamada a Atención al Cliente.

  A este respecto, el mail aportado por la denunciante a la Policía Nacional es ******USUARIO.1@GMAIL.COM.*** Esta misma dirección fue la utilizada por la reclamante en sus comunicados con la entidad en fechas 02/03/2022 y 07/03/2022 y proporcionado a la Agencia en su reclamación.

- Esa misma fecha solicitud de duplicado de SIM para las líneas ******TARJETA.2*** y ******TARJETA.1*.**

- En esa misma fecha consta una llamada de tienda indicando que "*realice un duplicado"*. El operador indica que no está en la lista de autorizados y le proporcionan dos números de DNI para gestionar otro usuario. Al ser estos DNI distintos al del titular le indican que no puede realizar la gestión y se comunica a Coordinación.

- El 01/03/2022 desde Atención al Cliente se solicita modificación de correo electrónico y duplicados de SIM para los números ******TARJETA.1, ***TARJETA.2***. Se realiza la gestión (DNI correcto ******NIF.1***) y se envían nuevos duplicados SIM.

  Figura como gestionada la solicitud, modificada la dirección de correo y constan dos órdenes de entrega asociadas a la denunciante al domicilio.

- El día 03/03/2022 consta reclamación donde se indica que un tercero de manera fraudulenta ha contratado un duplicado de SIM y han hecho cargos en su cuenta bancaria de ******CANTIDAD.1*** €.

- El día 07/03/2022 desde Atención al Cliente se incluye palabra de seguridad a petición del cliente.

- El día 11/05/2022 consta una notación en Atención Cliente sobre la reclamación presentada en relación con el duplicado de SIM de los números ******TARJETA.1, ***TARJETA.2.*** El cliente solicita un certificado que indique que se facilitó duplicado de las SIM sin su consentimiento e información sobre las tarjetas SIM fraudulentas (domicilio donde se remitieron, procedimiento de solicitud de modificación de las SIM, dirección de correo electrónico, fechas, …) Aporta denuncia ante la Policía junto con los correos electrónicos remitido desde la dirección ******USUARIO.1@gmail.com*** en fecha 02/03/2022 y 07/03/2022 a ***(...)@lowi.es.***

- El 01/06/2022 se aceptan las portabilidades de cuatro líneas, entre ellas las líneas ******TARJETA.2*** y ******TARJETA.1*,** y el 02/06/2022 solicita baja en la fibra por problemas con la compañía por suplantación de identidad.

- El día 8/06/2022 consta que el cliente reclama fraude y se confirma que la SIM fue enviada a la misma dirección del cliente. La entidad ha aportado una impresión de pantalla donde consta la entrega de las tarjetas SIM de fecha 2 de marzo.

A este respecto, la entidad manifiesta que, una vez recibida la reclamación, se procedió a realizar las investigaciones y gestiones oportunas a fin de resolver la incidencia acontecida y efectuar los nuevos cambios de SIM que devolvieran el control a la reclamante sobre las líneas.

Asimismo, se verificó que las gestiones, pese a tener la apariencia de veraces, eran de carácter fraudulento, procediéndose al bloqueo de las tarjetas SIM para evitar futuros

ataques, y se tramitaron dos nuevos duplicados SIM. En paralelo, el Departamento de Fraude procedió a calificar lo sucedido como un fraude.

Aportan carta remitida a la reclamante, de fecha 1 de agosto de 2022, en contestación a la reclamación donde se expone que se calificó como fraude, desactivando las tarjetas SIM fraudulentas y tramitando dos nuevos duplicados SIM. Asimismo, le informan que se han incluido sus datos personales en los ficheros de prevención de fraude de la entidad. Por último, le exponen que el cambio de una tarjeta SIM implica únicamente el acceso a la línea de teléfono asociada a ésta y no a los datos bancarios del titular.

Respecto de la Política de Seguridad

- La entidad dispone de una Política de Seguridad para la Contratación de Particulares en la que se establece qué tipo de información debe requerir al cliente para cada gestión solicitada, los procesos en caso de que el usuario no la pase y las actuaciones preventivas en situaciones de fraude. Es de obligado cumplimiento para todos los empleados.
- En la fecha de la reclamación, la identificación del titular de la línea telefónicamente se realizaba aportando: ***(…)*** en que tiene domiciliada sus facturas.

  El acceso al área privada de cliente es por código de usuario asignado al titular de la línea y contraseña.

  En el canal presencial, el cliente se debe personar en un distribuidor autorizado y acreditar su identidad exhibiendo su DNI, que será fotocopiado y conservado por el distribuidor.
- Ante cualquier indicio de sospecha de fraude se bloquea la línea y se solicita un nuevo duplicado que se remite al titular del servicio y una vez recibido por el cliente de forma automática dejan de estar operativos los SIM anteriores.

  Además, se notifica al departamento legal para su evaluación.

Mejoras de la Política de Seguridad

- La entidad manifiesta que, para reducir el riesgo de cualquier actuación fraudulenta, revisa y mejora continuamente su Política de Seguridad y las actuaciones de sus agentes y distribuidores autorizados:
  - ***(…)***
  - ***(…)***
    - ***(…)***
    - ***(…)***
    - ***(…)***

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

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad VODAFONE ESPAÑA, S.A.U. es una gran empresa constituida en el año 1994, y con un volumen de negocios de 2.928.817.000 euros en el año 2022.

SEXTO: Con fecha 13 de julio 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 LPACAP, la parte reclamada solicitó ampliación del plazo y copia del expediente que le fue concedido y presentó escrito de alegaciones las cuales reiteran básicamente las ya realizadas en el escrito de respuesta y en síntesis manifiesta*:<<Vodafone no ha infringido el artículo 6.1 del RGPD y ha aplicado las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y el tratamiento lícito de datos personales y no existe culpa en las infracciones imputadas y, en consecuencia, no puede imponerse sanción alguna.*

Señala, que la adopción de medidas técnicas y organizativas no es una obligación absoluta. Vodafone ha cumplido con el principio de licitud del tratamiento y con la obligación de adoptar medidas técnicas y organizativas adecuadas para garantizar el mismo. Así pues, el responsable del tratamiento está sujeto a una obligación de medios, no a una obligación de resultados en el sentido de entender que todo incidente es un incumplimiento del deber de garantizar un nivel de seguridad adecuado al riesgo.

Por tanto, del hecho de que un tercero, mediante la comisión de delitos, haya superado las medidas de seguridad de Vodafone no puede automáticamente inferirse que Vodafone no ha sido diligente en la verificación de la identidad de los clientes y, por tanto, no ha tratado los datos personales de la reclamante conforme al artículo 6.1 del RGPD.

Vodafone es responsable de adoptar medidas técnicas y organizativas dirigidas a que los duplicados de tarjetas SIM sean facilitados a los titulares de las líneas telefónicas.

Antes de analizar las concretas medidas adoptadas por Vodafone, es preciso poner de manifiesto que las medidas técnicas y organizativas implementadas por Vodafone están dirigidas única y exclusivamente a garantizar que el solicitante del duplicado de la tarjeta SIM es el titular de la línea telefónica contratada.

A Vodafone podrán achacársele infracciones sólo respecto de aquellos tratamientos de datos y medidas de seguridad de las que sea responsable, esto es, aquellas dirigidas a garantizar que el solicitante del duplicado de la tarjeta SIM es el titular de la línea; no están (ni pueden estar) dirigidas a evitar la suplantación de identidad (falsificación del DNI, por ejemplo) ni a evitar el acceso a las cuentas bancarias a través de la aplicación de la entidad de crédito en cuestión.

No estamos ante un fallo o error del sistema implementado por Vodafone, o ante una infracción consecuencia de un comportamiento de un tercero realizado en el marco normal de las relaciones jurídicas, sino ante un acceso ilícito que se produce como consecuencia de que un tercero (en muchas ocasiones en el seno de una organización criminal), actuando de forma dolosa, lleva a cabo actividades tendentes a superar el sistema de seguridad de mi mandante mediante la suplantación de la identidad del afectado.

Vodafone va modificando su política de seguridad para tratar de anticiparse a nuevos métodos criminales, dichas organizaciones van evolucionando e implementando nuevas formas de actuación con el fin de superar la seguridad de las operadoras, lo que hace que sea imposible una anticipación a la actividad criminal en todos los casos.

En el presente caso, el defraudador se hizo pasar por un establecimiento autorizado de Vodafone aportando sus credenciales y toda la información relativa a la reclamante para superar la política de seguridad de Lowi y conseguir los duplicados SIM.

Vodafone actuó en todo momento conforme a sus políticas de seguridad y realizó una correcta verificación del establecimiento autorizado, así como de los datos del cliente sobre el cual se solicitó la operación, por lo que, sí se llevó a cabo la verificación de la identidad correctamente no siendo posible constatar en el momento de la solicitud de los duplicados SIM que dicha información estuviese siendo utilizada de manera fraudulenta.

En efecto, Vodafone no ha probado la identidad del estafador y ciberdelincuente porque precisamente este sujeto ha ocultado su verdadera identidad y se ha hecho pasar por el cliente de Vodafone, superando mediante técnicas ilícitas las políticas de seguridad establecidas por mi mandante.

Así pues, no creemos que sea reprochable el hecho de que Vodafone no haya podido identificar a los criminales, tratándose esta una tarea más propia de las Fuerzas y Cuerpos de Seguridad del Estado, con los que Vodafone sí colabora.

Así, Vodafone ha realizado el cambio de tarjeta SIM porque el solicitante ha acreditado (de forma fraudulenta) que era agente de un establecimiento autorizado mediante la aportación de las credenciales correctas y los datos del titular de las líneas telefónicas mediante la aportación de todos los datos personales necesarios para superar la política de seguridad, habiendo obtenido los datos personales de las víctimas a través de técnicas de ingeniería social. Pretender que Vodafone pruebe la identidad de los solicitantes supone una suerte de prueba diabólica que no se puede exigir a Vodafone.

Subsidiariamente, y para el caso de que la Agencia entendiera que Vodafone ha infringido el artículo 6.1 del RGPD, no puede apreciarse la existencia de culpabilidad en las infracciones imputadas a Vodafone y, en consecuencia, no puede imponerse a la misma sanción alguna.

Asimismo, la Audiencia Nacional ha entendido, en casos similares al presente, en los que un tercero ha accedido, mediante actividades delictivas, a datos de los interesados custodiados por un responsable del tratamiento, que imputar tales hechos

al responsable del tratamiento podría conllevar la vulneración del principio de culpabilidad.

Estamos ante prácticas delictivas (que van evolucionando con el transcurso del tiempo) llevadas a cabo por estafadores y ciberdelincuentes (en muchos casos actuando a través de organizaciones criminales y bandas organizadas, como alguna de las desmanteladas a raíz de la colaboración de Vodafone con las Fuerzas y Cuerpos de Seguridad del Estado) quienes, actuando con dolo, utilizan la intervención humana ineludible en el sistema de Vodafone para aprovecharse de que una persona en concreto (el empleado u operador que tramita el cambio de SIM) pueda, de buena voluntad y sujeta al abuso del delincuente, relajar los protocolos establecidos. Se trata de delincuentes que, valiéndose de artimañas y actividades delictivas comenzadas en un momento temporal anterior a la solicitud de cambio de SIM (y, por tanto, en un estadio en el que ni Vodafone – ni ningún otro operador – puede hacer nada al respecto) roban datos de entidades, falsifican DNI, denuncias de robo de dichos DNI y consiguen los datos personales de la futura víctima a fin de superar los protocolos de seguridad establecidos por Vodafone. Suplantada la identidad y, en su caso, superadas las medidas de seguridad de la operadora de teléfono, estos terceros continúan con sus actividades delictivas tendentes a distraer otras medidas de seguridad, las establecidas por las entidades bancarias de los clientes de Vodafone.

Teniendo en cuenta lo anterior, deberá determinarse si Vodafone ha empleado la diligencia que le era exigible para garantizar la licitud del tratamiento de los datos personales de su cliente y evitar el duplicado de tarjetas SIM por parte de terceros distintos al titular. Esto es precisamente lo que ocurre en el presente supuesto, y es que en ningún caso el duplicado de las tarjetas SIM del cliente de Vodafone puede suponer la consideración de que Vodafone ha obrado culposamente.

Subsidiariamente, para el supuesto de que la Agencia entendiera que sí que ha existido infracción y que asimismo procede la imposición de una sanción a Vodafone, mi mandante considera que la misma deberá modularse a la baja.

La vinculación de la actividad de Vodafone con la realización de tratamientos de datos de carácter personal. Efectivamente, existe una vinculación entre la actividad de Vodafone y el tratamiento de datos personales de sus clientes que realiza para llevar a cabo la correcta prestación de los servicios contratados y atender las solicitudes y peticiones que éstos realicen. La Agencia hace referencia a la existencia de imprudencia cuando un responsable del tratamiento no se comporta con la diligencia exigible debiendo insistirse en el rigor y el exquisito cuidado para ajustarse a las prevenciones legales al respecto. Prueba del especial cuidado y cautela aplicada en el tratamiento de datos personales que lleva a cabo mi representada, son todas las medidas de seguridad implementadas.

Por lo que este factor, no debe ser tenido en cuenta como agravante a la hora de graduar la sanción.

Además de la medida atenuante indicada por la Agencia, entendemos que también deberían tomarse en consideración las siguientes atenuantes: El grado de responsabilidad del responsable del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32 del

RGPD. Vodafone ha implementado medidas técnicas y organizativas adecuadas para el riesgo generado por mi mandante, esto es, tendentes a asegurar que quien solicita el duplicado o cambio de una tarjeta SIM es el titular de la línea.

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 Mi mandante también entiende que su grado de cooperación con la Agencia durante las actuaciones previas de inspección ha sido alto.

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 Vodafone no ha obtenido ningún tipo de beneficio o evitado pérdidas a raíz de la duplicación fraudulenta de tarjetas SIM, sino todo lo contrario. En este sentido, la actividad criminal llevada a cabo por los estafadores y ciberdelincuentes también ha supuesto un perjuicio reputacional para mi mandante y una defraudación de sus políticas de seguridad.

En virtud de todo lo anterior, solicita 1) El sobreseimiento del expediente con el consiguiente archivo de las actuaciones, por no haberse cometido ninguna de las infracciones imputadas. 2) Subsidiariamente, que en caso de imponerse alguna sanción se imponga en cuantía mínima, a la luz de las circunstancias atenuantes indicadas en el presente escrito>>.

OCTAVO: Con fecha 17 de septiembre de 2023, el instructor del procedimiento acordó practicar las siguientes pruebas: *<<1.Se dan por reproducidos a efectos probatorios la reclamación interpuesta por* ***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/00345/2022. 2. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por* Vodafone España, S.A.U., *y la documentación que a ellas acompaña>>.*

NOVENO: Con fecha 11 de octubre de 2023**,** se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a Vodafone España, S.A.U. con NIF A80907397, anteriormente Vodafone Enabler España (LOWI), por la presunta infracción del artículo 6.1) tipificada en el artículo 83.5.a) del citado RGPD. con una multa de 70.000 euros (setenta mil euros).

DÉCIMO: Notificada la propuesta de resolución, la parte reclamada solicitó ampliación del plazo que le fue concedido y presentó escrito de alegaciones en el que, se reitera en las alegaciones previamente presentadas, y en síntesis manifiesta que: *"Vodafone ha actuado de forma diligente en la medida en la que tiene implementados los procesos necesarios para identificar correctamente a sus clientes, siendo la adopción de medidas técnicas y organizativas una obligación que no es absoluta.*

No obstante, si terceros, mediante técnicas ilícitas y fraudulentas, obtienen los datos confidenciales de los clientes y, a través de ellos, les usurpan la identidad y superan las medidas implementadas, eso no significa que la política sea insuficiente, sino que

se han obtenido los datos necesarios, por medios ajenos a mi representada, para superar sus medidas.

Por lo tanto, siempre va a existir un riesgo "residual" en el tratamiento de los datos, el cual prevalece pese a las medidas implementadas por el responsable, tal y como ha indicado esta Agencia en su Guía, de junio de 2021, sobre la "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales": "Por lo tanto, el concepto de "riesgo cero" no existe cuando hablamos de gestión del riesgo, en particular, cuando hablamos de los riesgos que pueden suponer los tratamientos de datos personales.

En consecuencia, lo que se puede solicitar a mi representada es que implemente un proceso de verificación de la identidad que sea acorde y que, en circunstancias normales, garantice un correcto tratamiento de los datos. Estas medidas estaban implementadas por parte de mi representada cuando se ejecutaron los dos duplicados SIM. En concreto, Vodafone realizó los cambios de tarjeta SIM en la medida en la que el solicitante acreditó (de forma fraudulenta) que era agente de un establecimiento autorizado mediante la aportación de las credenciales correctas y los datos de la reclamante, habiendo obtenido los datos personales de la reclamante a través de medios ajenos a mi representada, como, por ejemplo, técnicas de ingeniería social. Así pues, mi representada tomó las cautelas necesarias para que estos hechos no se produjeran. Vodafone no pudo comprobar que la solicitud se estaba realizando por un tercero en la medida en la que la identidad del estafador estaba oculta y se hacía pasar por el cliente de Vodafone, superando mediante técnicas ilícitas las políticas de seguridad establecidas por mi mandante. Así pues, no creemos que sea reprochable el hecho de que Vodafone no haya podido identificar a los criminales, tratándose esta una tarea más propia de las Fuerzas y Cuerpos de Seguridad del Estado, con los que Vodafone sí colabora.

Con todo ello, Vodafone acredita la implementación de un procedimiento robusto a la hora de verificar la identidad de sus clientes, que en circunstancias normales bloquea de manera inmediata cualquier intento fraudulento que pueda tener lugar. Es relevante reiterar que sólo un número limitado de tiendas autorizadas por Lowi pueden realizar duplicados SIM a través de su canal de soporte.

Aun así, y siendo consciente de que no existe un riesgo cero, desde Lowi, como se indicó en las alegaciones presentadas el 8 de agosto de 2023, se encuentra en un proceso constante de actualización y revisión de sus Política de Seguridad, implementando nuevas medidas y controles que traten de reducir al máximo posible el riesgo inherente al tratamiento de datos que realiza. ***(…)***

(…).

(…).

(…).

Como se ha venido defendiendo en múltiples procedimientos ante esta Agencia por parte de mi representada, a través de un duplicado SIM se puede llegar a obtener el servicio que tuviese contratado el titular de dicha tarjeta. Es decir, el solicitante podrá

acceder a la tarifa que se tiene contratada a través de la SIM, pudiendo recibir mensajes y llamadas, así como enviarlos, y tener servicio de internet, en el caso de que estuviese contratado. En consecuencia, si el duplicado SIM se realiza por un delincuente, como es el caso, tenemos que diferenciar dos fases del proceso (i) Previo al duplicado: el defraudador debería tener la información necesaria del cliente de Vodafone para superar las políticas de seguridad. Esta información se habría obtenido de fuentes ajenas a mi representada, habilitando al delincuente a superar las medidas de seguridad implementadas al suplantar la identidad del cliente. (ii) Posterior al duplicado: el defraudador tendría únicamente acceso al servicio contratado por el cliente de Vodafone para dicha SIM, no teniendo acceso, como mera consecuencia del duplicado, a información bancaria, contraseñas, dirección de correo electrónico, etc.

Por tanto, el duplicado fraudulento de la tarjeta SIM no es una actuación necesaria (hay entidades bancarias que no envían SMS con sus claves únicas) ni suficiente (se requiere el acceso a otros datos y claves) para lograr acceder a las cuentas de los sujetos afectados.

A Vodafone podrán achacársele infracciones sólo respecto de aquellos tratamientos de datos y medidas de seguridad de las que sea responsable, esto es, aquellas dirigidas a garantizar que el solicitante del duplicado de la tarjeta SIM es el titular de la línea; no están (ni pueden estar) dirigidas a evitar la suplantación de identidad (falsificación del DNI, por ejemplo) ni a evitar el acceso a las cuentas bancarias a través de la aplicación de la entidad de crédito en cuestión.

No puede apreciarse la existencia de culpabilidad en las infracciones imputadas a Vodafone y, en consecuencia, no puede imponerse a la misma sanción alguna.

Por otro lado, la AEPD entiende que el principio de proactividad transfiere a mi representada la obligación no solo de cumplir con la normativa, sino también la de poder demostrar dicho cumplimiento. Este aspecto ha sido cubierto ampliamente por Vodafone, no solo aportando los procesos que tiene implementados, sino las interacciones en sus sistemas que evidencian que se siguieron los procesos pertinentes.

Por lo tanto, mi representada sí que actuó con la diligencia debida, implementando las medidas técnicas y organizativas necesarias, y ha podido evidenciar la superación de sus políticas. No obstante, la Agencia defiende que existe dolo o culpa de mi representada únicamente observando el resultado de los hechos, la emisión fraudulenta de dos duplicados SIM, sin considerar todas las medidas de seguridad implementadas para evitar el fraude.

Sobre el agravante aplicado por la Agencia a la hora de evaluar la sanción, nos reiteramos en lo dispuesto en las Alegaciones al Acuerdo de Inicio:

La vinculación de la actividad de Vodafone con la realización de tratamientos de datos de carácter personal. *Efectivamente, existe una vinculación entre la actividad de Vodafone y el tratamiento de datos personales de sus clientes que realiza para llevar a cabo la correcta prestación de los servicios contratados y atender las solicitudes y peticiones que éstos realicen.*

La Agencia hace referencia a la existencia de imprudencia cuando un responsable del tratamiento no se comporta con la diligencia exigible debiendo insistirse en el rigor y el exquisito cuidado para ajustarse a las prevenciones legales al respecto. Prueba del especial cuidado y cautela aplicada en el tratamiento de datos personales que lleva a cabo mi representada, son todas las medidas de seguridad implementadas, además de la continua revisión de sus políticas y cumplimiento de las mismas.

Por lo que este factor, no debe ser tenido en cuenta como agravante a la hora de graduar la sanción.

Sobre los atenuantes no aplicados por la Agencia a la hora de evaluar la sanción:

El grado de responsabilidad del responsable del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32 del RGPD

Así pues, no creemos que sea reprochable el hecho de que Vodafone no haya podido identificar a los criminales, tratándose esta una tarea más propia de las Fuerzas y Cuerpos de Seguridad del Estado, con los que Vodafone sí colabora.

Así, Vodafone ha realizado el cambio de tarjeta SIM porque el solicitante ha acreditado (de forma fraudulenta) que era agente de un establecimiento autorizado mediante la aportación de las credenciales correctas y los datos del titular de las líneas telefónicas mediante la aportación de todos los datos personales necesarios para superar la política de seguridad, habiendo obtenido los datos personales de las víctimas a través de técnicas de ingeniería social. Pretender que Vodafone pruebe la identidad de los solicitantes supone una suerte de prueba diabólica que no se puede exigir a Vodafone.

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.

La Agencia, en su Propuesta de Resolución, desestima este atenuante en la medida en la que entiende que el RGPD "se refiere al 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. La respuesta de la reclamada al requerimiento informativo de la Subdirección de Inspección no cumplía esas finalidades, por lo que no es encuadrable en esa circunstancia atenuante".

En este sentido, informar a la Agencia de que Vodafone sí que ha puesto medios para remediar y mitigar los posibles efectos adversos de la practica fraudulenta de los duplicados SIM. Indicar lo contrario sería no tomar en consideración que Lowi, tal y como se ha venido indicando, se encuentra en un proceso constante de actualización y revisión de sus Política de Seguridad, implementando nuevas medidas y controles que traten de reducir al máximo posible el riesgo inherente al tratamiento de datos que realiza, tal y como se ha evidenciado en la manifestación primera de las presentes alegaciones.

Asimismo, en aquellos casos en los que la actividad criminal del estafador o ciberdelincuente ha logrado defraudar el sistema implementado por Vodafone, mi mandante ha reaccionado dirigiendo sus acciones hacia cuatro frentes distintos:

I. Acciones dirigidas hacia el cliente afectado, tales como bloqueo de la tarjeta SIM en cuestión y restricción en la recepción de SMS, contacto con el cliente, abono de las llamadas realizadas por el estafador o ciberdelincuente etcétera.

II. Acciones dirigidas hacia los agentes y empleados que aplican las medidas de seguridad para evitar la suplantación de identidad al solicitar el duplicado de la tarjeta SIM, tales como envío de comunicaciones periódicas con alertas, información sobre el modus operandi de las bandas criminales para detectar con mayor facilidad futuros casos, aplicación de penalizaciones a aquellos agentes que no han seguido las medidas de seguridad establecidas por Vodafone etcétera.

III. Acciones realizadas en colaboración con las Fuerzas y Cuerpos de Seguridad del Estado, como interposición de denuncias y colaboración con la Policía en la lucha contra este tipo de fraude. IV. Acciones dirigidas hacia terceros, como entidades de crédito; por ejemplo, el desarrollo e implementación de la herramienta "Vodafone Identity Hub (VIH)", que permite verificar por dichos terceros si el interesado ha realizado un cambio o duplicado de su tarjeta SIM de forma reciente.

En virtud de todo lo anterior, solicito que tenga por presentado este escrito y todos los documentos que lo acompañan y, en su virtud, tenga por efectuadas las manifestaciones en él contenidas y, tras los trámites oportunos, acuerde: 1) El sobreseimiento del expediente con el consiguiente archivo de las actuaciones, por no haberse cometido ninguna de las infracciones imputadas y no poder apreciarse la existencia de culpabilidad. 2) Subsidiariamente, que en caso de imponerse alguna sanción se imponga en cuantía mínima, a la luz de las circunstancias atenuantes indicadas en el presente escrito".

HECHOS PROBADOS

PRIMERO. - La reclamante formuló reclamación ante esta Agencia en fecha 11 de mayo de 2022, en la que se hace constar que Vodafone facilitó duplicados de sus dos tarjetas SIM, a un tercero sin su consentimiento, el día 28 de febrero de 2022 y valiéndose de la información contenida en su teléfono móvil, procedió en esa misma fecha a realizar diversos movimientos bancarios.

SEGUNDO. - Obra en el expediente, que el mismo día 28 de febrero de 2022 en que se emitieron los duplicados de las dos tarjetas SIM, se produjo el cambio de la dirección del correo electrónico de la reclamante por un tercero, fue solicitado mediante llamada a Atención al Cliente, lo que sirvió para que el suplantador tuviera acceso a sus datos.

TERCERO. - Se constata, que la solicitud de los duplicados de las tarjetas SIM se llevó a cabo a través de una petición telefónica efectuada por un establecimiento distribuidor a Vodafone.

CUARTO. - Obra en el expediente, que el distribuidor no está en la lista de autorizados de Vodafone y que los DNI aportados por el tercero no correspondían con el del titular de las tarjetas SIM.

QUINTO. - La parte reclamada reconoce que no puede aportar documentación en relación con la superación de la política de seguridad ya que el distribuidor no ha podido localizarlas.

SEXTO. - La reclamante contactó con Vodafone el día 1 de marzo de 2022, manifestando que había sufrido una suplantación de identidad y Vodafone procedió a suspender las líneas afectadas, calificar lo sucedido como fraude y devolver el control sobre su línea a la reclamante, y le facilitaron dos nuevos duplicados SIM.

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

Contestación a las alegaciones presentadas

La parte reclamada manifiesta que la emisión de los duplicados de la tarjeta SIM no es suficiente para realizar operaciones bancarias en nombre de los titulares, ciertamente, para completar la estafa, es necesario que un tercero "suplante la identidad" del titular de los datos ante la entidad financiera. Lo que conlleva a priori, un tratamiento al margen del principio de licitud pues un tercero está tratando datos, ya que tiene acceso a ellos, sin base legal alguna, además de la vulneración de otros principios como el de confidencialidad.

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

Idénticas consideraciones merece la actuación de las entidades bancarias que proporcionan servicios de pago, en cuyo ámbito se inicia este tipo de estafas, ya que el tercero tiene acceso a las credenciales del usuario afectado y se hace pasar por este.

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.

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.

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. Estas circunstancias han sido tenidas en cuenta a la hora de fijar la sanción.

En el presente procedimiento sancionador, la sanción se impone debido a que Vodafone facilitó a un tercero duplicados de las dos tarjetas SIM de la parte reclamante haciendo uso de sus datos personales sin su consentimiento, y por este motivo se imputa el artículo 6.1 del RGPD.

En cuanto a la responsabilidad de Vodafone, debe indicarse que, con carácter general Vodafone 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 otra parte, para completar la estafa, es necesario que un tercero “suplante la identidad” del titular de los datos, para la contratación de la línea móvil. Lo que conlleva a priori, un tratamiento al margen del principio de licitud pues un tercero está tratando datos, ya que tiene acceso a ellos, sin base legal alguna, además de la vulneración de otros principios como el de confidencialidad.

Por dicha razón, este es un proceso en donde la diligencia prestada por las operadoras es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que se implantan y mantienen medidas de seguridad apropiadas para proteger eficazmente la confidencialidad, integridad y disponibilidad de todos los datos personales de los cuales son responsables, o de aquellos que tengan por encargo de otro responsable.

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 Vodafone 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.*

Asimismo, solicita con carácter subsidiario que esta Agencia acuerde el archivo del procedimiento por inexistencia de culpabilidad.

Rige en el Derecho Administrativo sancionador el principio de culpabilidad (artículo 28 de la Ley 40/2015, de Régimen Jurídico del Sector Público, 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.

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.[...]".

Cabe preguntarse cuáles son los parámetros de la diligencia debida que Vodafone debía haber observado en relación con la conducta examinada. La respuesta es que la diligencia que debió observar es la que era precisa para cumplir las obligaciones que le impone la disposición Adicional Única de la Ley 25/2007 en relación con los artículos 5.2, 24 y 25 del RGPD, a la luz de la doctrina de la Audiencia Nacional y la jurisprudencia del Tribunal Supremo.

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".

Es plenamente aplicable al caso la SAN de 19 de septiembre de 2023 (rec. 403/2021), dice*:" contrató la póliza de seguro con un tercero sin control ni supervisión suficiente en cuanto no fue capaz de detectar que realmente, la persona que estaba manifestando su voluntad de contratar, no era quien decía ser. De haberse tomado las necesarias precauciones, a fin de asegurar la identidad la persona contratante (para lo que hubiera sido bastante atender a la incorrecta contestación a las preguntas de identificación y verificación del cliente)".*

III

Obligación incumplida

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".

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;"

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."*

En el presente caso, resulta acreditado en primer lugar que el mismo día en que se emitieron los duplicados de sus dos tarjetas SIM, el día 28 de febrero de 20223, se produjo el cambio su dirección del correo electrónico que paso de ******USUARIO.1@gmail.com*** a ******USUARIO.2@outlook.es***, fue solicitado mediante llamada a Atención al Cliente, lo que sirvió para que el suplantador tuviera acceso a sus datos.

En segundo lugar, la solicitud de los duplicados de sus dos tarjetas SIM para las líneas ******TARJETA.2*** y ******TARJETA.1,*** se hizo a través de una llamada de la tienda indicando que "*realice un duplicado*". Vodafone indica que no está en la lista de autorizados y le proporcionan dos números de DNI para gestionar otro usuario. Al ser estos DNI distintos al del titular le indican que no puede realizar la gestión. No obstante, la anotación en los sistemas de que el distribuidor no está en la lista de autorizados y que los dos DNI aportados no correspondían al titular se realizaron los duplicados.

Así las cosas, en este caso la reclamada declara que no se puede aportar documentación en relación con la superación de la política de Seguridad ya que el distribuidor no ha podido localizarlas.

Vodafone reconoce que una vez investigado los hechos ha comprobado que la solicitud se inició a consecuencia de una petición telefónica efectuado por un establecimiento distribuidor autorizado y que las gestiones eran de carácter fraudulento.

Por otra parte, en relación con la política de seguridad, en el momento de la reclamación, la identificación del titular: ***(…)***. Y en caso de distribuidores autorizados el DNI y hacer fotocopia para su custodia. El cambio de SIM hay que validar el origen del ICC.

En marzo de 2022, después de la incidencia reclamada, se establece que no se realizan cambios de SIM si el número solicitante se encuentra en el extranjero o no está identificado. En octubre de 2022 se crea una nueva versión de la política de seguridad, tanto para los cambios de SIM como para las modificaciones de datos de los clientes.

De esta forma, la parte reclamada facilitó duplicados de las tarjetas SIM de las líneas

***TARJETA.2** y *****TARJETA.1** del reclamante, sin su consentimiento y sin verificar la identidad de dicho tercero, el cual, ha accedido a información contenida en el teléfono móvil, tales como datos bancarios, contraseñas, dirección de correo electrónico y otros datos personales asociados al terminal. 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 los duplicados de la tarjeta SIM.

En este sentido, según ha manifestado la parte reclamada, en su escrito de contestación al requerimiento de esta Agencia de fecha 2 de agosto de 2022 *"Tras analizar la reclamación e investigar lo sucedido, LOWI ha podido comprobar que, el 14 de febrero y el 28 de febrero de 2022, un tercero solicitó, vía telefónica, duplicados de las tarjetas SIM de las líneas *****TARJETA.2** y *****TARJETA.1**, respectivamente, asociadas al ID de cliente de la reclamante. Para ello, la persona que contactó con el servicio de atención al cliente de LOWI aportó los datos necesarios para superar la Política de Seguridad de LOWI.*

Posteriormente, la reclamante indicó haber sufrido una suplantación de identidad y denunció los duplicados SIM, al haber perdido acceso a la red LOWI. Por tal motivo, el propio día 1 de marzo, el servicio de atención al cliente de LOWI procedió a suspender las líneas afectadas, calificar lo sucedido como un fraude y devolver el control sobre su línea a la reclamante, tramitando dos nuevos duplicados SIM y enviando los mismos a la reclamante.

Así, tras verificar LOWI que estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento, mi representada procedió al bloqueó de las tarjetas SIM de la reclamante para evitar futuros ataques, se devolvió a la reclamante el control sobre sus tarjetas SIM y se tramitaron dos nuevos duplicados SIM.

En paralelo, el Departamento de Fraude procedió a calificar lo sucedido como un fraude y, consecuentemente, aplicó las medidas de seguridad correspondiente en estos casos.

Una vez recibida la presente reclamación, LOWI verificó que lo sucedido se había calificado como un fraude y que las líneas afectadas se encontraban bajo la titularidad de la reclamante.

Asimismo, mi mandante incluyó los datos personales de la reclamante en los ficheros de prevención de fraude de LOWI para evitar que se pueda volver a producir una situación similar en el futuro>>.

A este respecto, y esto es lo esencial, la reclamada no acredita la legitimación para el tratamiento de los datos de la reclamante.

El respeto al principio de licitud que está en la esencia del derecho fundamental de protección de datos de carácter personal exige que conste acreditado que la responsable del tratamiento desplegó la diligencia imprescindible para acreditar ese extremo. De no actuar así -y de no exigirlo así esta Agencia, a quien le incumbe velar

por el cumplimiento de la normativa reguladora del derecho de protección de datos de carácter personal- el resultado sería vaciar de contenido el principio de licitud.

En el presente caso, resulta acreditado que Vodafone trató indebidamente los datos de la parte reclamante, dado que facilitó a un tercero duplicados de sus dos tarjetas SIM, sin legitimación para ello, aunque el suplantador tenía los datos de la reclamante, por parte de la reclamada no siguió los protocolos de verificación implementados a la hora de solicitar un duplicado de la tarjeta SIM.

Hay que resaltar, que Vodafone, no verificó la personalidad del que solicitó duplicados de las dos tarjetas SIM de la reclamante, 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 Vodafone para identificar a la persona que solicitó el duplicado de la tarjeta SIM.

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.

IV

Tipificación y calificación de la infracción

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

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

La LOPDGD, 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 establecidos en el artículo 6 del Reglamento (UE) 2016/679"*.

V

Sanción de multa: Determinación del importe

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.”

Vodafone solicita que se aprecien las siguientes circunstancias atenuantes:

El grado de responsabilidad del responsable del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32 del RGPD.

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.

No se admite ninguna de las circunstancias invocadas.

El Artículo 83.2.d) RGPD: “*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;”.*

La reclamada se ha limitado a declarar que el tercero que contrató con ella superó la política de seguridad de la compañía sin aportar ninguna prueba que demuestre que recabó de la persona que intervino en la contratación algún documento que acreditara que era efectivamente el titular de los datos que había facilitado como propios o que articuló algún mecanismo que permitiera contrastar la veracidad de los datos de identidad proporcionados.

Por otra parte, el principio de proactividad supone transferir al responsable del tratamiento la obligación no solo de cumplir con la normativa, también la de poder demostrar su cumplimiento. Entre los mecanismos que el RGPD contempla para

lograrlo se encuentran los previstos en el artículo 25, "*protección de datos desde el diseño*", a tenor del cual el responsable debe aplicar *"tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento*" medidas técnicas y organizativas que garanticen que hace una efectiva aplicación de los principios del RGPD con ocasión de los tratamientos que realiza.

El artículo 83.2.f) del RGPD se refiere al *"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;".* La respuesta de la reclamada al requerimiento informativo de la Subdirección de Inspección no cumplía esas finalidades, por lo que no es encuadrable en esa circunstancia atenuante.

La consideración de la cooperación con la Agencia como atenuante, tal y como pretende la reclamada, no está ligada a ninguno de los supuestos en los que pueda existir una colaboración o cooperación o requerimiento por mor de un mandato legal, cuando las actuaciones son debidas y obligadas por la Ley, como en el caso que nos ocupa.

A tal efecto hay que tener en consideración las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, las cuales señalan que *"deben considerarse que el deber ordinario de cooperación es obligatorio y, por tanto, debe considerarse neutro (y no un factor atenuante)."*

Así queda confirmado en las mismas Directrices del CEPD sobre la aplicación y la fijación de las multas administrativas a efectos del Reglamento 2016/679, adoptadas el 3 de octubre de 2017, en las que se asevera que *"Dicho esto, no sería apropiado tener en cuenta por añadidura la cooperación que la ley exige; por ejemplo, en todo caso se exige a la entidad permitir a la autoridad de control acceso a las instalaciones para realizar auditorías o inspecciones".*

Por ello podemos concluir que no puede entenderse como *"cooperación"* aquello que es exigido o de obligado cumplimiento por mor de la Ley para el responsable del tratamiento, como sucedió en este caso.

En aras a graduar el importe de la sanción de multa que se impone a Vodafone por la infracción del artículo 6.1 del RGPD, estimamos que concurre la circunstancia a la que nos referiremos a continuación, que opera en calidad de agravante.

- 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."

En calidad de atenuantes:

Procedió la parte reclamada a solventar la incidencia objeto de reclamación de forma efectiva (art. 83.2 c).

Procede graduar la sanción a imponer a la reclamada y fijarla en la cuantía de 70.000 € por la infracción del artículo 6.1) tipificada en el artículo 83.5 a) del RGPD.

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

PRIMERO: IMPONER a VODAFONE ESPAÑA, S.A.U. con NIF A80907397, anteriormente VODAFONE ENABLER ESPAÑA (LOWI), por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de por un importe de 70.000 euros (setenta mil euros).

SEGUNDO: NOTIFICAR la presente resolución a VODAFONE ESPAÑA, S.A.U. con NIF A80907397, anteriormente VODAFONE ENABLER ESPAÑA (LOWI)

TERCERO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte 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 ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante 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: CAIXESBBXXX)***, 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