- **Expediente N.º: EXP202204288**

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 nombre y representación de Dña. ***B.B.B.*** (en adelante, la parte reclamante) con fecha 10 de marzo de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ORANGE ESPAGNE, S.A.U. con NIF A82009812 (en adelante, la parte reclamada o Orange). Los motivos en que basa la reclamación son los siguientes:

La mercantil "Telecomunicaciones y Energías Renovables R2I, S.L" suscribió un contrato de telefonía con la entidad reclamada, siendo la reclamante trabajadora y apoderada de dicha mercantil, así como usuaria de una de las líneas de telefonía móvil contratada. Manifiesta que, en fecha 17 de enero de 2022, su línea móvil ******TELEFONO.1*** se quedó sin cobertura, obedeciendo dicha incidencia a que la entidad reclamada facilitó a un tercero un duplicado de la tarjeta SIM de dicha línea móvil, sin el consentimiento de la mercantil titular de la línea, ni de la usuaria (reclamante).

A raíz de la información contenida en el teléfono móvil, dicho tercero accedió a la banca electrónica, realizando transferencias fraudulentas desde la cuenta de la mercantil, así como también desde la cuenta personal de la reclamante (en fecha 17 y 18 de enero de 2022). Tras lo ocurrido, la reclamante (a través de su abogado) solicitó a la entidad reclamada, sin éxito, que le facilitase copia de la grabación relativa a la solicitud del duplicado controvertido, así como de la documentación que fue entregada por el tercero a la hora de realizar la solicitud en el establecimiento implicado, procediendo dicha entidad al cierre de las reclamaciones, aludiendo a la normativa de protección de datos.

Asimismo, presenta denuncia ante la Policía, en fecha 18 de enero de 2022, incoándose las correspondientes diligencias previas.

Por otro lado, manifiesta que, para recuperar la línea, tuvo que solicitar un nuevo duplicado de la tarjeta SIM y, en la factura correspondiente al mes de enero de 2022, figura una devolución de dinero por "cambio de SIM", devolución que no fue solicitada por la reclamante, por lo que considera que es una forma de reconocer, la entidad reclamada, su responsabilidad por lo sucedido.

Solicita a esta Agencia que requiera a la entidad reclamada la aportación de la grabación de la solicitud del duplicado y de la documentación que fue facilitada para la entrega del citado duplicado.

Y, aporta entre otra, la siguiente documentación relevante:

Denuncia presentada ante la Policía y ampliación de la misma de fechas 18 de enero y 4 de febrero de 20223, indicándose que el duplicado de la tarjeta se realizó el 14 de enero de 2022 sobre las 19 horas, según la información facilitada a la reclamante por el servicio de atención al cliente de Orange el 19 de enero del mismo año.

Factura telefónica, a nombre de la mercantil, de fecha 5 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 27 de abril 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 27 de mayo de 2022 se recibe en esta Agencia escrito de respuesta indicando: *"que se detectó el duplicado de e-SIM usurpando la identidad de la reclamante. Los autores de la usurpación de identidad se pusieron en contacto con un empleado del Punto de Venta del establecimiento de TIENDA ORANGE SALT Centro Comercial ESPAI GIRONES haciéndose pasar por un empleado de otro Punto de Venta (concretamente de un empleado del Phone House de la calle Juan de Austria), haciendo uso de la jerga y lingo propios de la misma, demostrando conocimientos concretos sobre usos y características de las bases de datos de esta mercantil. Tras esto, por un error del todo involuntario del Agente del Punto de Venta y, saltándose las especificaciones indicadas en este tipo de situaciones por esta mercantil, facilitó los datos de la reclamante, al entender que estaba hablando con un compañero de otro establecimiento.*

Obtenidos los citados datos, fue cuando esta persona solicitó el duplicado de e-SIM expuesto por la reclamante. En el momento en el que la 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.

Cabe indicar a esta Agencia las medidas adicionales que, con motivo del estudio realizado, se han llevado a cabo por parte de la compañía. En primer lugar, indicar que desde esta mercantil se solicitó en fecha 27 de enero de 2022 una revisión del inventario en el Punto de Venta donde se realizó el duplicado, indicándose que debían bloquearse aquellas SIM que no fueran localizadas. Asimismo, del estudio realizado se ha detectado que el duplicado se realizó a través de un servicio "On Call" disponible en algunos canales de venta disponible para tramitar altas cuando tienen incidencias. En la actualidad se ha reforzado la formación en este sentido, así como las indicaciones sobre duplicados de SIM, motivo por el cual operaciones de esta naturaleza ya no es posible solicitarlas y realizarlas a través de este canal. Habida

cuenta de lo acontecido en el presente caso se ha procedido a realizar un comunicado al canal para reforzar la formación de los agentes en este sentido. Se aporta como documento anexo nº1 el comunicado remitido.

De igual forma, y en colaboración con las autoridades, desde la compañía se ha procedido a rastrear el IMEI del dispositivo desde el que se realizó el duplicado de eSIM fraudulento, incluyéndolo en BlackList interna, de forma que el mismo no pueda volver a ser utilizado.

Por último, señalar que la respuesta de esta mercantil ante el caso que nos ocupa fue muy ágil, inmediata, pues nada más poner la reclamante en conocimiento del personal de Orange lo ocurrido, la compañía procedió a la anulación del duplicado irregular, a la realización de cuantos ajustes correspondían tal y como se la misma ha expuesto en su reclamación y se puso en marcha la exhaustiva investigación anteriormente expuesta en aras a determinar el alcance de dicho incidente y la causa origen que provocó esta incidencia. De todo lo anterior fue informado el reclamante dado que continua activo en esta mercantil".

TERCERO: Con fecha 1 de junio 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 el 18 de enero de 2022 se produce una solicitud para emitir un duplicado de tarjeta SIM. La misma se produce a través de "Atención al Canal", un servicio de soporte para los empleados y agentes de los puntos de venta de Orange. Así, la incidencia se debe a un error puntual humano.*

Desde el departamento de Fraude de Orange se identifica un incumplimiento del protocolo establecido (solicitud a través de la herramienta "On Call") en el proceso de activación de duplicado de tarjeta SIM en cuestión. Por ello, se somete el mismo a un proceso de verificación, de forma que se revisa el proceso de solicitud y concesión de la misma.

Mientras el departamento de Fraude de Orange está en proceso de verificación de la solicitud de duplicado de SIM, la "Reclamante", se pone en contacto con esta parte para informar de que ha sido víctima de una suplantación de identidad.

Inmediatamente, desde el departamento de Fraude se produce la categorización del duplicado de SIM como irregular, procediendo de forma inmediata a bloquear la línea.

En colaboración con las autoridades, desde Orange se ha procedido a rastrear el IMEI del dispositivo desde el que se realizó el duplicado de SIM fraudulento, identificando el mismo e incluyéndolo en una BlackList interna, de forma que no pueda volver a ser utilizado.

Si bien hasta ahora se suplantaba la identidad de los clientes de Orange, ahora vemos cómo procede a suplantar la identidad de empleados y agentes de Orange. Es por ello que, frente al establecimiento por los delincuentes de nuevas vías y técnicas de comisión del fraude, Orange procederá de nuevo al establecimiento de protocolos y medidas de seguridad adicionales. Es por ello que no resulta posible apreciar culpabilidad de Orange en el presente supuesto de hecho, no siendo jurídicamente válida la apreciación que realiza la Agencia de comisión de infracción por esta mercantil.

En atención a la comisión de fraudes como el que nos ocupa, Orange ha puesto en marcha un plan de acción que estima tener implementado a finales de este año, con el objetivo de mitigar la comisión de fraudes en los procesos de duplicados de SIM a través de métodos como el "Sim Swapping". Las actuaciones previstas se concretan en las siguientes medidas: - Implantación de un doble factor de identificación, cuyo proyecto piloto ya se encuentra activo, estando en fase de testeo con ciertos usuarios. - Proyecto "Whitelist IP" de limitación de acceso a sistemas internos de Orange desde IPs no identificadas. En atención a todas las medidas enunciadas, considera esta parte que se ha acreditado, por parte de Orange, el empleo de un nivel de diligencia adecuado con el que, si bien no resulta posible, por limitación de la tecnología y los medios humanos, la existencia de un riesgo cero, sí es actualizado y revisado periódicamente en conforme el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Así, el presente supuesto resulta análogo al recogido en el EXP202104010 a Orange, también por un supuesto de fraude 'Sim Swapping', el cuál fue objeto de archivo por la AEPD.

Sobre este particular, procede resaltar que hechos similares a los que son objeto de reclamación han sido investigados por esta Agencia y sancionados en el procedimiento sancionador PS/00022/2021, tramitado contra la parte reclamada, por resolución de fecha 10/11/2021, por lo que no procede el inicio de un nuevo procedimiento sancionador". Todos y cada uno de los elementos identificados por la AEPD como motivos de archivo en este EXP202104010 se reproducen y son totalmente aplicables al presente procedimiento 202204288. No obstante, el expediente identificado no constituye un caso aislado. El EXP202104011, también con relación a un supuesto de Sim Swapping y también archivado por la AEPD a Orange, indica, de forma idéntica: "procede resaltar que hechos similares a los que son objeto de reclamación han sido investigados por esta Agencia y sancionados en el procedimiento sancionador PS/00022/2021, tramitado contra la parte reclamada, por resolución de fecha 10/11/2021, por lo que no procede el inicio de un nuevo procedimiento sancionador". Y, nuevamente y en idéntico sentido, en el

EXP202105686 a Orange, también relativo a un supuesto de 'Sim Swapping', se procede a su archivo por la AEPD: "Sobre este particular, procede resaltar que los hechos reclamados 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 que se publicará en la la página web www.aepd.es. […]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.

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. 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, atendiendo a los argumentos manifestados en el cuerpo del presente escrito de alegaciones".

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 15 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 7 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:

"La AEPD inicia su fundamentación reiterando la forzada interpretación de que la tarjeta SIM no sólo contiene, sino que, constituye, en sí misma, un dato de carácter personal.

Si bien esta parte reconoce que el proceso de emisión de un duplicado de tarjeta SIM implica el tratamiento de datos, ha de puntualizarse que los datos que supuestamente hacen de la tarjeta SIM un dato personal para la AEPD son: • El MSISDN es el número de teléfono del titular de la línea (precedido el prefijo nacional). Como es evidente a tenor del supuesto de hecho, los supuestos suplantadores de identidad ya conocían el número de teléfono del titular de la línea de forma previa a tener contacto con ORANGE, en tanto fue facilitado por los mismos al solicitar el duplicado de tarjeta SIM. • El IMSI es información técnica que identifica al abonado en la línea, pero únicamente para su compañía telefónica, que dispone de la información suficiente para relacionarla con su titular. Para cualquier persona que no tenga acceso a los sistemas de la compañía telefónica (en este caso ORANGE), no resulta posible relacionar este dato con una concreta persona. Complementariamente a lo anterior, es especialmente relevante un hecho que la AEPD ha pasado por alto y es que el abonado es, en este caso, una persona jurídica.

Por tanto, aun en el supuesto totalmente improbable de que un tercero pudiese llegar a *relacionar los datos contenidos en la tarjeta con un abonado, lo cierto es que no identificaría a una persona física, sino a una mercantil, que es la titular de la línea: en concreto, la mercantil "Telecomunicaciones y Energías Renovables R2l", S.L. Esta mercantil es la entidad que ha contratado con ORANGE, siendo su único cliente en el presente supuesto.*

Es decir, que tanto el número de teléfono como el IMSI afectados en el presente supuesto de hecho, se sitúan fuera de la definición de dato personal que realiza el artículo 4 del RGPD. Así, dicho tratamiento quedaría fuera del ámbito de aplicación de la normativa de protección de datos personales y, consiguientemente, fuera del ámbito de actuación de la autoridad de control. Todo ello, teniendo en cuenta además que es evidente que el suplantador de identidad conocía y tenía bajo su control – de forma previa a cualquier contacto con ORANGE- los datos de la línea telefónica suplantada.

Esta información, obtenida antes de dirigirse a ORANGE, es la que ha permitido que el suplantador consiguiese tener acceso a un duplicado de la tarjeta SIM de la mercantil. Por ello, más allá de la conceptualización teórica de los datos incluidos en una tarjeta SIM como datos personales, no se ha acreditado que se haya producido, en el presente supuesto, un tratamiento de datos personales.

Es un hecho que las entidades bancarias son las únicas responsables de la seguridad de sus operaciones, tal y como lo afirma la Autoridad Bancaria Europea (en adelante, la "EBA") en los siguientes pronunciamientos: • Opinion on the implementation of the RTS on SCA and CSC: en su apartado relativo a quién decide sobre los medios a emplear para dicha autenticación (puntos 37 y 38), dictamina que las credenciales de seguridad utilizadas para realizar la autenticación segura de los usuarios de los servicios de pago son responsabilidad de la entidad gestora de servicios de cuenta (en el caso que nos ocupa, las entidades financieras). • Qualification of SMS OTP as an authentication factor | European Banking Authority: indica que el uso de SMS ordinarios no es factible para la confirmación de operaciones bancarias, por no ser suficientemente seguros conforme a los estándares de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior (PSD2). En este sentido, indica que: "el artículo 22 (1) del Reglamento exige que 'los proveedores de servicios de pago garantizarán la

confidencialidad e integridad de las credenciales de seguridad personalizadas del usuario del servicio de pago, incluidos los códigos de autenticación, durante todas las fases de la autenticación' y el artículo 22, apartado 4, del Reglamento Delegado establece que 'los proveedores de servicios de pago garantizarán que el procesamiento y el enrutamiento de las credenciales de seguridad personalizadas y de los códigos de autenticación generados de conformidad con el Capítulo II tengan lugar en entornos seguros en consonancia con estándares firmes y ampliamente reconocidos del sector". La negrita corresponde a esta parte. Por lo tanto, es indudable que el proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas, pero en ningún caso impedir que puedan producirse. De esta forma, el supuesto de hecho quedaría a lo dispuesto en el régimen previsto en el Real Decreto-Ley 19/2018, de 23 de noviembre, de Servicios de Pago y otras Medidas Urgentes en Materia financiera, debiendo valorarse la responsabilidad del proveedor de los servicios de pago.

Así, contradice cualquier lógica jurídica trasladar toda la responsabilidad a la entidad que presta servicios de telefonía, tratándose del mero canal de comunicación seleccionado por la propia entidad financiera y sin que a esta le conste, en modo alguno, que los datos transmitidos a través de los mensajes remitidos contengan claves de operaciones bancarias. Extrapolando el supuesto de hecho a otros entornos, resultaría inaudito responsabilizar a entidades que permiten la creación de cuentas de correo electrónico, como Google o Yahoo, que ha tenido lugar una suplantación de identidad a través de un ataque "phishing", empleando el atacante el correo electrónico como medio para llevar a cabo la operación fraudulenta posterior.

Destacar que ORANGE no ofrece servicios de confianza online a operadores bancarios, ni tampoco ofrece servicios propios de una entidad de certificación o acreditación. Las entidades bancarias pueden no haber contratado ningún servicio a ORANGE, y, aun así, emplear los SMS para llevar a cabo sus actuaciones con clientes. Por ello, no se puede responsabilizar a ORANGE de la configuración del envío de SMS como segundo factor de autenticación empleado por responsables de otros servicios, como son los operadores bancarios. Es totalmente improcedente pretender que, si las entidades bancarias deciden confiar en la identificación realizada por terceros, se responsabilice a éstos de tal decisión, salvo que presten este tipo de servicios, conforme a los establecido en el Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas. Y este no es el caso de los servicios prestados por ORANGE.

ORANGE no puede hacerse cargo de la seguridad de la operativa de terceras entidades por el mero hecho de que usen servicios de telecomunicaciones. Este hecho es todavía más evidente en el presente caso, puesto que ha de reiterarse que, si bien se ha podido ver afectada por la suplantación en la solicitud de la tarjeta SIM una persona física, la titular de la línea telefónica afectada por la suplantación y el fraude SIM SWAPPING es una persona jurídica, no habiendo por tanto una relación directa entre la identidad de la persona física y la supuesta suplantación de la línea telefónica.

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. Es obvio que las personas jurídicas actúan por medio de sus representantes, empleados y colaboradores y que son estos quienes deben cumplir en el ejercicio de sus funciones con los protocolos establecidos. En este caso, como ha quedado acreditado, la entidad cuenta con un protocolo adecuado para la correcta tramitación de las solicitudes (cuya efectividad en la prevención del fraude es muy elevada, superando el 99%). En este caso, la suplantación deriva de la actuación inadecuada de uno de los agentes. En este sentido, ha de tenerse en consideración que no es factible la eliminación del riesgo asociado al factor humano, puesto que el incumplimiento de los procedimientos establecidos no es materialmente evitable, salvo que se prescinda de la intervención humana en todo proceso de contratación, lo cual, aparte de inviable, implicaría la toma de decisiones de forma totalmente automatizada, lo que es considerado como un riesgo por el propio RGPD.

Conviene recordar a la Agencia, que es el Tribunal Constitucional (en lo sucesivo, TC), el que, desde su Sentencia nº 76/1990 de 26 de abril, ha venido advirtiendo del problema de la inadmisibilidad en nuestro ordenamiento jurídico de la responsabilidad objetiva y, consecuente con ello, la exigencia en todo caso de que la Administración, a la hora de sancionar, pruebe algún grado de intencionalidad en el sancionado. En la indicada sentencia se vino a señalar que la posibilidad de imponer una sanción exige la concurrencia de culpabilidad en los grados de dolo y culpa o negligencia grave, no siendo suficiente la mera negligencia. Es por ello que se excluye la posibilidad de sancionar por la mera concurrencia de un resultado, entendiendo el TC que "el mero error humano no puede dar lugar, por sí mismo (y sobre todo cuando se produce con carácter aislado), a la atribución de consecuencias sancionadoras; pues, de hacerse así, se incurriría en un sistema de responsabilidad objetiva vedado por nuestro orden constitucional". En virtud de lo anterior, resulta posible afirmar que este proceder, utilizado en la actual Propuesta de la AEPD, que asocia al mero error humano consecuencias sancionadoras, no resulta conforme a derecho, como ya se ha indicado también por la Audiencia Nacional, entre otras, en su Sentencia de la Sala de lo Contencioso-administrativo, Sección 1ª, de 23 de Diciembre de 2013, Rec. 341/2012.

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

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/04288/2022. 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"

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

HECHOS PROBADOS

PRIMERO: La parte reclamante manifiesta que, el 17 de enero de 2022, se quedó sin cobertura en su línea móvil ******TELEFONO.1***, obedeciendo dicha incidencia a que la entidad reclamada facilitó a un tercero un duplicado de la tarjeta SIM de dicha línea móvil, sin el consentimiento de la mercantil titular de la línea, ni de la usuaria (reclamante).

SEGUNDO: La parte reclamante ha aportado copia de la denuncia que presentó ante la Policía y ampliación de la misma de fechas 18 de enero y 14 de febrero de 2023, manifestando que el duplicado de la tarjeta se realizó el 14 de enero de 2022 sobre las 19 horas, según información facilitada a la reclamante por el servicio de atención al cliente de Orange el 19 de enero del mismo año.

TERCERO: Orange reconoció tanto en el escrito de respuesta de fecha 27 de mayo, como en el de alegaciones del 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 el 18 de enero de 2022 se produce una solicitud para emitir un duplicado de tarjeta SIM. La misma se produce a través de "Atención al Canal", un servicio de soporte para los empleados y agentes de los puntos de venta de Orange. Así, la incidencia se debe a un error puntual humano".*

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 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:

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

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

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

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

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

Este acceso no autorizado a los datos personales de los afectados resulta determinante para las actuaciones posteriores desarrolladas por las personas

suplantadoras, ya que aprovechan el espacio de tiempo que trascurre hasta que el usuario detecta el fallo en la línea, se pone en contacto con la operadora, y ésta detecta el problema, para realizar operaciones bancarias fraudulentas y que sin el duplicado de la tarjeta SIM hubiera devenido imposible su realización.

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

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

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

Por otra parte, para completar la estafa, es necesario que un tercero “suplante la identidad” del titular de los datos, para recibir el duplicado de la tarjeta SIM. Lo que conlleva a priori, un tratamiento al margen del principio de licitud pues un tercero está tratando datos, ya que tiene acceso a ellos, sin base legal alguna, además de la vulneración de otros principios como el de confidencialidad.

Por dicha razón, este es un proceso en donde la diligencia prestada por las operadoras es fundamental para evitar este tipo de estafas y vulneraciones del RGPD. Diligencia que se traduce en el establecimiento de medidas adecuadas para garantizar que se implantan y mantienen medidas de seguridad apropiadas para proteger eficazmente la confidencialidad, integridad y disponibilidad de todos los datos personales de los cuales son responsables, o de aquellos que tengan por encargo de otro responsable.

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

Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este

tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

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

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

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

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

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

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

Ciertamente, el principio de responsabilidad previsto en el artículo 28 de la LRJSP, dispone que: "*Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les*

reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

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

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

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

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, parcialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, Rec 1067/2006, que *"aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa".*

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

Pues bien, resulta acreditado que Orange reconoció en su escrito de respuesta de fecha 27 de mayo y en sus alegaciones de fecha 18 de octubre de 2022 a esta Agencia que la incidencia se debió 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, 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.

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