- **Expediente N.º: EXP202203638**

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 1 de marzo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra contra ORANGE ESPAGNE, S.A.U. con NIF A82009812 (en adelante, Orange) por los siguientes motivos:

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, el 24 de febrero de 2022, se quedó sin línea en uno de sus dos teléfonos móviles. Tras contactar con su operador de telefonía (entidad reclamada) le indican que se había realizado un duplicado de su tarjeta SIM, solicitud que no hizo el reclamante, por lo que acude a una tienda física y le facilitan los datos relativos a dicho duplicado, siendo la localidad Barcelona, pese a que el reclamante reside en Madrid.

Y, aporta la siguiente documentación relevante:

Copia del DNI del reclamante.

Documento relativo a la solicitud de duplicado de tarjeta SIM. Punto de Venta del establecimiento de ***ESTABLECIMIENTO.1. No figura firma del reclamante.

Denuncia presentada ante la Guardia Civil de la localidad de Arganda del Rey (Madrid), en fecha 25 de febrero 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 7 de abril de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 9 de mayo de 2022 se recibe en esta Agencia escrito de respuesta indicando: <<*que los días 24 y 25 de febrero del presente año, se detectó el duplicado*

*de e-SIM usurpando la identidad del reclamante. Los autores de la usurpación de identidad se pusieron en contacto con un empleado del Punto de Venta del establecimiento de ***ESTABLECIMIENTO.1 accediendo a sus credenciales de cuentas de correo y otros datos para vaciar sus cuentas bancarias y/o Criptomonedas, hecho que ha sido denunciado por parte de esta mercantil a finales de marzo. Esta denuncia amplia otras de casos previos, estando judicializado en caso en las diligencias previas 114/2022 del Juzgado de Primera Instancia e Instrucción núm. 1 de ***LOCALIDAD.1.*

Pues bien, una vez obtenidas las credenciales, fue cuando esta persona solicitó el duplicado de e-SIM expuesto por el reclamante. En el momento en el que el reclamante se dio cuenta de esta circunstancia se puso en contacto con esta mercantil, procediéndose a bloquear la línea, así como a realizar los ajustes pertinentes.

A este respecto, cabe señalar que, en ningún caso se han visto afectados o comprometidos los sistemas de seguridad de la información de la compañía, que no han sufrido brecha en su funcionamiento.

Asimismo, se han actualizado los datos de acceso a sistemas de ese punto de venta, de forma que no puedan volver a ser utilizados por la persona que de mala fe llevó a cabo el duplicado irregular.

Que han puesto en marcha un plan de acción que está previsto a corto plazo, estimando poder lanzarlo a finales (…) de 2022, concretándose en las siguientes medidas:

- *Implantación de un doble factor de identificación.*

- *El proyecto denominado "Whitelist IP">>*

TERCERO: Con fecha 17 de mayo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 23 de septiembre de 2022**,** 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.

QUINTO: Notificado el citado acuerdo de inicio 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), la parte reclamada solicitó ampliación del plazo para formular alegaciones por cinco días hábiles, y con fecha 18 de octubre de 2022 presentó escrito de alegaciones en el que, en síntesis, manifestaba
su disconformidad con el contenido de los fundamentos expuestos en la Acuerdo de Inicio y se ratifica y da por reproducidas las alegaciones y argumentaciones jurídicas

de su anterior escrito, y manifiesta: *"Que los días 24 y 25 de febrero de 2022 se realiza, a través de Siebel 8 (sistema interno de activación de tarjetas de Orange móvil solicitadas desde tiendas), un pedido de duplicado de SIM (en concreto una e-SIM) asociado al Punto de Venta de ***ESTABLECIMIENTO.1. El modo en que es gestionada la solicitud de duplicado de la e-SIM, con las credenciales de uno de los empleados del Punto de Venta de ***ESTABLECIMIENTO.1, pero sin el seguimiento del protocolo habitual (llamada para solicitar autorización), provoca que el departamento de Fraude de Orange identifique y revise el proceso en cuestión.*

Se inicia el procedimiento de verificación de la solicitud y concesión de la e-SIM, con el fin de identificar la existencia de posibles irregularidades. Mientras se llevaba a cabo este proceso de verificación, el reclamante se pone en contacto, en el mismo día, con el departamento de atención al cliente de Orange para informar que ha sido víctima de una suplantación de identidad, lo que sirve para confirmar las sospechas sobre la operación. Seguidamente, el departamento de Fraude procede a categorizar la contratación como irregular y a anular el duplicado de e-SIM. En consecuencia, Orange realiza inmediatamente los ajustes necesarios. Se crea una alerta indicando que el cliente ha sido víctima de usurpación de identidad, y limitando la realización de pedidos, para permitir su control.

*En el posterior análisis del supuesto de hecho por parte del departamento de Análisis de Riesgos de Orange, se concluyó que se había producido un robo de las credenciales de Siebel 8 del Punto de Venta de ***ESTABLECIMIENTO.1 (perteneciente a una tercera entidad, franquiciada de Orange). En las averiguaciones se tuvo conocimiento de que, tras engañar a uno de los usuarios del Punto de Venta, éste reveló sus credenciales, que fueron empleadas posteriormente para la realización del trámite fraudulento.*

*En consecuencia, se concluye que la incidencia se debe a un error puntual humano, por parte del Agente del Punto de Venta que, ante la insistencia y conocimiento de los delincuentes del 'argot' de la compañía -por lo que creyó que estaba tratando con un compañero- consiguieron que el Agente revelase sus credenciales, incumpliendo todos los protocolos e instrucciones que se le habían comunicado en relación con la confidencialidad de las mismas. Estos hechos han sido denunciados por Orange, constando la denuncia con nº de diligencias previas 114/2022 del Juzgado de Primera Instancia e Instrucción nº 1 de ***LOCALIDAD.1. Así mismo, en colaboración con las autoridades, desde Orange se ha procedido a rastrear el IMEI del dispositivo desde el que se realizó el duplicado de eSIM fraudulento, identificando el mismo e incluyéndolo en una BlackList interna, de forma que no pueda volver a ser utilizado.*

Igualmente, se informó desde Orange al Reclamante de todas las actuaciones y averiguaciones efectuadas. El Reclamante continúa siendo un cliente activo de esta parte.

El 7 de abril de 2022, Orange recibe el traslado de la reclamación interpuesta por el Reclamante ante la AEPD con ocasión del presente supuesto de hecho, respondiendo y atendiendo a las cuestiones que presentaba el mismo mediante alegaciones que se presentaron el 9 de mayo de 2022.

En atención al presente supuesto de hecho que nos ocupa, quisiera esta parte reseñar que, si bien hasta ahora se suplantaba la identidad de los clientes de Orange, ahora se suplanta la identidad de empleados y agentes de Orange.

Las aplicaciones móviles se instalan en el dispositivo móvil concreto, por lo que para poder acceder a las mismas, los suplantadores de identidad deberían contar o bien con información adicional del Reclamante, o bien con su terminal móvil. En este sentido, la Agencia no es capaz de justificar que efectivamente se haya tenido conocimiento de esta información por parte de los delincuentes durante el proceso de duplicado. Por lo que, más allá de la conceptualización teórica de los datos incluidos en una tarjeta SIM como datos personales, no se ha acreditado que su confidencialidad haya sido afectada.

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 la comisión 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.

"En este caso, una vez analizadas las razones expuestas por ORANGE ESPAGNE, S.A.U., que obran en el expediente, se considera que no procede el inicio de un procedimiento sancionador al haber sido atendida la reclamación, procediendo acordar el archivo de la reclamación examinada". Es por ello que no resulta posible en el presente la imputación de una infracción a esta parte, cuando en supuestos manifiestamente equivalentes se viene adoptando un criterio de archivo. De lo contrario, nos encontraríamos ante una situación de indefensión e inseguridad jurídica para Orange.

Por todo lo anterior, Orange: 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 Procedimiento Nº: PS/03638/2022.

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 el Acuerdo de Inicio notificado a Orange"

SEXTO: Con fecha 19 de octubre de 2022, el instructor del procedimiento acordó practicar las siguientes pruebas:

"1. Se dan por reproducidos a efectos probatorios la reclamación interpuesta por la reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación. 2. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento

sancionador referenciado, presentadas por Orange, y la documentación que a ellas acompaña".

SÉPTIMO: Con fecha 10 de noviembre de 2022, se notificó a Orange la Propuesta de Resolución, por la que se propone sancionar a Orange por presunta infracción del artículo 6.1) del RGPD, tipificada en el artículo 83.5.a) del RGPD.

OCTAVO: Notificada la propuesta de resolución, la parte reclamada solicitó ampliación del plazo para formular alegaciones por cinco días hábiles, y con fecha 2 de diciembre de 2022 presentó escrito de alegaciones en el que, en síntesis, manifestaba su disconformidad con el contenido de los fundamentos expuestos en la Propuesta de Resolución y se ratifica y da por reproducidas las alegaciones y argumentaciones jurídicas de su anterior escrito, y manifiesta:

"En el presente procedimiento sancionador, la sanción se impone debido a que ORANGE facilitó un duplicado de la tarjeta SIM 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 este sentido, la AEPD ignora el hecho de que ORANGE ha elaborado e implementado un protocolo de solicitud de duplicado de la tarjeta SIM, y lo comunicado a los agentes encargados de tramitar estas solicitudes. No se incluye la más mínima consideración sobre su contenido o la adecuación del mismo para evaluar el despliegue de diligencia que ha llevado a cabo ORANGE.

El hecho de que el protocolo no haya sido seguido supone un incumplimiento contractual por parte del agente de la entidad colaboradora, sancionado por ORANGE (que no dispone de capacidad legal para actuar directamente frente al agente, por lo que se dirige contra su empleadora). En este sentido, resulta inapropiada la pretendida personificación de ORANGE, como si la entidad ejecutase materialmente alguna acción.

Por todo lo anterior, Orange: 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 Procedimiento Nº: PS/03638/2022. 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".

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: La parte reclamante manifiesta que, el 24 de febrero de 2022, se quedó sin línea en uno de sus dos teléfonos móviles. Tras contactar con Orange le indican que

se había realizado un duplicado de su tarjeta SIM, solicitud que no hizo el reclamante, por lo que acude a una tienda física y le facilitan los datos relativos a dicho duplicado, siendo la localidad Barcelona, pese a que el reclamante reside en Madrid.

SEGUNDO: La parte reclamante ha aportado la copia de la denuncia que presentó ante la Guardia Civil de la localidad de Arganda del Rey (Madrid) por estos hechos y documento relativo a la solicitud de duplicado de la tarjeta SIM. Punto de Venta del establecimiento de ***ESTABLECIMIENTO.1, no constando la firma del reclamante.

TERCERO: Orange manifiesta que los días 24 y 25 de febrero de 2022 se realiza, a través de Siebel 8 (sistema interno de activación de tarjetas de Orange móvil solicitadas desde tiendas), un pedido de duplicado de SIM (en concreto una e-SIM) asociado al Punto de Venta de ***ESTABLECIMIENTO.1. El departamento de Fraude procede a categorizar la contratación como irregular y a anular el duplicado de e-SIM.

CUARTO: Orange reconoció en el escrito de respuesta de fecha 18 de octubre de 2022 a esta Agencia que la incidencia se debe a un error puntual humano, por parte del Agente del Punto de Venta de Orange que, ante la insistencia y conocimiento de los delincuentes del 'argot' de la compañía -por lo que creyó que estaba tratando con un compañero- consiguieron que el Agente revelase sus credenciales, incumpliendo todos los protocolos e instrucciones que se le habían comunicado en relación con la confidencialidad de las mismas.

QUINTO: Estos hechos han sido denunciados por Orange, constando la denuncia con nº de diligencias previas 114/2022 del Juzgado de Primera Instancia e Instrucción nº 1 de ***LOCALIDAD.1. Así mismo, en colaboración con las autoridades, desde Orange se ha procedido a rastrear el IMEI del dispositivo desde el que se realizó el duplicado de eSIM fraudulento, identificando el mismo e incluyéndolo en una BlackList interna, de forma que no pueda volver a ser utilizado.

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

Tipificación y calificación de la infracción

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 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).

En este sentido, conviene aclarar que, dentro del terminal móvil, va insertada la tarjeta SIM. Es una tarjeta inteligente, de plástico y 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.

La tarjeta SIM es posible introducirla en más de un terminal móvil, siempre que éste se halle liberado o sea de la misma compañía.

En España, desde el año 2007, mediante la Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, se exige que los titulares de

todas las tarjetas SIM, ya sean de prepago o de contrato, estén debidamente identificados y registrados. Esto es importante por cuanto la identificación del abonado será imprescindible para dar de alta la tarjeta SIM, lo que conllevará que a la hora de obtener un duplicado de esta la persona que lo solicite haya de identificarse igualmente y que su identidad coincida con la del titular.

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.

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".

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 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>>

III

Obligación Incumplida

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

De los Hechos Probados, se deduce que ORANGE ha facilitado duplicado de tarjeta SIM 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.

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".*

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 SIM 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 SIM, sino de que, si en el proceso de expedición de un duplicado de tarjeta SIM no se verifica adecuadamente la identidad del solicitante, la operadora estaría facilitando la suplantación de identidad.

ORANGE cita en su descargo una serie de resoluciones dictadas por la AEPD, manifestando que el presente supuesto resulta análogo al recogido en los procedimientos EXP202104010; EXP202104011 y EXP202105686 a ORANGE, también por casos de fraudes de "Sim Swapping", los cuales fueron objeto de archivo

por la AEPD.

Sobre este particular, procede resaltar que dichos procedimientos tuvieron por objeto analizar los procedimientos seguidos para gestionar las solicitudes de cambio de SIM por parte de ORANGE, identificando las vulnerabilidades que puedan existir en los procedimientos operativos implantados, para detectar las causas por las cuales se pueden estar produciendo estos casos, así como encontrar puntos de incumplimiento, mejora o ajuste, para determinar responsabilidades, disminuir los riesgos y elevar la seguridad en el tratamiento de los datos personales de las personas afectadas. Los hechos reclamados, en los procedimientos citados, se refieren al mismo procedimiento operativo de protección de datos que ha sido investigado y sancionado por la AEPD mediante resolución de fecha 10/11/2021 en el marco del procedimiento sancionador PS/00022/2021, tramitado contra la parte reclamada y se le imputa la violación del artículo 5.1f).

En el presente procedimiento sancionador, la sanción se impone debido a que ORANGE facilitó un duplicado de la tarjeta SIM 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 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.

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 este sentido, ORANGE cuenta con una red de comerciales, puntos de venta y distribuidores homologados a través de un contrato de distribución para ofrecer los servicios de ORANGE. Entre estos servicios ofrecidos desde sus puntos de venta, está la realización de duplicados de tarjetas SIM correspondientes a una línea de telefonía móvil.

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

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

Orange reconoció en sus alegaciones de fecha 18 de octubre y de 12 de diciembre de 2022 a esta Agencia que la incidencia se debe a un error puntual humano, por parte del Agente del Punto de Venta de Orange que, ante la insistencia y conocimiento de los delincuentes del ‘argot’ de la compañía -por lo que creyó que estaba tratando con un compañero- consiguieron que el Agente revelase sus credenciales, incumpliendo

todos los protocolos e instrucciones que se le habían comunicado en relación con la confidencialidad de las mismas.

De conformidad con las evidencias de las que se dispone, se estima que la conducta de la parte reclamada vulnera el artículo 6,1 del RGPD 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."*

IV

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, en una valoración inicial, se estiman concurrentes en el presente caso los siguientes factores:

En calidad de agravantes:

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

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

En calidad de atenuantes:

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

Procede graduar la sanción a imponer a la reclamada y fijarla en la cuantía de 70.000 € 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 70.000 euros (setenta mil euros).

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

TERCERO: Advertir 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***, 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.

938-181022

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