- **Expediente nº.: EXP202210101**

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por ORANGE ESPAGNE, S.A.U. (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 23 de enero de 2024, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 23 de enero de 2024, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202210101, en virtud de la cual se imponía a ORANGE ESPAGNE, S.A.U., 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).

Dicha resolución, que fue notificada a la parte recurrente en fecha 25 de enero de 2024, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00307/2023, quedó constancia de los siguientes:

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.

TERCERO: La parte recurrente ha presentado en fecha 26 de febrero de 2024, en esta Agencia Española de Protección de Datos, recurso de reposición.

Como fundamento del recurso la recurrente reitera los argumentos expuestos a lo largo del procedimiento, en síntesis manifiesta que en el presente procedimiento, no se ha acreditado de forma alguna que el tercero haya tenido acceso a los datos bancarios, ni tampoco a otros datos personales asociados al terminal.

Añade, pese a que Orange establezca medidas de seguridad y las someta a revisión y mejora continua, es imprescindible que los particulares, como titulares de sus datos personales, tengan cierta diligencia a la hora de custodiarlos, sin ponerlos a disposición de terceros o descuidarlos, permitiendo a terceros hacerse con su información personal, de modo que faciliten su suplantación.

Por otra parte, alega que Orange no participa del proceso de identificación de un usuario ante su banco, sino que es éste quien determina el modo en que quiere llevar a cabo esta comprobación, por lo que no cabe trasladar la responsabilidad ante las operadoras de telefonía.

Sobre la inadmisibilidad de la responsabilidad objetiva, señala que la AEPD limita su argumentación al resultado y solicita que se dicte resolución por medio de la cual señale el archivo del procedimiento. Subsidiariamente, culmine el procedimiento mediante un apercibimiento y, en última instancia, se modere o module la sanción.

FUNDAMENTOS DE DERECHO

I
Competencia

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

II
Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho II al V, de la Resolución recurrida, tal como se transcribe a continuación:

<<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 ******TELÉFONO.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>>.

III
Conclusión

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ORANGE ESPAGNE, S.A.U. contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 23 de enero de 2024, en el expediente EXP202210101.

SEGUNDO: NOTIFICAR la presente resolución a ORANGE ESPAGNE, S.A.U..

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea notificada la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 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 en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Si la fecha de la notificación 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 Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer 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) 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 LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-21112023

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