- **Expediente nº.: EXP202301160**

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por VODAFONE ESPAÑA, 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 8 de mayo de 2024, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 8 de mayo de 2024, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202301160, en virtud de la cual se impone a VODAFONE ESPAÑA, S.A.U. con NIF A80907397, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de por un importe de 200.000 euros (doscientos mil euros).

Dicha resolución, que fue notificada a la parte recurrente en fecha 14 de mayo 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/00425/2023, quedó constancia de los siguientes:

"PRIMERO. - Obra en el expediente, que con fecha 1 de diciembre de 2022 se solicitó por un tercero a través del acceso al área privada de la reclamante a Lowi marca de Vodafone un duplicado de su tarjeta SIM y se facilitó por la tercera persona para realizar la entrega del pedido del duplicado de la tarjeta SIM un domicilio distinto del que figuraba en el registro de Vodafone para la facturación de la reclamante.

SEGUNDO. - Obra en el expediente, que el duplicado SIM es entregado el día 2 de diciembre de 2022 en la dirección postal facilitada por el tercero.

TERCERO. - Vodafone, reconoce en su escrito de fecha 16 de marzo de 2023 que ha podido comprobar que no dispone de la evidencia que permita confirmar el paso de la política de seguridad, y tampoco de la evidencia que permita confirmar el paso de la política de seguridad completa llamando al 121, para la activación de la tarjeta SIM, manifestando que no dispone de la grabación del trámite telefónico referido en tanto que no se produjo la grabación de dicha llamada.

CUARTO. – Obra en el expediente que anteriormente en fecha 30 de noviembre de 2022, se produjeron dos intentos de cambio de la dirección de correo electrónico por vía telefónica, supuestamente para poder acceder al área privada de cliente de la

reclamante, dicha petición no fue llevada a cabo al no superar la Política de Seguridad".

TERCERO: La parte recurrente ha presentado en fecha 14 de junio de 2024, en esta Agencia Española de Protección de Datos, recurso de reposición, en el que muestra su disconformidad con la resolución, reiterando los argumentos expuestos en sus alegaciones, fundamentándolo básicamente en los siguientes motivos:

1) Vodafone ha actuado de forma diligente en la medida en la que tiene implementados los procesos necesarios para identificar correctamente a sus clientes, siendo la adopción de medidas técnicas y organizativas una obligación que no es absoluta.

2) Para la entrega de un duplicado SIM, Vodafone tiene contratado un servicio de entrega exclusiva con la empresa de transportes colaboradora con esta entidad.

3) La realización de un duplicado SIM no conlleva el acceso a información bancaria, contraseñas, dirección de correo electrónico, etc., de los clientes de Vodafone, sino a los servicios de móvil e internet que pudieran tener contratados los clientes de mi representada.

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

5) Subsidiariamente, y para el caso de que la Agencia entienda que ha existido infracción y deba imponerse una sanción a Vodafone, deberá graduarse bajo el principio de proporcionalidad, así como tenerse en cuenta las circunstancias agravantes y atenuantes mencionadas.

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 LPACAP y el artículo 48.1 de la 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, III, IV y V de la Resolución recurrida, tal como se transcribe a continuación:

<<II

Contestación a las alegaciones presentadas

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

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

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

En tanto que estas entidades son responsables del tratamiento de los datos de sus clientes, les competen idénticas obligaciones que las señaladas hasta ahora para las operadoras referidas al cumplimiento del RGPD y la LOPDGDD, y además las derivadas del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

A este respecto, conviene aclarar que, dentro del terminal móvil, va insertada la tarjeta SIM. Es una tarjeta inteligente, en formato físico y de reducidas dimensiones, que contiene un chip en el que se almacena la clave de servicio del suscriptor o abonado usada para identificarse ante la red, esto es, el número de línea telefónica móvil del cliente MSISDN (Mobile Station Integrated Services Digital Network -Estación Móvil de la Red Digital de Servicios Integrados-), así como el número de identificación personal del abonado IMSI (International Mobile Subscriber Identity -Identidad Internacional del Abonado móvil-) pero también puede proporcionar otro tipo de datos como la información sobre el listado telefónico o el de llamadas y mensajes.

Por otro lado, la emisión de un duplicado de tarjeta SIM supone el tratamiento de los datos personales de su titular ya que se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador (artículo 4.1) del RGPD).

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

En suma, tanto los datos que se tratan para emitir un duplicado de tarjeta SIM como la tarjeta SIM (Subscriber Identity Module) que identifica de forma inequívoca y unívoca

al abonado en la red, son datos de carácter personal, debiendo su tratamiento estar sujeto a la normativa de protección de datos.

En cuanto a la responsabilidad de Vodafone, debe indicarse que, con carácter general Vodafone trata los datos de sus clientes al amparo de lo previsto en el artículo 6.1 b) del RGPD, por considerarse un tratamiento necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. En otros casos, fundamenta la licitud del tratamiento en las bases previstas en el artículo 6.1.a), c), e) y f) del RGPD.

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

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.

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

En cuanto a la conducta de Vodafone se considera que responde al título de culpa. Como depositaria de datos de carácter personal a gran escala, por lo tanto, habituada o dedicada específicamente a la gestión de los datos de carácter personal de los clientes, debe ser especialmente diligente y cuidadosa en su tratamiento. Es decir, desde la óptica de la culpabilidad, estamos ante un error vencible ya que, con la aplicación de las medidas técnicas y organizativas adecuadas, estas suplantaciones de identidad se hubieran podido evitar.

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

ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

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

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

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

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

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

A propósito de la culpabilidad de la persona jurídica procede citar la STC 246/1991, 19 de diciembre de 1991 (F.J. 2), conforme a la cual, respecto a las personas jurídicas, el elemento subjetivo de la culpa se ha de aplicar necesariamente de forma distinta a como se hace respecto de las personas físicas y añade que "Esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos. Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz [...]".

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

En cumplimiento del principio de culpabilidad la AEPD ha acordado en numerosas ocasiones el archivo de procedimientos sancionadores en los que no concurría el elemento de la culpabilidad del sujeto infractor. Supuestos en los que, pese a existir un comportamiento antijurídico, había quedado acreditado que el responsable había obrado con toda la diligencia que resultaba exigible, por lo que no se apreciaba culpa alguna en su conducta. Ese ha sido el criterio mantenido por la Sala de lo Contencioso

Administrativo, sección 1ª, de la Audiencia Nacional. Pueden citarse, por ser muy esclarecedoras, las siguientes sentencias:

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

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

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

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

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

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

"Responsabilidad del responsable del tratamiento"
"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas

técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.
2.Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.
3.La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento."

El artículo 25 del RGPD, "Protección de datos desde el diseño y por defecto", establece:
"1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
2.[...]".

Es plenamente aplicable al caso la SAN de 17 de octubre de 2007 (rec. 63/2006), que, después de referirse a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, dice: "[...] el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto.

III
Obligación incumplida

Se imputa a la parte reclamada la comisión de una infracción por vulneración del artículo 6 del RGPD, "Licitud del tratamiento", que señala en su apartado 1 los supuestos en los que el tratamiento de datos de terceros es considerado lícito:
"1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

En el presente caso, resulta acreditado en primer lugar que la solicitud del duplicado de la tarjeta SIM, se hizo a través del área privada de la parte reclamante y se indicó en dicha petición que se enviara la tarjeta SIM a un domicilio postal distinto al de la facturación.

Además, la parte reclamada no dispone de la evidencia que permita confirmar el paso de la política de seguridad completa llamando al 121, para la activación de la tarjeta sim una vez entregada a la tercera persona, manifestando que no disponen de la grabación del trámite telefónico referido en tanto que no se produjo la grabación de dicha llamada, ni aportan copia del contacto donde se refleje el paso de la política de seguridad.

De esta forma, la parte reclamada facilitó duplicado de la tarjeta SIM de la línea de la reclamante, sin su consentimiento y sin verificar la identidad de dicho tercero, el cual, ha accedido a información contenida en el teléfono móvil. Así pues, la reclamada, no verificó la personalidad del que solicitó el duplicado de la tarjeta SIM, no verificó la personalidad de quien estaba activando tal duplicado de la tarjeta sim, esto es, no tomó las cautelas necesarias para que estos hechos no se produjeran.
Hay que destacar, que tal como reconoce Vodafone en su escrito de fecha 16 de marzo de 2023: <<Vodafone ha podido comprobar que se efectuaron distintas acciones presuntamente fraudulentas sobre la línea de telefonía móvil perteneciente a la reclamante. Previo a la incidencia objeto de la reclamación, en fecha 30 de noviembre de 2022, se produjeron dos intentos de cambio de la dirección de correo electrónico por vía telefónica, supuestamente para poder acceder al área privada de cliente.

Sin embargo, dicha petición no fue llevada a cabo al no superar la Política de Seguridad, en la medida en que los dígitos de la cuenta bancaria facilitados por la reclamante en aplicación de la Política de Seguridad no coincidían con la numeración obrante en los sistemas internos. Pese a lo cual, y a pesar de no haberse obtenido el cambio de dirección de correo electrónico que facultaría a la persona llamante a lograr el acceso al área privada de cliente, se tramitó de forma online una petición de duplicado de SIM, en fecha 1 de diciembre de 2022, a través del área privada de cliente>>. Sin embargo, Vodafone no tomo las cautelas necesarias para que estos hechos no se produjeran.
En este sentido, la SAN, de fecha 19 de septiembre de 2023 (REC 403/2021), que dice: "contrató 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 de la persona contratante (por lo que hubiera sido bastante atender a la incorrecta contestación de las preguntas de identificación y verificación del cliente) se hubiera evitado la infracción del artículo 6.1 de la LOPD imputada por la AEP"

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

En todo caso, no se siguió el procedimiento implantado por la parte reclamada, ya que, de haberlo hecho, se debió haber producido la denegación del mismo.
A la vista de lo anterior, Vodafone no logra acreditar que se haya seguido ese procedimiento y por consiguiente hubo un tratamiento ilícito de los datos personales de la parte reclamante, contraviniendo con ello el artículo 6 del RGPD.

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."

IV
Tipificación y calificación de la infracción

La infracción se tipifica en el artículo 83.5 del RGPD, que considera como tal:
"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

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

V
Sanción de multa: Determinación del importe

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

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

“2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.”

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

“1. Las sanciones previstas en los apartados 4,5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

“2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.”

Vodafone solicita que se aprecien las siguientes circunstancias atenuantes:

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

- *El grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción.*

- *Cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.*

No se admite ninguna de las circunstancias invocadas.

El Artículo 83.2.d) RGPD: “El grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;”.

La reclamada se ha limitado a declarar que el tercero que contrató con ella superó la política de seguridad de la compañía sin aportar ninguna prueba que demuestre que recabó de la persona que intervino en la contratación algún documento que acreditara

que era efectivamente el titular de los datos personales que había facilitado como propios o que articuló algún mecanismo que permitiera contrastar la veracidad de los datos de identidad proporcionados.

Por otra parte, el principio de proactividad supone transferir al responsable del tratamiento la obligación no solo de cumplir con la normativa, también la de poder demostrar su cumplimiento. Entre los mecanismos que el RGPD contempla para lograrlo se encuentran los previstos en el artículo 25, "protección de datos desde el diseño", a tenor del cual el responsable debe aplicar "tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento" medidas técnicas y organizativas que garanticen que hace una efectiva aplicación de los principios del RGPD con ocasión de los tratamientos que realiza.

El artículo 83.2.f) del RGPD se refiere al "grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;".

La respuesta de la reclamada al requerimiento informativo de la Subdirección de Inspección no cumplía esas finalidades, por lo que no es encuadrable en esa circunstancia atenuante.

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 Vodafone alega.

Además, conforme al artículo 83.1 del RGPD la imposición de las sanciones de multa está presidida por los siguientes principios: deberán estar individualizadas para cada caso particular, ser efectivas, proporcionadas y disuasorias. La admisión de que opere como una atenuante la ausencia de beneficios es contraria al espíritu del artículo 83.1 del RGPD y a los principios por los que se rige la determinación del importe de la sanción de multa. Si a raíz de la comisión de una infracción del RGPD se califica como atenuante que no han existido beneficios, se anula en parte la finalidad disuasoria que se cumple a través de la sanción. Aceptar la tesis de Vodafone en un supuesto como el que nos ocupa supondría introducir una rebaja artificial en la sanción que verdaderamente procede imponerse; la que resulta de considerar las circunstancias del artículo 83.2 RGPD que sí deben de ser valoradas.

La Sala de lo Contencioso Administrativo de la Audiencia Nacional ha advertido que, el hecho de que en un supuesto concreto no estén presentes todos los elementos que integran una circunstancia modificativa de la responsabilidad que, por su naturaleza,

tiene carácter agravante, no puede llevar a concluir que tal circunstancia es aplicable en calidad de atenuante. El pronunciamiento que hace la Audiencia Nacional en su SAN de 5 de mayo de 2021 (Rec. 1437/2020) -por más que esa resolución verse sobre la circunstancia del apartado e) del artículo 83.2. del RGPD, la comisión de infracciones anteriores- es extrapolable a la cuestión planteada, la pretensión de la reclamada de que se acepte como atenuante la "ausencia" de beneficios siendo así que tanto el RGPD como la LOPDGDD se refieren solo a "los beneficios obtenidos".

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

- *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 que "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 […] o a cualquier infracción anterior 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 del RGPD:

i.EXP202204287 Resolución dictada el 24 de octubre de 2022 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación. Vodafone se acogió a una de las dos reducciones previstas.

ii.EXP202203916. Resolución dictada el 24 de octubre de 2022 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación. Vodafone se acogió a una de las dos reducciones previstas.

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

La reclamada argumenta que los anteriores procedimientos sancionadores, son relativos a clientes de Vodafone que no son clientes de la marca Lowi y cuyos duplicados SIM se tramitaron por canales diferentes al del caso aquí analizado, y por lo tanto no deben de ser aplicados como agravante.

Queda acreditado que Lowi es una marca bajo la misma denominación legal que Vodafone, son la misma empresa y por lo tanto 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.

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

La Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), en la que, respecto de entidades cuya actividad lleva aparejado en continuo tratamiento de datos de clientes, indica que "…el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto."
Procede graduar la sanción a imponer a la reclamada y fijarla en la cuantía de 200.000 € por la por la presunta infracción del artículo 6.1) tipificada en el artículo 83.5.a) del citado RGPD".

En definitiva, en el caso analizado, queda en entredicho la diligencia empleada por parte de la reclamada para identificar a la persona que solicitó el duplicado de la tarjeta SIM, dado que hubo dos intentos de cambio de la dirección de correo electrónico por vía telefónica y el suplantador no superó la política de seguridad y a pesar de ello Vodafone no tomó las medidas necesarias para que estos hechos no ocurrieran.

Por lo tanto, cabe apreciar falta de diligencia en la actuación de Vodafone, sin que quepa apreciar falta de culpabilidad.

La AEPD no se descuelga de ningún razonamiento ni tampoco achaca toda la responsabilidad a Vodafone. Le reprocha la responsabilidad que le corresponde como responsable de ese tratamiento específico "Emisión de un duplicado de tarjeta SIM", toda vez que conforme a la definición del artículo 4.7 del RGPD es quien determina la finalidad y medios del tratamiento realizado.

Vodafone en su condición de operador deber ser más exigente a la hora de proporcionar un duplicado de una tarjeta SIM. Las verificaciones de identidad deben ser exhaustivas para evitar problemas de suplantación de identidad.

En el momento en el que se logra la tarjeta SIM duplicada se tiene también acceso al segundo factor de autenticación y, por tanto, desde ese instante, se podrían materializar fraudes bancarios.

Por tanto, analizadas las alegaciones efectuadas en el presente recurso potestativo de reposición, se comprueba que no se han aportado en ellas nuevos argumentos jurídicos siendo prácticamente a las indicadas durante el trascurso del procedimiento, y por tanto no permiten reconsiderar el sentido de la resolución sancionadora dictada en fecha 8 de mayo de 2024.

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 VODAFONE ESPAÑA, S.A.U. contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 8 de mayo de 2024, en el expediente EXP202301160.

SEGUNDO: NOTIFICAR la presente resolución a VODAFONE ESPAÑA, 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