- **Expediente N.º: EXP202212696**

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 10 de octubre 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 (en adelante, la parte reclamada o Vodafone). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que Vodafone facilitó a terceras personas duplicados de sus tarjetas SIM de dos líneas de telefonía móvil, y que estos hechos se llevaron a cabo los días 19 y 20 de abril y 3 de junio del año 2022, a través de solicitudes realizadas telefónicamente, llegando incluso a realizar cambio de titularidad de ambas líneas telefónicas.

Añade que, tras la realización de los citados duplicados, dichos terceros se valieron de la información contenida en su teléfono móvil para acceder a sus datos bancarios, efectuando numerosas transferencias fraudulentas desde su cuenta, con el consiguiente perjuicio económico.

Señala que pese a haber puesto los hechos en conocimiento de la parte reclamada, indicando que no se realizasen duplicados de su tarjeta SIM de forma telefónica, sino tan solo de forma presencial, Vodafone no adoptó ninguna medida al respecto, llevándose a cabo con posterioridad, más copias ilícitas.

Y, aporta la siguiente documentación relevante:

Denuncias presentadas ante la Policía Nacional, los días 20 de abril, 7 y 16 de junio del año 2022.

Comunicaciones enviadas a través del correo electrónico por su abogado a la parte reclamada y las respuestas recibidas, desde el día 14 junio hasta el día 28 del mismo mes y año 2022.

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 19 de diciembre de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 24 de enero de 2023 se recibe en esta Agencia escrito de respuesta indicando: *<<Tras analizar la reclamación e investigar lo sucedido, Vodafone ha podido comprobar que se efectuaron distintas acciones fraudulentas sobre las dos líneas de telefonía móvil pertenecientes al reclamante.*

Sobre la línea ******TELEFONO.1****, se tramitaron dos duplicados de SIM, en fecha 19 de abril de 2022 y 3 de junio de 2022. Así como también se tramitaron otros dos duplicados de SIM sobre la línea* ******TELEFONO.2****, en idénticas fechas.*

La totalidad de los duplicados de SIM mencionados, fueron gestionados de forma telefónica, a través de un colaborador de esta entidad en la gestión del servicio de atención al cliente.

Tras las actuaciones fraudulentas mencionadas, se produjo un intento de cambio de titular en ambas líneas de telefonía móvil relativas al reclamante.

Primeramente, sobre la línea ******TELEFONO.1*** *se tramitaron dos cambios de titularidad diferentes con fecha 10 de junio de 2022, 13 de junio de 2022, realizándose en fecha 14 de junio de 2022 un ulterior cambio a fin de restituir el dominio de la línea de telefonía móvil al reclamante.*

En segundo lugar, sobre la línea ******TELEFONO.2****, se tramitó un cambio de titularidad con fecha 13 de junio de 2022, restituida la titularidad del reclamante sobre su línea de telefonía móvil en fecha 14 de junio de 2022.*

Quiere esta parte señalar que la efectiva gestión de un duplicado de tarjeta SIM conlleva la superación de las políticas de seguridad que Vodafone 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.

En vista de los hechos acontecidos, una vez que el reclamante se percató de los hechos denunciados, el día 14 de junio de 2022, se puso en contacto con mi representada indicando que las gestiones anteriores se habían realizado supuestamente sin su consentimiento, siendo este el primer momento en que Vodafone tuvo conocimiento de los hechos objeto de reclamación.

En este sentido, mi representada procedió a realizar las investigaciones y gestiones oportunas a fin de resolver la incidencia acontecida.
Por ello, el mismo día en el que se tuvo constancia de los hechos objeto de la reclamación, tras verificar Vodafone que estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento; procedió a desactivar las tarjetas

SIM fraudulentas y gestionar el cambio de titular para rectificar esta incidencia, activando sobre la cuenta de cliente del reclamante medidas de seguridad adicionales para evitar cualquier otro perjuicio al reclamante.

Por tanto, mi representada logró solventar las incidencias objeto de reclamación de forma efectiva el 14 de junio de 2022, es decir, el mismo día en el que se tuvo constancia de los hechos y con anterioridad a la recepción del presente requerimiento por parte de la Agencia>>.

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 10 de octubre de 2022, se comunica que su reclamación ha sido admitida a trámite, el día 10 de enero de 2023, 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:

El día 19 de abril y 3 de junio de 2022 se realizaron duplicados de las tarjetas SIM de dos líneas del reclamante, a raíz de solicitudes realizadas mediante llamada telefónica con numeración oculta. Los duplicados se emitieron por establecimientos externos autorizados. El 13 de junio de 2022 se realizó el cambio de titular, de nuevo mediante llamada telefónica con numeración oculta, también para las dos líneas del reclamante.

Indican que las actuaciones denunciadas por el reclamante han sido calificadas como fraudulentas, tanto los duplicados de sus tarjetas SIM como el cambio de titularidad.

Asimismo, manifiestan que lo sucedido fue declarado como fraudulento por el Departamento de Fraude de la entidad y que se implementaron medidas de seguridad adicionales sobre la cuenta de cliente del reclamante para que no se produjeran incidencias similares en el futuro.

En la documentación que aportan consta un comentario sobre que el *“cliente no entiende porque se ha tramitado con los antecedentes anteriores y amenaza baja”.* No obstante, no se encuentra en la documentación aportada ninguna solicitud de marcado

como víctima de fraude por parte del cliente. Se indica en la documentación que se contactó con el cliente, pero no quería el bloqueo ya que prefería consultar con sus abogados.

La parte reclamada manifestó que, una vez que el reclamante se percató de los hechos denunciados, el día 14 de junio de 2022, se puso en contacto indicando que las gestiones anteriores se habían realizado sin su consentimiento, manifestando la parte reclamada que este es el primer momento en que tuvieron conocimiento de los hechos objeto de reclamación.

Los correos electrónicos aportados por el reclamante junto a su reclamación, en los que pone los hechos en conocimiento de Vodafone, son posteriores al citado día 14 de junio de 2022.

En las presentes actuaciones de Investigación se ha requerido a la parte reclamada para que aporte documentación acreditativa de haber verificado la identidad del solicitante de los duplicados SIM realizados el 19/04/2022 y el 3/06/2022, así como los cambios de titularidad del día 13/06/2022.

Ante ello indican que el protocolo de actuación de la entidad cuando se realiza una solicitud de duplicado SIM por teléfono es la comprobación de la identidad del solicitante mediante la superación de la Política de Seguridad para Contratación de Particulares, sin que se requiera documentación adicional al solicitante para el cambio, y que si el solicitante supera esta Política de Seguridad se activan los trámites oportunos para atender su petición. No aportan ninguna documentación que acredite el efectivo paso de la Política, ni la efectiva solicitud de los datos por parte del operador para pasar la política, ni qué datos fueron facilitados por el solicitante, en su caso.

Añaden que no disponen de las grabaciones telefónicas ya que las llamadas no fueron grabadas. Indican que las llamadas telefónicas recibidas por los servicios de atención al cliente de la entidad solo son grabadas de forma aleatoria y con fines de calidad de la atención dispensada al cliente, siendo prácticamente inviable la grabación y conservación de la totalidad de las gestiones efectuadas telefónicamente ante los servicios de atención al cliente de la entidad.

Exponen que en fecha 14 de junio de 2022, día en el que tuvieron conocimiento de los hechos que originaron la incidencia, se activó una marca de víctima de fraude en la ficha de cliente del reclamante.

Aportan captura de pantalla en la que consta para el 14/06/2022 "*Activación del check Víctima…".* Indican que como consecuencia de la aplicación de la marca de víctima de fraude, se insertó un aviso de seguridad en la cuenta de cliente del reclamante con la leyenda: "*No facilitar información, realizar modificaciones, activación de productos, pedidos etc., si el cliente llama desde líneas distintas a las que tiene contratadas en Vodafone, ocultación de llamada y origen internacional. Se debe consultar y seguir siempre la política de seguridad*". Aportan una captura de pantalla en la que se refleja este aviso de seguridad.

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 26 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 y presentó escrito de alegaciones el día 16 de agosto de 2023 en el que, en síntesis, manifiesta: *<<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 del reclamante conforme al artículo 6.1 del RGPD.*

Así las cosas, y como ya se ha expuesto anteriormente en las alegaciones como respuesta a los requerimientos de información sobre el expediente objeto de las presentes, siendo el 14 de junio de 2022 el primer momento en que Vodafone tuvo conocimiento de los hechos objeto de reclamación, mi representada procedió a realizar las investigaciones y gestiones oportunas a fin de resolver la incidencia acontecida, verificado que Vodafone estaba ante gestiones que, pese a tener la apariencia de veraces, eran de carácter fraudulento, procediendo en consecuencia a desactivar las tarjetas SIM fraudulentas y activando sobre la cuenta de cliente del reclamante medidas de seguridad adicionales para evitar cualquier otro perjuicio al reclamante. De este modo, mi representada logra solventar las incidencias objeto de reclamación de forma efectiva el 14 de junio de 2022, esto es, el mismo día en que se tuvo conocimiento de los hechos.

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.

En el presente caso, el defraudador se hizo pasar por el titular de las líneas proporcionando toda la información relativa al reclamante para superar la política de seguridad de Vodafone y conseguir los duplicados SIM, aportando a la gestión en todo

momento apariencia de licitud y veracidad. Vodafone actuó en todo momento conforme a sus políticas de seguridad y realizó una correcta verificación 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.

Respecto a la prueba de la superación de la política de privacidad, cabe reafirmar que el protocolo de actuación de Vodafone cuando se realiza una solicitud de duplicado SIM vía telefónica es la comprobación de la identidad del solicitante mediante su vinculación a la superación de la Política de Seguridad sin que se requiera documentación adicional del solicitante para el cambio, por lo que habiendo superado el solicitante lo previsto en la Política de Seguridad se activan los trámites oportunos para atender su petición. En el mismo sentido, y con respecto a la grabación telefónica de las llamadas a través de las cuales el defraudador consigue los duplicados SIM, mi representada, debido a que las llamadas telefónicas recibidas por los servicios de atención al cliente de Vodafone solo son grabadas de forma aleatoria y con fines de calidad de la atención dispensada al cliente, conforme se informa expresamente a los interesados en la realización de cualquier trámite por canal telefónico, no dispone de la grabación en tanto dichas llamadas no fueron grabadas.

Consecuencia de la ausencia de las grabaciones telefónicas y del paso de la Política de Seguridad vía telefónica por parte del defraudador que no requiere documentación acreditativa adicional, no es posible aportar prueba fehaciente de la superación de la Política de Seguridad solicitada a petición de esta Agencia. No obstante lo anterior, la Política de Seguridad seguida por todos los empleados de Vodafone, incluidos los agentes telefónicos, prevé los pasos necesarios para que, en atención a trámite efectuado, se compruebe la identidad del contratante, por lo que, pese a no existir la grabación de los concretos trámites telefónicos, Vodafone presume que dichas gestiones se supeditaron a la superación de la Política de Seguridad y, por tanto, entendió en ese momento que la gestión realizada era legal y con apariencia de veracidad.

Asimismo, y en relación con la diligencia debida por parte de los agentes colaboradores de Vodafone en los servicios de atención al cliente, cabe destacar que las entidades a las que estos pertenecen actúan en calidad de encargadas del tratamiento de Vodafone, quedando sujetas a la obligación, de acuerdo con el artículo 28.3.a) del RGPD, de tratar los datos personales únicamente siguiendo las instrucciones del responsable del tratamiento. Siendo así, mi representada, no solo ha escogido en todo caso a sus colaboradores en base a las garantías de cumplimiento de los requisitos contemplados en la normativa aplicable en materia de protección de datos ofrecidas por estos, sino que ha regulado la relación con los mismos de forma robusta formalizando el correspondiente acuerdo de tratamiento de datos y proporcionando todas las políticas e instructivos necesarios para el desarrollo de la actividad, no solo al inicio de la relación contractual, sino durante el desarrollo de la

misma, tal y como se ha venido acreditando anteriormente mediante la aportación de los comunicados realizados por mi representada, entendiéndose todos ellos como instrucciones claras sobre los procedimientos internos de Vodafone en el marco de la relación responsable-encargado y, por tanto, de obligado cumplimiento.

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.

Con carácter subsidiario, en el caso de que esta Agencia entendiera que Vodafone sí ha infringido el artículo 6.1 del RGPD, no procede la imposición de sanción alguna a mi mandante por los motivos que se verán a continuación. Vodafone no ha actuado culposamente, por lo que no procede la imposición de sanción alguna.

Por ello, en el caso de que la Agencia entendiera que la conducta de Vodafone es constitutiva la infracción indicada en el Acuerdo de Inicio, es claro que no concurre en la conducta de Vodafone culpabilidad ninguna, ni a título de dolo ni a título de culpa.

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.

Vodafone ha diseñado políticas de seguridad para prevenir el cambio fraudulento de tarjetas SIM. Dichas políticas de seguridad son seguidas por los agentes y son "apropiadas para garantizar un nivel de seguridad adecuado al riesgo" y por ende “el tratamiento lícito de los datos personales”. Vodafone no sólo ha implementado políticas de seguridad para hacer frente a los duplicados fraudulentos de tarjetas SIM, sino que ha ido actualizando dichas medidas de seguridad y envía comunicados y alertas a sus tiendas y agentes para asegurarse de que éstas se mantienen alerta.

En consecuencia, Vodafone ha actuado en todo momento cumpliendo con la diligencia debida que le es exigible, no pudiendo imputársele culpabilidad alguna.

Por ello, teniendo en cuenta la especial naturaleza del Derecho administrativo sancionador que determina la imposibilidad de imponer sanciones sin tener en cuenta la culpabilidad y la diligencia, o los errores que hayan podido determinar el incumplimiento de una obligación legal, esta parte mantiene la improcedencia de la imposición de sanción alguna.

En su Acuerdo de Inicio, la Agencia entiende que, en relación con la supuesta infracción del artículo 6.1 del RGPD, concurrirían los siguientes agravantes y

atenuantes: 1. Agravantes: • Toda infracción anterior cometida por el responsable o el encargado del tratamiento. • La vinculación de la actividad de Vodafone con la realización de tratamientos de datos de carácter personal. 2. Atenuantes: Procedió la parte reclamada a solventar la incidencia objeto de la reclamación de forma efectiva.

Mi mandante discrepa respetuosamente de los agravantes indicados en el Acuerdo de Inicio por los motivos que se expondrán a continuación y por los cuales entiende que la sanción – de ser impuesta – debe modularse a la baja.

I. Toda infracción anterior cometida por el responsable o el encargado del tratamiento.

En los tres expedientes mencionados por la Agencia efectivamente Vodafone se acogió a una reducción de la sanción, sin asunción de culpa.

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.

Además de la medida atenuante indicada por la Agencia en el Acuerdo de Inicio, con las que mi mandante está conforme, 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, solicito 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 12 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/00028/2023. 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: Notificada la propuesta de resolución conforme a las normas establecidas en, la LPACAP, la parte reclamada solicitó ampliación del plazo y presentó escrito de alegaciones el día 23 de noviembre de 2023 en el que, en síntesis, manifiesta: << *Vodafone se remite en su integridad a las Alegaciones al Acuerdo de Inicio*, *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 La Agencia, en su Propuesta de Resolución, indica que Vodafone no verificó la identidad de la reclamante para gestionar el duplicado de dos tarjetas SIM y que por tanto no siguió el procedimiento implementado por ella misma, hecho que motiva la infracción que se impone en el Acuerdo. Ante esta afirmación manifestamos nuestra respetuosa disconformidad, pues Vodafone tiene implementadas las medidas técnicas y organizativas adecuadas para identificar correctamente a sus clientes. 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 o que el procedimiento implantado no se haya seguido con la diligencia debida, sino que se han obtenido los datos necesarios, por medios ajenos a mi representada, para superar sus medidas.*

Asimismo, es preciso recordar que, siempre existirá un riesgo inherente o inicial implícito en cualquier tratamiento y, una vez que se hayan aplicado medidas y garantías que lo minimicen, seguirá existiendo un riesgo residual".

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. En este sentido debemos destacar que la política de seguridad de Vodafone ha sido actualizada con frecuencia desde la fecha en la que los hechos fueron denunciados por el reclamante en aras de reforzar el proceso y disminuir el volumen de incidencias de este tipo.

Por todo ello, Vodafone ha implementado las medidas técnicas y organizativas necesarias y adecuadas al riesgo del tratamiento de datos que realiza, minimizando al máximo posible el riesgo prevalente asociado a la propia actividad.

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.

La Agencia entiende que, en la medida en la que mi representada ha inobservado su deber de cuidado, existe dolo o culpa y, por ende, existe una responsabilidad sancionadora. No obstante, la AEPD no toma en consideración para su análisis todas las medidas que existían en el momento en el que ocurrieron los hechos objeto de sanción y las medidas de mejora que ha ido implementando Vodafone, obrando con la máxima diligencia que le es exigible.

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 mediante la aportación de los procesos que tiene implementados. Con respecto a la ausencia de pruebas fehacientes de superación de la política de seguridad, ya sea, bien mediante la aportación de las grabaciones de las llamadas telefónicas, bien mediante documentación acreditativa recabada durante el proceso, cabe reafirmar que el protocolo de actuación de Vodafone contempla la grabación aleatoria de llamadas con motivos de calidad motivo por el cual no se dispone del 100% de las llamadas, y, con respecto a la comprobación de la identidad del solicitante mediante su vinculación a la superación de la Política de Seguridad, no se requiere documentación adicional del solicitante para el cambio.

El criterio adoptado por mi representada en este sentido sigue el principio de minimización de datos y, en particular con respecto a la obtención de copia del DNI como prueba fehaciente de superación de la política de seguridad, lo indicado por el Comité Europeo de Protección de Datos en las Directrices 1/2022, v. 2.0, de 28 de marzo de 2023, que recogen el carácter residual que debe revestir el tratamiento del DNI como método de identificación atendiendo al riesgo que puede suponer, avalado a su vez por esta Agencia en su informe 0048/2023; en particular cabe resaltar lo

siguiente: • En relación a lo dispuesto en el artículo 70 del mencionado texto que establece que "si el responsable del tratamiento tiene motivos razonables para dudar de la identidad de la persona solicitante, podrá solicitar información adicional o confirmar la identidad del interesado. No obstante, el responsable del tratamiento debe asegurarse al mismo tiempo de que no recoge más datos personales de los necesarios para permitir la identificación de la persona solicitante. Por lo tanto, el responsable del tratamiento llevará a cabo una evaluación de la proporcionalidad, que deberá tener en cuenta tipo de datos personales tratados (por ejemplo, categorías especiales de datos o no), la naturaleza de la solicitud, el contexto en el que se realiza la solicitud, así como cualquier daño que pueda derivarse de una divulgación indebida. Al evaluar la proporcionalidad, debe recordarse que debe evitarse una recopilación excesiva de datos, garantizando al mismo tiempo un nivel adecuado de seguridad del tratamiento" Vodafone ha llevado a cabo tal juicio de proporcionalidad, concluyendo que, si el solicitante supera exitosamente la Política de Seguridad, no existe motivo alguno para dudar de su identidad y, que por tanto, solicitar copia del documento de identidad supondría una recopilación y tratamiento de datos excesivo para el fin perseguido. • De acuerdo con el artículo 71, "el responsable del tratamiento debe aplicar un procedimiento de autenticación (verificación de la identidad del interesado) para estar seguro de la identidad de las personas (…) El método utilizado para la autenticación debe ser pertinente, adecuado, proporcionado y respetar el principio de minimización de datos. Si el responsable del tratamiento impone medidas destinadas a identificar al interesado que son gravosas, debe justificarlo adecuadamente y garantizar el cumplimiento de todos los principios fundamentales, incluida la minimización de los datos y la obligación de facilitar el ejercicio de los derechos de los interesados (artículo 12, apartado 2, del RGPD)" la Política de Seguridad de mi representada constituye procedimiento de verificación de la identidad de los solicitantes, encontrándose cualquier operación como son los duplicados SIM supeditada a la superación de la misma, procedimiento que, mediante el requerimiento verbal de ciertos datos personalísimos como son el número de DNI y los últimos dígitos de la cuenta bancaria, permite verificar la identidad de la persona respetando el principio de minimización al evitar tratar datos excesivos contenidos en el DNI a los que se tendría acceso al requerir copia del documento.

• En relación al riesgo que supone la utilización de una copia del documento de identidad como parte del proceso de autenticación, el Comité Europeo considera que "crea un riesgo para la seguridad de los datos personales y puede dar lugar a un tratamiento no autorizado o ilícito, por lo que debe considerarse inadecuada, salvo que sea estrictamente necesario, adecuado y conforme con el Derecho nacional" Por lo tanto, mi representada sí que actuó con la diligencia debida, implementando las medidas técnicas y organizativas necesarias.

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.

En consecuencia, a través de esta lógica argumental se impone a Vodafone la obligación de evitar todos los fraudes, siendo una obligación absoluta, no una de medios, lo que iría en contra de lo dispuesto por la Audiencia Nacional.

Subsidiariamente, y para el caso de que la Agencia entienda que ha existido infracción y deba imponerse una sanción a Vodafone, deberán tenerse en cuenta las siguientes circunstancias agravantes y atenuantes La Agencia, a través de su Propuesta de Resolución, ha desestimado las alegaciones presentadas por mi mandante respecto de los agravantes y atenuantes aplicables al caso.

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

I. Toda infracción anterior cometida por el responsable o el encargado del tratamiento.

En los tres expedientes mencionados por la Agencia efectivamente Vodafone se acogió a una reducción de la sanción, sin asunción de culpa y, en todo caso, es necesario aclarar una serie de extremos:

Así las cosas, esta parte considera que la aplicación de esta agravante no ha sido lo suficientemente motivada por parte de la Agencia, suponiendo su aplicación un perjuicio grave para la defensa de mi mandante y la seguridad jurídica dado que cualquier incumplimiento del artículo 6.1 del RGPD en general, sin atender a los hechos probados de cada caso, valdría como mera prueba de la aplicación de esta agravante con la inherente consecuencia de graduar el importe de la sanción al alza.

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 La Agencia, en su Propuesta de Resolución, desestima este atenuante en la medida en la que entiende que "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". 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 el 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 Vodafone, 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 A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS 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.>>

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

HECHOS PROBADOS

PRIMERO. - La parte reclamante formuló reclamación ante esta Agencia el día 10 de octubre de 2022 en la que se hace constar que Vodafone tramitó duplicados de las tarjetas SIM de sus dos líneas de telefonía móvil a un tercero desconocido, que estos hechos se llevaron a cabo los días 19 y 20 de abril y 3 de junio del año 2022, a través de solicitudes realizadas telefónicamente, y también llevaron a cabo un cambio de la titularidad de las dos líneas de telefonía móvil.

SEGUNDO. - Obra en el expediente, que con fechas 19 de abril y 3 de junio de 2022 se realizaron duplicados de las tarjetas SIM de dos líneas del reclamante, a raíz de solicitudes realizadas mediante llamada telefónica con numeración oculta. Los duplicados se emitieron por establecimientos externos autorizados por Vodafone.

TERCERO. - Obra en el expediente, que los días 10 y 13 de junio de 2022 se tramitaron dos cambios de la titularidad de una de las dos líneas de la parte reclamante y de la otra línea el 13 de junio de 2022, mediante llamadas telefónicas con numeración oculta fueron gestionados de forma telefónica, a través de un colaborador de Vodafone en la gestión del servicio de atención al cliente.

CUARTO. - Vodafone, reconoce tanto en su escrito de fecha 16 de marzo de 2023 y en sus alegaciones de fecha 16 de agosto del mismo año, lo siguiente: *<<no se recabó copia del documento nacional de identidad del solicitante del duplicado SIM. Asimismo, esta representación debe indicar que no dispone de la grabación telefónica solicitada en tanto que dicha llamada no fue grabada.>>*

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 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.*

No obstante, Vodafone 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.

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.[...]".

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*".

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 que a petición de un tercero los días 19 de abril y 3 de junio del año 2022 se llevaron a cabo el duplicado de la tarjeta SIM de las dos líneas de teléfono del reclamante, a raíz de las solicitudes realizadas mediante llamada telefónica con numeración oculta.

Así las cosas, con fecha 13 de junio de 2022, se efectuó por Vodafone el cambio de la titularidad de las dos líneas del reclamante, de nuevo mediante llamada telefónica con numeración oculta, por lo que dicho tercero tuvo acceso a sus datos bancarios y realizó diversas operaciones no autorizadas.

Pues bien, estos hechos están clasificados de fraudulentos por la parte reclamada.

No obstante, Vodafone no aportó en la solicitud de requerimiento de esta Agencia la documentación acreditativa de haber verificado la identidad del solicitante para estos casos concretos, y con fecha 14 de junio de 2022 marcó en su sistema de información

al reclamante como víctima de fraude, declarando que fue la fecha en la que tuvo conocimiento de los hechos.

Sobre lo anterior, debemos manifestar que para que el tratamiento de datos efectuado por la reclamada pudiera estar fundado en alguna de las circunstancias legitimadoras del tratamiento sería preciso que, en su condición de responsable del tratamiento, pudiera acreditar que el titular de los datos tratados fue efectivamente quien los facilitó.

Así, en la respuesta a la solicitud informativa de la AEPD de fecha 16 de marzo de 2023, Vodafone adujo << *no se recabó copia del documento nacional de identidad del solicitante del duplicado SIM.*

Asimismo, esta representación debe indicar que no dispone de la grabación telefónica solicitada en tanto que dicha llamada no fue grabada>>.

En línea con lo expuesto con anterioridad, Vodafone, reconoce en el escrito citado que los duplicados de la tarjeta SIM fueron fraudulentos, pero ni tiene la documentación ni las grabaciones. Además, la llamada para la petición de los duplicados se realizó utilizando números ocultos.

En definitiva, 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 todo caso, no se siguió el procedimiento implantado por ella misma, ya que, de haberlo hecho, se debió haber producido su denegación.

A la vista de lo anterior, Vodafone no logra acreditar que se haya seguido ese procedimiento y por consiguiente hubo un tratamiento ilícito de los datos personales de la parte reclamante, contraviniendo con ello el artículo 6 del RGPD.

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.

Hay que resaltar, que Vodafone, no verificó la personalidad del que solicitó duplicados de las tarjetas SIM, ni tampoco del cambio de la titularidad de los dos líneas del 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 tanto los duplicados de la tarjeta SIM, como el cambio de la titularidad.

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"*.

IV

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.

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.

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;".*

El grado de cooperación con la Agencia tampoco puede considerarse un atenuante toda vez que la notificación de la brecha a la AEPD, así como la aportación de la información al respecto, es algo a lo que están obligados los responsables del

tratamiento de conformidad con el artículo 33 del RGPD. La consideración de la cooperación con la Agencia como atenuante, tal y como pretende Vodafone, 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 *"debe considerarse que el deber ordinario de cooperación es obligatorio y, por tanto, debe considerarse neutro (y no un factor atenuante)."*

Así queda confirmado en la mismas Directrices del CEPD sobre la aplicación y la fijación de 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.

Sobre la aplicación del artículo 76.2.c) de la LOPDGDD, en conexión con el artículo 83.2.k), inexistencia de beneficios obtenidos, cabe señalar que tal circunstancia no puede ser considerada como un criterio atenuante, en todo caso se trataría de una circunstancia neutra.

El artículo 83.2.k) del RGPD se refiere a *"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." Y el artículo 76.2c) de la LOPDGDD dice que "2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta: [..] c) Los beneficios obtenidos como consecuencia de la comisión de la infracción."* Ambas disposiciones mencionan como factor que puede tenerse en cuenta en la graduación de la sanción los "beneficios" obtenidos, pero no la "ausencia" de éstos, que es lo que Vodafone alega.

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 la ausencia de beneficios es contraria al espíritu del artículo 83.1 del RGPD y a los principios por los que se rige la determinación del importe de la sanción de multa. Si a raíz de la comisión de una infracción del RGPD se califica como atenuante que no han existido beneficios, se anula en parte la finalidad disuasoria que se cumple a través de la sanción. Aceptar la tesis de Vodafone 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.

La Sala de lo Contencioso Administrativo de la Audiencia Nacional ha advertido que, el hecho de que en un supuesto concreto no estén presentes todos los elementos que integran una circunstancia modificativa de la responsabilidad que, por su naturaleza, tiene carácter agravante, no puede llevar a concluir que tal circunstancia es aplicable en calidad de atenuante. El pronunciamiento que hace la Audiencia Nacional en su SAN de 5 de mayo de 2021 (Rec. 1437/2020) -por más que esa resolución verse sobre la circunstancia del apartado e) del artículo 83.2. del RGPD, la comisión de infracciones anteriores- es extrapolable a la cuestión planteada, la pretensión de la reclamada de que se acepte como atenuante la "ausencia" de beneficios siendo así que tanto el RGPD como la LOPDGDD se refieren solo a "los beneficios obtenidos":

En aras a graduar el importe de la sanción de multa que se propone imponer a Vodafone 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 202204287 Resolución dictada el 24 de octubre de 2022 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación. Vodafone se acogió a una de las dos reducciones previstas.

ii.EXP 202203916. Resolución dictada el 24 de octubre de 2022 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación. Vodafone se acogió a una de las dos reducciones previstas.

iii.EXP202203914 Resolución dictada el 24 de octubre de 2022 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación. Vodafone se acogió a una de las dos reducciones previstas.

- 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 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 VODAFONE ESPAÑA, S.A.U. con NIF A80907397, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de por un importe de 200.000 euros (doscientos mil euros).

SEGUNDO: NOTIFICAR la presente resolución a VODAFONE ESPAÑA, S.A.U. con NIF A80907397.

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