- **Expediente N.º: EXP202210101**

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 15 de agosto de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ORANGE ESPAGNE, S.A.U. con NIF A82009812 (en adelante, la parte reclamada u Orange). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, sin su consentimiento, Orange facilitó a un tercero un duplicado de la tarjeta SIM de su teléfono móvil y este accedió a sus datos bancarios, y cuya consecuencia derivó en un perjuicio patrimonial.

Así las cosas, señala que el día 1 de agosto de 2022, su teléfono móvil dejó de funcionar y recibió varios correos electrónicos relativos a un aviso de consumo de 100Mb del contrato y otro correo electrónico indicando lo siguiente: *"Se ha tramitado con éxito la activación de tu tarjeta eSIM"*.

A raíz de lo ocurrido, contactó con la parte reclamada solicitando la anulación de la tarjeta SIM, indicando la parte reclamada *"que no podían anular dicha tarjeta por protocolo"*, por lo que tuvo que esperar cuatro días para recibir, físicamente, una nueva y poder así anular la anterior.

Y, aporta la siguiente documentación relevante:

- Reclamación formulada ante Orange.
- Impresión de pantalla de los mensajes recibidos (entre ellos, el mensaje relativo a la activación de la tarjeta eSIM).
- Impresión de pantalla de las llamadas realizadas al Servicio de Atención al Cliente.
- Impresión de pantalla de la conversación mantenida con la parte reclamada, a través del chat. En ellas se aprecia que el reclamante indica que su móvil ha dejado de funcionar (su tarjeta está deshabilitada) y que él no ha solicitado ninguna tarjeta eSIM, solicita un duplicado nuevo y Orange manifiesta que tendría que enviárselo.
- Denuncia presentada ante la Policía Nacional el día 3 de agosto de 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 3 de octubre de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 3 de noviembre de 2022 se recibe en esta Agencia escrito de respuesta indicando: << *Orange dio traslado al Grupo de Análisis de Riesgos de esta mercantil, el cual procedió a hacer un estudio de la incidencia, cuyos pormenores se reproducen a continuación. Derivado del análisis anteriormente mencionado se detectó que el duplicado de e-SIM se había realizado usurpando la identidad del Reclamante.*

En este sentido, el usurpador accedió al área privada web de Cliente (en adelante, APC) del Reclamante, iniciando posteriormente una conversación con el Canal digital asistido y solicitando a través de este medio el duplicado de eSIM. Habiéndose, pues, constatado la irregularidad en la solicitud del duplicado, el equipo de Análisis de Riesgos confirmó que el Reclamante, titular de la línea ******TELEFONO.1****, ha sido, probablemente, víctima de phishing, smishing o algún otro instrumento de ingeniería social (el cual no ha podido ser identificado por esta mercantil en el curso de las investigaciones) a través de su APC desde donde se solicitó el duplicado e-SIM sin haberse solicitado un reseteo de las contraseñas, es decir, el malhechor ya la conocía previamente*.

Al detectar dicha irregularidad en la solicitud del duplicado SIM, se registró esta incidencia en los sistemas internos de esta mercantil en aras a evitar que se devengasen cargos por la generación de los duplicados en factura. Es por ello que no se realizó ningún cargo adicional en Orange al Reclamante por estos sucesos, ni el suplantador de identidad pudo contratar más servicios o líneas con el duplicado de SIM del Reclamante en Orange.

Adicionalmente, se procedió a rastrear el IMEI del dispositivo desde el que se realizó el duplicado de e-SIM fraudulento, incluyéndolo en BlackList interna, de forma que el mismo no pudiera volver a ser utilizado a estos efectos.

Por último, se procedió a realizar ajustes al Reclamante por los cargos generados por los dos duplicados de SIM quedando informado de tales extremos por parte del equipo que gestionó la incidencia.

En el momento de solicitar el duplicado de e-SIM fraudulento, el usurpador accedió a la APC del Reclamante sin haber realizado previamente un cambio o reseteo de contraseña, solicitando el duplicado electrónico de la tarjeta SIM (E-sim), y, debido a que facilitó adecuadamente los datos personales del Reclamante, se le envió el QR de activación de la e-SIM vía email, produciéndose así a la activación del duplicado.

Es decir, que el suplantador de identidad tenía en su poder los datos personales del Reclamante necesarios para acceder a su área privada. Por lo tanto, de forma previa a que éste tuviese contacto alguno con Orange, el mismo ya tenía conocimiento de los datos personales del Reclamante, a los cuales no accedió a través de esta mercantil.

Gracias a tener en su disposición los datos del Reclamante, le resulta posible activar el duplicado de tarjeta SIM.

Así, en el presente supuesto, se evidencia que la incidencia deviene, principalmente, de que el suplantador tuviera acceso a las credenciales del Reclamante para acceder al área privada, de forma previa a que intervenga esta entidad.

Desde el 12 de agosto de 2022 es obligatorio que los clientes se identifiquen de manera estricta con su DNI para cualquier cambio o contratación que quieran realizar desde el Canal digital asistido a través del APC, a pesar de haber accedido a la plataforma con su usuario y contraseña.

De igual manera, desde la citada fecha no se permite realizar duplicados de SIM o E-sim desde el APC, remitiendo al cliente a un punto de venta para gestionar dicha solicitud.

Asimismo, y de forma adicional, para el resto de los actos comerciales, exceptuando tal y como se ha indicado el duplicado de sim/E-sim, se está implementando de forma gradual que se establezca un sistema obligatorio de validación con Token, enviado a la línea del contrato>>.

TERCERO: Con fecha 11 de noviembre de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Solicitud y activación de la eSIM

En el traslado de la reclamación efectuado previamente la parte reclamada manifestó que en el caso concreto del reclamante la vía de solicitud de eSIM fue el Área Privada del Cliente, accediendo con el usuario y clave del cliente.

En las presentes actuaciones se ha requerido a la parte reclamada aportar documentación que acredite el acceso y la solicitud del eSIM por esa vía, así como documentación acreditativa de la conversación mantenida por el solicitante con el Canal digital asistido del Área Privada del Cliente.

En la contestación la parte reclamada indica que el usurpador accedió por dicha vía, probablemente tras haber sido víctima de *phishing, smishing* o algún otro instrumento

de ingeniería social, iniciando posteriormente una conversación con el Canal digital asistido y solicitando a través de este medio el duplicado de eSIM.

Aportan, dentro de los contactos registrados con el cliente o su supuesto suplantador, varios de fecha 01/08/2022 que reflejan que a las 19:03 se produjo un cambio de la dirección de correo electrónico del cliente, efectuado desde el Área del Cliente, y a las 20:07 el envío de un SMS informando de que puede escanear el código de activación del eSIM. Entre estos contactos que aportan no constan otros registros intermedios, no obstante, entre ambas horas se debió producir la solicitud de eSIM.

Por otra parte, cuando se requiere a la parte reclamada la fecha de activación de la eSIM, aportan una impresión de un registro de las 20:06 del 01/08/2022 en el que consta "canal digital asistido" categorizado como "cambio" "tarjeta SIM", indicando los representantes de la entidad que a esa hora se realizó la solicitud. A las 20:26 consta un contacto con el texto "*se ha tramitado con éxito la activación de tu tarjeta eSIM*".

Resolución del incidente

Constan contactos posteriores a los ya relatados, consistentes en comunicaciones del reclamante a la parte reclamada indicando que no ha solicitado un eSIM para solucionar el problema: a las 23:43 del mismo día de los hechos (01/08/2022) consta contacto en el que el cliente pregunta por qué se ha contratado una eSIM sin solicitarlo. Constan otros contactos entre ellos uno del día siguiente a los hechos (02/08/2022) con la anotación "*cliente se comunica porque el día de ayer quería duplicar su sim pero que le llegara ayer mismo, el agente le contrató una esim pero [el cliente] afirma que no le llegó ningún momento ni al correo ni por sms se comunica a cancelar el proceso y hoy se dirige a duplicar la sim en la tienda pero el sistema no le permite debido a que la esim está en espera de ser activada, se le indica en soluciones, entre un de ellas es dejar a que la esim se cancele en 72 horas y ahí sí generar el duplicado".*

Consta un contacto de fecha 03/08/2022 avisando de la entrega del pedido correspondiente a la SIM nueva. Consta un contacto de fecha 04/08/2022 indicando que ha sido entregado.

Se ha solicitado a la parte reclamada que informe sobre los motivos por los cuales no se desactivó la tarjeta eSIM cuando los hechos fueron puestos de manifiesto por el reclamante.

Los representantes de la parte reclamada manifiestan al respecto que debido a la naturaleza de este tipo de actos comerciales que implican solicitudes de duplicado tarjeta SIM, de desvío de llamadas, de cambios en datos de contacto etc., los protocolos establecidos para atención por parte del personal de primeras líneas para este tipo de gestiones son muy estrictos y requieren de medidas de carácter formal, ya sea la aportación de denuncias u otras políticas de identificación por lo que es probable que, el agente que atendió la solicitud del reclamante, al requerirle la denuncia y esta no ser aportada es probable que no pudo ejecutar la solicitud en primera instancia.

Indican que en fecha 3 de agosto de 2022 se bloqueó la numeración por robo/pérdida.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad ORANGE ESPAGNE, S.A.U. es una gran empresa constituida en el año 1998, y con un volumen de negocios de ***CANTIDAD.1** euros en el año 2021.

SEXTO: Con fecha 25 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 copia del expediente y ampliación del plazo que le fue concedido y presentó escrito de alegaciones en el que, en síntesis, se reitera en las alegaciones efectuadas el día 3 de noviembre de 2022 e indica*:<<que en un inicio las suplantaciones de identidad se concentraban en la solicitud de duplicados de tarjeta SIM de forma presencial y física; en la actualidad, los intentos de fraude han evolucionado especialmente en el ámbito digital y se concentran en la solicitud de duplicados y activación de tarjetas SIM por canales no presenciales, si bien hasta ahora se solicitaba un duplicado de tarjeta SIM física, vemos que, como en el supuesto actual, los delincuentes centran su objetivo en las tarjetas electrónicas "e-SIM" y por canales protegidos con credenciales de seguridad personales de los usuarios, lo que evidencia una sofisticación importante en las técnicas utilizadas por los delincuentes que comenten este tipo de delitos de suplantación de identidad.*

Añaden que, Orange ha decidido desactivar esta posibilidad de autogestión a través del Área Privada, estableciendo a su vez medidas de garantía adicional dentro del Canal Digital Asistido para la solicitud de realización de trámites y contrataciones que tal canal incorpore, exigiendo de forma previa y obligatoria, una verificación adicional por control directo desde el departamento de Fraude, quien analizará la documentación del cliente que solicita un duplicado de tarjeta SIM y será quien emita la autorización al equipo de gestión que soporta dicho canal digital asistido. La medida reseñada ha sido implementada en los sistemas de Orange con fecha 12 de agosto de 2022.

Asimismo, indican que no se produce un acceso no autorizado, sino que, como resultado de la obtención previa e ilícita de las credenciales de acceso del reclamante, el tercero se identifica en el área privada del reclamante de forma ordinaria. La protección con contraseña es una técnica de control de acceso, garantizando que solo se puede acceder por parte de la persona conocedora de las credenciales correctas, siendo la herramienta de seguridad de datos más extendida conforme al estado de la técnica actual.

El suplantador de identidad en ningún momento accedió al teléfono móvil - ni, consiguientemente, a la información que éste puede contener-, en tanto el teléfono móvil está en todo momento en posesión del Reclamante, como él mismo manifiesta en su reclamación.

En este sentido, es preciso establecer con rigurosidad los hechos acreditados, así como conocer la operativa de cada dispositivo: la tarjeta SIM no contiene los datos del teléfono o terminal móvil, por lo que el acceso a un duplicado de la misma no permite a un tercero el acceso a las aplicaciones que el Reclamante pueda tener instaladas en el mismo, como pueden ser las aplicaciones de las entidades bancarias. Adicionalmente, para poder acceder a las aplicaciones bancarias, los suplantadores de identidad deben conocer las credenciales bancarias del Reclamante.

La AEPD debe distinguir claramente este hecho, en tanto basa en el mismo, pese a ser equívoco, su fundamentación jurídica de la infracción. Derivado de lo anterior, no resulta posible imputar a esta parte la realización de un tratamiento de datos sin legitimación, en tanto el tercero se identifica de forma regular ante Orange, dentro de su entorno privado, fruto de la obtención de los datos del Reclamante de forma previa y supuestamente ilícita, sin que existiera en esa fecha reseteo de contraseña o indicio alguno de un acceso irregular a dicha área personal online.

Así, el tratamiento de datos de Orange resulta legítimo, teniendo base en la relación contractual existente con el Reclamante, tal y como recoge el Considerando 40 extractado por la Agencia en su fundamentación. Es por ello que no se produce un tratamiento ilegítimo de los datos del Reclamante ni se puede imputar a Orange falta de diligencia en la identificación del mismo, tal y como la Agencia identifica en su Acuerdo de Inicio, no siendo imputable a esta parte una infracción del Artículo 6.1 del RGPD.

El presente Acuerdo de Inicio de la Agencia se basa exclusivamente en un análisis del resultado, considerando que la obtención de un duplicado de tarjeta e-SIM por un tercero conlleva la automática consideración de que no se verificó la personalidad del contratante y, por tanto, a juicio de la AEPD, surgiendo automáticamente la responsabilidad directa por parte de Orange.

Es por ello que no resulta posible apreciar culpabilidad de Orange en el presente supuesto de hecho, no siendo jurídicamente válida la apreciación que realiza la Agencia de comisión de infracción por esta mercantil.

En atención a todas este despliegue de medidas mencionadas y diseñadas por Orange, considera esta parte que queda acreditado, no sólo la firme voluntad de esta mercantil en la protección de los derechos de los particulares, sino el empleo de un nivel de diligencia adecuado por parte de Orange con el que, si bien no resulta posible, por limitación de la tecnología y los medios humanos, la existencia de un riesgo cero, es actualizado y revisado periódicamente en conforme el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Tal y como se viene plasmando en las alegaciones presentadas, Orange ha demostrado haber actuado con la diligencia debida en la identificación del Reclamante, no teniendo lugar tratamiento de datos alguno sin legitimación. Sin perjuicio de lo anterior, y en el hipotético caso de que la Agencia considerase que existe algún tipo de incumplimiento, la sanción incluida en el Acuerdo de Inicio resulta, en todo caso, desproporcionada, atendiendo a las circunstancias y contenido de la

supuesta infracción, que Orange niega rotundamente. En este sentido, cabe destacar los siguientes puntos que conforme a la interpretación de la Agencia son calificados de agravantes, sin que concurran las circunstancias para su consideración en relación con los hechos analizados: Toda infracción anterior cometida por el responsable o encargado del tratamiento (artículo 83.2 e) del RGPD.

La valoración realizada por la Agencia únicamente tiene en cuenta las infracciones impuestas por vulneración del artículo 6.1 del RGPD, no obstante, el mismo abarca diferentes supuestos de hecho. Esta parte ha reseñado a lo largo del presente escrito las particularidades del presente supuesto, así como la innovación de las técnicas y medios empleados por los suplantadores de identidad para ejecutar las tentativas de comisión de fraude.

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). Si bien es cierto que la actividad de Orange hace necesario el tratamiento de datos personales de sus clientes, lo cierto es que este factor es ambiguo en su valoración para incluirlo como agravante, ya que dicha vinculación no supone ni mucho menos una relación directa con la supuesta infracción. El artículo 83.2 k) exige que dicho agravante sea puesto en relación con el supuesto de hecho concreto.

En este sentido, el tratamiento de datos no nace de una intención de la entidad, sino que tiene lugar la comisión de un delito del que Orange es parte perjudicada. Por todo ello, no cabe interpretar este aspecto como agravante. Adicionalmente, quisiera señalar esta parte que el perjuicio aludido por el Reclamante, consistente en la sustracción de fondos de sus cuentas bancarias, no se encuentra incluido en la actividad de esta mercantil.

ORANGE no puede hacerse cargo de la seguridad de la operativa de terceras entidades por el mero hecho de que usen servicios de telecomunicaciones.

Adicionalmente, y según lo establecido en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, además de la atenuante ya reconocida expresamente por la AEPD en su Acuerdo de Inicio: Procedió la parte reclamada a bloquear la línea en cuanto tuvo conocimiento de los hechos (art. 83.2 c); Concurren en el presente las siguientes circunstancias atenuantes que no han sido consideradas en la adecuada graduación de la sanción: En ningún momento se han tratado categorías especiales de datos.
El grado de cooperación de Orange con la AEPD con el fin de poner remedio a una supuesta infracción y mitigar sus posibles efectos adversos: ha quedado acreditado que se ha contestado en tiempo y forma a todos los requerimientos de información solicitados por esta Agencia, en línea con la práctica habitual de esta mercantil de total colaboración con la autoridad de protección de datos. El inexistente beneficio obtenido por parte de Orange derivado del tratamiento de datos que ocupa este procedimiento.

En todo caso, Orange se ha visto perjudicada, como ya se ha señalado, siendo parte perjudicada incluso en el procedimiento judicial en el que se denuncia la comisión del delito que nos ocupa.

Orange solicita que se dicte resolución por medio de la cuál señale el archivo del Procedimiento. Subsidiariamente, culmine el procedimiento mediante un apercibimiento y, en última instancia, si considera que procede la imposición de una sanción, modere o module su propuesta recogida en el Acuerdo de Inicio notificado a Orange, atendiendo a los argumentos manifestados en el cuerpo del presente escrito de alegaciones>>.

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/00403/2022. 2.Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por* ***ORANGE ESPAGNE, S.A.U.****, y la documentación que a ellas acompaña>>.*

NOVENO: Con fecha 17 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 ORANGE ESPAGNE, S.A.U. con NIF A82009812, por la presunta infracción del artículo 6.1) tipificada en el artículo 83.5.a) del citado RGPD. con una multa de 200.000 euros (doscientos 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, en síntesis, se reitera en las alegaciones alegaciones previamente presentadas, y en síntesis manifiesta que: *<<Si bien esta parte reconoce que el proceso de emisión de un duplicado de tarjeta SIM implica el tratamiento de datos, ha de puntualizarse que durante el mismo, Orange no ha puesto a disposición de los suplantadores de identidad ningún dato.*

El único interviniente que ha facilitado datos en el presente supuesto de hecho es el propio suplantador de identidad, al acceder al Área Privada de Clientes de Orange, en concreto, al facilitar el usuario y contraseña utilizado como credenciales de seguridad por el Reclamante, necesario para acceder.

Tras ello, el solicitante realiza una petición de duplicado de tarjeta SIM, la cuál se le concede al constar, mediante sus credenciales de seguridad, identificado como el titular de la línea. Tras ello, se le remite un email con el código para activar la SIM.

En el presente caso, consta probado que a lo que tuvo acceso el suplantador fue a un duplicado de una tarjeta e-SIM vacía, sin ninguna información personal. Y no consta referencia alguna entre las pruebas que constan en el expediente, de que se hubiese accedido a ninguna información personal del Reclamante como consecuencia de la puesta a disposición del duplicado de la SIM.

La tarjeta SIM no contiene los datos del teléfono o terminal móvil, por lo que el acceso a un duplicado de la misma no permite a un tercero el acceso a las aplicaciones que el Reclamante pueda tener instaladas en el mismo, como pueden ser las aplicaciones de las entidades bancarias. Adicionalmente, para poder acceder a las aplicaciones

bancarias, los suplantadores de identidad deben conocer las credenciales bancarias del Reclamante.

Así, el tratamiento de datos de Orange resulta legítimo, teniendo base en la relación contractual existente con el Reclamante. Durante dicho proceso no se facilitó por parte de Orange ningún dato personal al solicitante ni a ninguna otra persona, por lo que no se ha producido un tratamiento no legitimado de datos personales.

El hecho de que la persona que realiza los trámites no se corresponda, supuestamente, con la titular del contrato no supone per se que exista ninguna falta de legitimación en su tratamiento.

Es un hecho que las entidades bancarias son las únicas responsables de la seguridad de sus operaciones, tal y como lo afirma la Autoridad Bancaria Europea (en adelante, la "EBA") en los siguientes pronunciamientos: • Opinion on the implementation of the RTS on SCA and CSC: en su apartado relativo a quién decide sobre los medios a emplear para dicha autenticación (puntos 37 y 38), dictamina que las credenciales de seguridad utilizadas para realizar la autenticación segura de los usuarios de los servicios de pago son responsabilidad de la entidad gestora de servicios de cuenta (en el caso que nos ocupa, las entidades financieras). • Qualification of SMS OTP as an authentication factor | European Banking Authority: indica que el uso de SMS ordinarios no es factible para la confirmación de operaciones bancarias, por no ser suficientemente seguros conforme a los estándares de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior (PSD2).

En este sentido, indica que: "el artículo 22 (1) del Reglamento exige que 'los proveedores de servicios de pago garantizarán la confidencialidad e integridad de las credenciales de seguridad personalizadas del usuario del servicio de pago, incluidos los códigos de autenticación, durante todas las fases de la autenticación' y el artículo 22, apartado 4, del Reglamento Delegado establece que 'los proveedores de servicios de pago garantizarán que el procesamiento y el enrutamiento de las credenciales de seguridad personalizadas y de los códigos de autenticación generados de conformidad con el Capítulo II tengan lugar en entornos seguros en consonancia con estándares firmes y ampliamente reconocidos del sector".

Por lo tanto, es indudable que el proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas, pero en ningún caso impedir que puedan producirse.

Así, contradice cualquier lógica jurídica trasladar toda la responsabilidad a la entidad que presta servicios de telefonía, tratándose del mero canal de comunicación seleccionado por la propia entidad financiera y sin que a esta le conste, en modo alguno, que los datos transmitidos a través de los mensajes remitidos contengan claves de operaciones bancarias.

Destacar que Orange no ofrece servicios de confianza online a operadores bancarios, ni tampoco ofrece servicios propios de una entidad de certificación o acreditación. Las

entidades bancarias pueden no haber contratado ningún servicio a Orange, y, aun así, emplear los SMS para llevar a cabo sus actuaciones con clientes. Por ello, no se puede responsabilizar a Orange de la configuración del envío de SMS como segundo factor de autenticación empleado por responsables de otros servicios, como son los operadores bancarios.

En consecuencia, se reitera por esta parte que la responsabilidad de las operadoras de telefonía por los supuestos de suplantación de identidad para la solicitud de copias de tarjetas SIM no puede abarcar aquella derivada de las operaciones bancarias que los delincuentes puedan realizar como consecuencia de que las medidas de seguridad implementadas por las entidades bancarias sean inadecuadas.

Orange no puede hacerse cargo de la seguridad de la operativa de terceras entidades por el mero hecho de que usen servicios de telecomunicaciones. En consecuencia, el razonamiento seguido para responsabilizar a Orange en calidad de operadora por el fraude a la entidad bancaria no es jurídicamente aceptable.

Con esta exposición, enfocada exclusivamente en el resultado, la Agencia deduce directamente que Orange ha llevado a cabo una conducta negligente, sin considerar, en modo alguno, las medidas desplegadas por esta parte.

Por tanto, a juicio de la Agencia, la superación de las medidas de seguridad de Orange por un tercero, con independencia de su contenido, conlleva automáticamente la consideración de su actuación como negligente. Este razonamiento jurídico supone una palmaria materialización de la responsabilidad objetiva en el ámbito sancionador, la cuál no resulta admisible en nuestro ordenamiento jurídico. A este respecto, la Sentencia del Tribunal Supremo 543/2022, de 15 de febrero del año 2022, establece, en su Fundamento Jurídico Tercero, y sienta jurisprudencia; que: "La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento". Así, el Tribunal Supremo configura dicha obligación como una de medios, en las que (Fundamento Jurídico Tercero): "el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".

Por tanto, además de lo expuesto y tal como ha quedado acreditado, la entidad cuenta con un protocolo adecuado para la correcta tramitación de las solicitudes (cuya efectividad en la prevención del fraude es muy elevada, superando el 99%).

Conviene recordar, así mismo, que es el Tribunal Constitucional (en lo sucesivo, TC), el que, desde su Sentencia nº 76/1990, de 26 de abril, ha venido advirtiendo del problema de la inadmisibilidad en nuestro ordenamiento jurídico de la responsabilidad objetiva y, consecuente con ello, la exigencia en todo caso de que la Administración, a la hora de sancionar, pruebe algún grado de intencionalidad en el sancionado. En este sentido cabe mencionar asimismo lo expuesto por la Audiencia Nacional, entre otras,

en su Sentencia de la Sala de lo Contenciosoadministrativo, Sección 1ª, de 23 de Diciembre de 2013, Rec. 341/2012: "Efectivamente, en materia sancionadora rige el principio de culpabilidad (SSTC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa. Como dice la sentencia del Tribunal Supremo de 23 de enero de 1998 , "...puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril, al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho.

La cuestión, pues, ha de resolverse conforme a los principios propios del derecho punitivo dado que el mero error humano no puede dar lugar, por sí mismo (y sobre todo cuando se produce con carácter aislado), a la atribución de consecuencias sancionadoras; pues, de hacerse así, se incurriría en un sistema de responsabilidad objetiva vedado por nuestro orden constitucional.

En el presente supuesto, se evidencia la existencia de un estricto control, previo y posterior a la contratación, el establecimiento de medidas previas y a posteriori, así como la existencia de medidas concretas encaminadas a evitar de forma previa estas prácticas (ya indicadas por esta parte en las alegaciones al requerimiento de información de la AEPD).

Es por ello que no resulta posible apreciar culpabilidad de Orange en el presente supuesto de hecho, no siendo jurídicamente válida la apreciación que realiza la Agencia de comisión de infracción por esta mercantil.

Es decir, se reconoce la existencia de los protocolos de ORANGE y la introducción de mejoras y nuevas medidas para incrementar su efectividad, así como la diligencia de ORANGE en la minimización del impacto y la implementación de los protocolos, no obstante, en la fundamentación, la AEPD califica los mismos como no adecuados, en tanto "son susceptibles de mejora".

De nuevo, como ya se ha manifestado en numerosas ocasiones, tanto en la contestación al requerimiento como en las alegaciones en relación con el Acuerdo de Inicio de Procedimiento Sancionador, esta mercantil ha adaptado las medidas de seguridad de forma complementaria a la evolución de las técnicas de ingeniería social utilizadas por los ciberdelincuentes.

Por tanto, queda acreditada la implicación y la proactividad de esta parte en la protección de los derechos de los particulares, así como el empleo de un nivel de diligencia adecuado por parte de Orange con el que, si bien no resulta posible, por limitación de la tecnología y los medios humanos, la existencia de un riesgo cero, es actualizado y revisado periódicamente en conforme el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Para mayor énfasis, el procedimiento establecido y aplicado por Orange, que la Agencia no ha evaluado, remite al cliente un aviso de forma simultánea a la realización del trámite y gestión del duplicado, de forma que necesariamente se utiliza el email del titular de la línea, pero además, por seguridad, se informa al titular de la línea telefónica de forma directa. De hecho, es dicha medida implantada por Orange, como ya se ha señalado, la que habilita al Reclamante a identificar que ha sido víctima de un fraude 'phising'.

Así, el procedimiento de Orange incorpora medidas de seguridad adicionales (que han demostrado en el presente caso ser eficaces), en cumplimiento de los criterios estipulados por la Audiencia Nacional como acreditativos del despliegue de diligencia suficiente en la solicitud de duplicados de tarjetas SIM.

Orange ha demostrado, a través, tanto de las alegaciones presentadas como en la documentación anterior puesta a disposición de esta Agencia, que ha actuado en todo momento con la diligencia debida en la identificación del Reclamante, no teniendo lugar tratamiento de datos alguno sin legitimación.

No obstante lo anterior, en el hipotético caso de que la Agencia considerase que existe algún tipo de incumplimiento, la sanción incluida en el Acuerdo de Inicio resulta, en todo caso, desproporcionada, atendiendo a las circunstancias y contenido de la supuesta infracción, que Orange niega rotundamente.

En este sentido, cabe destacar los siguientes puntos que conforme a la interpretación de la Agencia son calificados de agravantes, sin que concurran las circunstancias para su consideración en relación con los hechos analizados:

• *Toda infracción anterior cometida por el responsable o encargado del tratamiento (artículo 83.2e) del RGPD.*

Esta parte ha indicado tanto en el presente escrito como en los anteriores remitidos a esta Agencia, las particularidades del supuesto que nos ocupa, así como la innovación de las técnicas y medios empleados por los suplantadores de identidad para ejecutar las tentativas de comisión de fraude.

Dicho en términos de análisis de riesgos, no cabe exigir la existencia de medidas

• 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).

El tratamiento de los datos personales por parte de Orange es estrictamente necesario para poder desempeñar las actividades que le caracterizan como operadora. Por tanto, imponer el agravante descrito teniendo en cuenta que no existe una relación directa con la supuesta infracción, no concuerda con lo expuesto en el artículo 83.2.k) ya que este exige que el agravante que nos ocupa se aplique teniendo en cuenta el caso concreto.

Así pues, en ningún caso ha formado parte de la voluntad de Orange que ocurriera la situación en la que se ha visto envuelto el Reclamante y es necesario reiterar que esta

operadora también se ha visto perjudicada por la misma. Por ende, no es posible considerar la aplicación de este agravante. Adicionalmente, tal y como se ha expuesto con anterioridad en las presentes alegaciones, quisiera señalar esta parte que el perjuicio al que hace alusión el Reclamante, consistente en la sustracción de fondos de sus cuentas bancarias, no se encuentra incluido en la actividad de esta mercantil.

Como ya se ha señalado en el presente escrito, las entidades bancarias son las únicas responsables de la seguridad de sus operaciones (EBA, Opinion on the implementation of the RTS on SCA and CSC y Qualification of SMS OTP as an authentication factor).

Como adición a lo expuesto, y según lo establecido en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, además de la atenuante ya reconocida expresamente por la AEPD en su Acuerdo de Inicio.

• Procedió la parte reclamada a bloquear la línea en cuanto tuvo conocimiento de los hechos (art. 83.2 c).

Concurren en el presente las siguientes circunstancias atenuantes que no han sido consideradas en la adecuada graduación de la sanción:

• En ningún momento se han tratado categorías especiales de datos.

• El grado de cooperación de Orange con la AEPD con el fin de poner remedio a una supuesta infracción y mitigar sus posibles efectos adversos: ha quedado acreditado que se ha contestado en tiempo y forma a todos los requerimientos de información solicitados por esta Agencia, en línea con la práctica habitual de esta mercantil de total colaboración con la autoridad de protección de datos.

En los escritos remitidos a la AEPD se han reseñado detalladamente las medidas implementadas a propósito de la circunstancia en la que se ha visto envuelto el Reclamante, poniendo remedio, por tanto, a la supuesta infracción, mitigando, asimismo, sus efectos.

• El inexistente beneficio obtenido por parte de Orange derivado del tratamiento de datos que ocupa este procedimiento.

En todo caso, Orange se ha visto perjudicada, como ya se ha señalado, siendo parte perjudicada incluso en el procedimiento judicial en el que se denuncia la comisión del delito que nos ocupa.

Pese a que la AEPD en su Propuesta indica que este no puede considerarse un atenuante, Orange no se ha visto beneficiada en ningún caso, sino que ha sido, asimismo, víctima de las actuaciones de ciberdelincuentes, al igual que el Reclamante.

SOLICITA a la Agencia Española de Protección de Datos que tenga por presentado el presente escrito, sirva admitirlo, tenga por formuladas las anteriores alegaciones y, previos los trámites oportunos, dicte resolución por medio de la cuál señale el archivo del EXP2022101101. Subsidiariamente, en el caso de que la AEPD resuelva en contra

de la fundamentación jurídica que sostiene ORANGE, se solicita a la AEPD que tenga en cuenta las circunstancias atenuantes fundamentadas en las anteriores alegaciones y, consecuentemente, culmine el procedimiento mediante un apercibimiento y, en última instancia, si considera que procede la imposición de una sanción, modere o module su propuesta recogida en la Propuesta de Sanción notificado a ORANGE, atendiendo a los argumentos manifestados en el cuerpo del presente escrito de alegaciones>>.

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

HECHOS PROBADOS

PRIMERO: La parte reclamante formula reclamación el día 15 de agosto de 2022, manifestando que su teléfono móvil dejó de funcionar el día 1 de agosto de 2022 y que recibió varios correos electrónicos relativos a un aviso de consumo y otro correo electrónico indicando que se había activado con éxito su tarjeta eSIM.

SEGUNDO: Obra en el expediente que la vía de solicitud de la tarjeta eSIM fue a través del Área Privada del reclamante de internet, accedieron con el usuario y clave del reclamante el día 1 de agosto de 2022, y solicitaron la generación de una tarjeta e-SIM y Orange procedió a emitir el duplicado de tarjeta en la modalidad e-SIM.

TERCERO: Obra en el expediente que Orange procedió a enviar un correo electrónico al reclamante con el aviso de la solicitud de la tarjeta e-SIM dentro de los contactos registrados con el cliente o su supuesto suplantador, varios de fecha 1 de agosto de 2022 que reflejan que a las 19:03 se produjo un cambio de la dirección de correo electrónico del reclamante, efectuado desde el Área de Cliente y a las 20:07 el envío de un SMS informando de que puede escanear el código de activación del eSIM.

CUARTO: Obra en el expediente que el reclamante, tras recibir el SMS de Orange, contacta con la parte reclamada para solicitar la anulación del duplicado de tarjeta eSIM, indicando que no lo ha realizado.

QUINTO: Consta que con fecha 3 de agosto de 2022 se bloqueó la numeración de la línea telefónica por robo/pérdida.

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

Alegaciones

En respuesta a las alegaciones presentadas por la entidad reclamada se debe señalar lo siguiente:

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

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

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.

Dentro del proceso de emisión de eSIM no se necesita una tarjeta física, sino que para la activación de la misma se requiere que el solicitante escanee un código QR que se remite vía electrónica (SMS o correo electrónico).

En el presente caso, resulta acreditado que Orange facilitó un duplicado de la tarjeta eSIM de la parte reclamante a un tercero, sin su consentimiento, el cual, accedió a la 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 tomó las cautelas necesarias para que estos hechos no se produjeran.

Pues bien, resulta acreditado que un tercero accedió al área privada web de Cliente del Reclamante, y procedió al cambio de su dirección de correo electrónico e iniciando

posteriormente una conversación con el Canal digital asistido y solicitando a través de este medio el duplicado de eSIM.

Hay que tener en cuenta, sin perjuicio de lo indicado anteriormente, que cuando se produjo la activación de la eSIM objeto de reclamación, el reclamante recibió un aviso de la parte reclamada, y se quedó sin línea, por lo que se puso en contacto telefónico manifestando no haber solicitado el eSIM.

Es importante resaltar, que aun cuando la parte reclamante avisó de que no había realizado ese trámite. Orange no bloqueó el teléfono permitiendo así que se produjera la suplantación por la demora por parte de Orange en llevar a cabo el bloqueo de la numeración. Dos días después se bloqueó la numeración, y tres días después le facilitaron un nuevo SIM físico.

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

De los Hechos Probados, se deduce que ORANGE ha facilitado duplicado de tarjeta eSIM a un tercero distinto del legítimo titular de la línea móvil, tras la superación por tercera persona de la política de seguridad existente, lo que evidencia un incumplimiento del deber de proteger la información de los clientes.

Este acceso no autorizado a los datos personales del afectado resulta determinante para las actuaciones posteriores desarrolladas por las personas suplantadoras, ya que aprovechan el espacio de tiempo que trascurre desde el 1 de agosto de 2022 fecha en que el usuario detecta el fallo en la línea y se pone en contacto con la operadora, hasta el día 3 de agosto de 2022 en que Orange bloqueó la línea para realizar operaciones bancarias fraudulentas, que sin el duplicado de la tarjeta eSIM hubiera devenido imposible su realización.

Negar la concurrencia de una actuación negligente por parte de ORANGE equivaldría a reconocer que su conducta -por acción u omisión- ha sido diligente. Obviamente, no compartimos esta perspectiva de los hechos, puesto que ha quedado acreditada la falta de diligencia debida. Resulta muy ilustrativa, la SAN de 17 de octubre de 2007 (rec. 63/2006), partiendo de que se trata de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica que "…*el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*

Así en este sentido la sentencia de la Audiencia Nacional San de 19 de septiembre de 2023 (rec 403/2021), indica que *"… 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) en definitiva al no haberse actuado con la necesaria diligencia, se trataron los datos del denunciante sin contar con su consentimiento".

Resulta acreditado en el expediente que no se ha garantizado una seguridad adecuada en el tratamiento de los datos personales, habida cuenta del resultado que ha producido la suplantación de identidad. Es decir, un tercero ha conseguido acceder a los datos personales del titular de la línea sin que las medidas de seguridad que afirma ORANGE que existen, hayan podido impedirlo. Así pues, estamos ante la concurrencia de una conducta típica, antijuridica y culpable.

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

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

En el presente procedimiento sancionador, la sanción se impone debido a que ORANGE facilitó un duplicado de la tarjeta eSIM de la parte reclamante a un tercero, sin su consentimiento y sin verificar la identidad de dicho tercero, y por este motivo se imputa el artículo 6.1 del RGPD.

En el supuesto ahora examinado, la AEPD, tras la realización de las investigaciones oportunas, y en relación con una serie de hechos concretos que considera probados, incardina los mismos en el tipo infractor que considera adecuado, conforme a la aplicación e interpretación de la normativa, motivando de manera prolija y suficiente tal actuación. Y es que, la AEPD se encuentra vinculada por el principio de legalidad que implica la aplicación e interpretación de las normas atendiendo al supuesto de hecho específico que concurra en cada caso.

En cuanto a la responsabilidad de ORANGE, debe indicarse que, con carácter general ORANGE 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 recibir el duplicado de la tarjeta eSIM. 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 ORANGE 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.*

El sistema informático y las tecnologías intervinientes deberán ser las adecuadas para evitar la suplantación de identidad y estar correctamente configurados.

No comparte esta Agencia las afirmaciones de ORANGE en cuanto a las circunstancias que han quedado acreditadas.

Es cierto que existen protocolos para prevenir las suplantaciones de identidad en estos procesos; que se han trasladado a los implicados en la tramitación; que se han introducido mejoras tras conocer ciertas vulnerabilidades; que existen penalizaciones por su incumplimiento. Sin embargo, no compartimos el hecho de que esos protocolos o procedimientos internos puedan considerarse como adecuados en tanto que son susceptibles de mejora. Hay que reforzar los mecanismos de identificación y autenticación con medidas técnicas y organizativas que resulten especialmente apropiadas para evitar suplantaciones.

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

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

No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo que en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas.

Según la STC 246/1991 " (...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos.

Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma" (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, Rec 1067/2006, que *"aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su*

inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa".

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

En el presente caso, resulta acreditado que Orange facilitó un duplicado de la tarjeta eSIM de la parte reclamante a un tercero, 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 eSIM, no tomó las cautelas necesarias para que estos hechos no se produjeran.

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

Pues bien, resulta acreditado tal como reconoce la parte reclamada en su escrito de contestación a esta Agencia, y en las alegaciones presentadas *<<, el usurpador accedió al área privada web de Cliente (en adelante, APC) del Reclamante, iniciando posteriormente una conversación con el Canal digital asistido y solicitando a través de este medio el duplicado de eSIM. Habiéndose, pues, constatado la irregularidad en la solicitud del duplicado, el equipo de Análisis de Riesgos confirmó que el Reclamante, titular de la línea* ******TELEFONO.1****, ha sido, probablemente, víctima de phishing, smishing o algún otro instrumento de ingeniería social (el cual no ha podido ser identificado por esta mercantil en el curso de las investigaciones) a través de su APC desde donde se solicitó el duplicado e-SIM sin haberse solicitado un reseteo de las contraseñas, es decir, el malhechor ya la conocía previamente>>.*

De conformidad con las evidencias de las que se dispone en este momento procesal, se estima que la conducta de la parte reclamada vulnera el artículo 6,1 del RGPD pudiendo ser constitutiva de la infracción tipificada en el artículo 83.5.a) del citado Reglamento 2016/679.

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."*

III

Obligación Incumplida

El artículo 4 del RGPD, bajo la rúbrica “Definiciones”, dispone lo siguiente:

“1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”

ORANGE, es la responsable de los tratamientos de datos referidos en los antecedentes expuestos, toda vez que conforme a la definición del artículo 4.7 del RGPD es la que determina la finalidad y medios de los tratamientos realizados con las finalidades señaladas en su Política de Privacidad.

Asimismo, la emisión de un duplicado eSIM 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).

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".

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:

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

La LOPDGDD, 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

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.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679."

De acuerdo con los preceptos transcritos a efectos de fijar el importe de la sanción de multa a imponer a la entidad reclamada como responsable de una infracción tipificada en el artículo 83.5.a) del RGPD y 72.1 b) de la LOPDGDD, se estiman concurrentes en el presente caso los siguientes factores:

En calidad de circunstancias agravantes:

- La circunstancia del artículo 83.2.e) RGPD: "*Toda infracción anterior cometida por el responsable o el encargado del tratamiento".*

El considerando 148 del RGPD señala "*A fin de reforzar la aplicación de las normas del presente Reglamento [...]"* e indica a ese respecto que *"Debe no obstante, prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional [...] o a cualquier infracción pertinente [...]*".

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 RGPD:

i.EXP202204288 Resolución dictada el 31 de enero de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.

ii.EXP202203638. Resolución dictada el 30 de enero de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.

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

La Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), en la que, respecto de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica que *"…el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto."*

En calidad de circunstancias atenuantes:

Orange solicita que se aprecien las siguientes circunstancias atenuantes:

En ningún momento se han tratado categorías especiales de datos. El grado de cooperación de Orange con la AEPD con el fin de poner remedio a una supuesta infracción y mitigar sus posibles efectos adversos. El inexistente beneficio obtenido por parte de Orange derivado del tratamiento de datos que ocupa este procedimiento.

No se admite ninguna de las circunstancias invocadas.
Respecto a que no se han tratado categorías especiales de datos art. 83.2.g RGPD, sería una circunstancia agravante, por lo que no es encuadrable en esa circunstancia atenuante.

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, sino 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 *"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 las 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".*

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 solo puede operar como agravante y en ningún caso como circunstancia atenuante.

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 Orange 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 ORANGE 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”:

- 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 ORANGE ESPAGNE, S.A.U., con NIF A82009812, 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 ORANGE ESPAGNE, S.A.U.

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