- **Expediente N.º: EXP202213029**

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 27 de octubre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra DIGI SPAIN TELECOM, S.L. con NIF B84919760 (en adelante, DIGI). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que sin su consentimiento se facilitó y activó por parte de DIGI una segunda tarjeta SIM, sin presentar el DNI original e incumpliendo todo el protocolo necesario para la entrega de estas tarjetas.

Que a las 10:30 de la mañana del día 26 de octubre de 2022 su teléfono móvil ******TELÉFONO.1*** se quedó sin servicio tras lo cual recibió un email de DIGI explicándole que con su número había sido activada una segunda tarjeta SIM, se puso en contacto con la operadora para indicarles que él no había sido y tras esto intentaron entrar en sus cuentas bancarias por lo que dio la orden a su entidad bancaria que anularan todas sus tarjetas y cambiaran sus claves.

Posteriormente, DIGI le facilitó una segunda SIM la cual se activó a las 13:50 horas del indicado día y se estableció otro filtro de seguridad con una clave que proporcionó el reclamante para que para cualquier trámite se tuviera que facilitar la misma.

El mismo día a las 16:20 se quedó de nuevo sin línea y recibió otro correo electrónico informándole que se había vuelto activar otra SIM con su número, por un supuesto suplantador.

Añade que contactó de nuevo con DIGI, le facilitaron otra SIM la cual recogió en una tienda física de su localidad al igual que la primera y en la que tuvo que identificarse con su DNI original, pero en ningún momento le pidieron el filtro que se estableció el de facilitar la clave para autorizar y facilitarle la tarjeta SIM.

Junto a su reclamación aporta los correos electrónicos remitidos a la parte reclamada de fechas 26 y 27 de octubre de 2022, y contestación de DIGI del día 27 del mismo mes y año.

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 DIGI, 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 19 de diciembre de 2022 como consta en el acuse de recibo que obra en el expediente. Solicitando DIGI, con fecha 19 de enero de 2023, ampliación de plazo para contestar a esta Agencia.

Con fecha 2 de febrero de 2023 se recibe en esta Agencia escrito de respuesta indicando: "Que un primer duplicado de la tarjeta SIM asociada a la línea móvil ***TELÉFONO.1*: *Tal y como consta registrado en los sistemas de DIGI, el día 25 de octubre de 2022 a las 19:39 horas, se recibió, en el stand de DIGI ubicado en el centro comercial ***ESTABLECIMIENTO.1 (***DIRECCIÓN.1*), *una solicitud de duplicado de SIM para la línea móvil ***TELÉFONO.1*. *Para la tramitación de esta solicitud, el solicitante y presunto titular de la línea, se identificó como el reclamante, mediante un documento de identidad original, copia del cual se obtuvo en aquel momento.*

La citada solicitud de duplicado, junto con la documentación que la acompañaba, fue remitida al equipo de BackOffice de DIGI, conforme al procedimiento que actualmente tiene DIGI en vigor, y que exige, no solo la obtención de una copia del documento de identidad del solicitante, sino también la revisión de la solicitud y de la documentación por parte de dicho equipo.

Así pues, en vista de que presumiblemente la solicitud, y la documentación asociada a la misma era correcta, se validó la solicitud por parte del equipo de BackOffice de DIGI, y se procedió a la activación del duplicado de SIM al día siguiente a las 10:11 horas.

*En el momento en que el duplicado se encontró activo, se envió un SMS informativo al número de teléfono ***TELÉFONO.1** informando de la activación exitosa del duplicado solicitado.*

*Un segundo duplicado de la tarjeta SIM asociada a la línea móvil ***TELÉFONO.1*: *El 26 de octubre de 2022 a las 12:07 horas, una persona identificada como el reclamante, contactó con DIGI de forma telefónica para informar de que había recibido un SMS en su línea móvil indicando que se había llevado a cabo un duplicado de SIM para ese mismo número.*

Ante esta información, tras pasar el correspondiente desafío de seguridad para identificar al llamante como titular de la línea, y confirmar con el mismo los siguientes pasos, DIGI procedió a bloquear la línea como medida de seguridad, hasta que el titular confirmara haber realizado un nuevo duplicado. Asimismo, se abrió un ticket interno por posible caso de usurpación de identidad, y se solicitó al llamante, el reclamante, que presentará ante la Policía y luego remitiera a DIGI la correspondiente denuncia junto con una copia de su documento de identidad para poder continuar con el análisis oportuno.

*El 26 de octubre de 2022 a las 13:06 horas se recibió una solicitud de un segundo duplicado SIM para la línea ***TELÉFONO.1*. *Este nuevo duplicado se solicitó en el establecimiento de nuestro distribuidor **B.B.B. (***DIRECCIÓN.2).** *Para la tramitación de esta solicitud, el solicitante y presunto titular de la línea, se identificó como el*

reclamante, mediante su documento de identidad original, copia del cual se obtuvo en aquel momento.

Esta nueva solicitud de duplicado, junto con la documentación que la acompañaba, fue remitida de nuevo al equipo de BackOffice de DIGI para su validación conforme al procedimiento implantado por DIGI. Tras la correspondiente revisión de la solicitud y su documentación, y teniendo constancia de la anterior llamada de reclamación del titular de la línea advirtiendo de una suplantación, y del ticket interno abierto, se procedió a la activación del nuevo duplicado de SIM a las 13:58 horas de ese mismo día 26 de octubre de 2022.

En el momento en que el duplicado se encontró activo, de nuevo, se envió SMS informativo informando de la activación exitosa del duplicado solicitado. El mismo día 26 de octubre de 2022, a las 15:23, se recibió una nueva llamada desde la línea ******TELÉFONO.2*** *de una persona que de nuevo se identificaba como el reclamante, preguntando por su línea. Se le pregunta por la denuncia por usurpación, a lo cual el interlocutor indica que no ha puesto ninguna denuncia, se pone nervioso y cuelga.*

Desde el equipo de Reclamaciones de DIGI, analizados los hechos, y tras la citada llamada, se procede a indicar, en el ID de la línea en cuestión, una anotación en rojo con la siguiente literalidad: Reclamaciones//Se ha utilizado un duplicado de SIM fraudulento para este cliente, hemos añadido DNI real al ID//Por favor revisar DNI antes de validar duplicado//Gracias //Comprobamos que posible usurpador está llamando desde la línea ******TELÉFONO.2****, si llama alguien desde esta línea, no dar ningún dato ni información Adicionalmente, a las 15:41 desde DIGI se llama al cliente titular de la línea (llamando a la línea* ******TELÉFONO.1*** *que estaba siendo objeto del presunto fraude), y el titular informa que enviará copia de la denuncia y de su documento de identidad.*

Se acuerda con el cliente asimismo establecer una palabra clave de seguridad, que se deja también anotada en rojo y asociada al ID.

Un tercer duplicado de la tarjeta SIM asociada a la línea móvil ******TELÉFONO.1****: El mismo día 26 de octubre de 2022, a las 16:19 horas, se recibió una tercera solicitud de duplicado para la línea móvil* ******TELÉFONO.1****. Este tercer duplicado se solicitó en el establecimiento de nuestro distribuidor* ***C.C.C. (***DIRECCIÓN.3).***

Para la tramitación de esta solicitud, el solicitante se volvió a identificar como el reclamante, mediante un documento de identidad original, copia del cual se obtuvo en aquel momento. La nueva solicitud de duplicado, junto con la documentación que la acompañaba, de nuevo fue remitida al equipo de BackOffice de DIGI para su validación.

No obstante, en esta validación, el asesor al que se asignó la tarea no siguió el procedimiento que DIGI tiene establecido internamente (y respecto al cual todos sus asesores de BackOffice están informados y formados) para la validación de duplicados SIM conforme al procedimiento actualmente vigente en DIGI.

Cabe mencionar que este procedimiento, como no puede ser de otra forma, implica, entre otras cosas, la obligación del asesor de DIGI de (1) revisar toda la

documentación asociada al ID de la línea para la cual se está solicitando un duplicado, incluyendo los tickets y observaciones que figuran en dicho ID; (2) comprobar si existen solicitudes de duplicado previas, que puedan constituir un indicio de que el titular pudiera estar siendo víctima de algún tipo de fraude por suplantación; y (3) contactar con el cliente para confirmar la palabra clave que este hubiera puesto como medida de seguridad para evitar duplicados no autorizados.

Desafortunadamente, en este caso, por una negligencia, el asesor que tenía asignada esta validación, no llevo a cabo ninguna de estas comprobaciones, incumpliendo sus obligaciones laborales, y procedió a validar la nueva solicitud de duplicado, siendo el mismo activado a las 16:30 horas del 26 de octubre de 2022, enviándose el correspondiente SMS informativo.

Un cuarto duplicado de la tarjeta SIM asociada a la línea móvil ******TELÉFONO.1****: El mismo día 26 de octubre de 2022, a las 17:44 horas, se recibió nuevamente llamada de una persona, presuntamente el reclamante, para informar de que había vuelto a sufrir un duplicado fraudulento en la tarjeta SIM asociada a su línea. Tras pasar el correspondiente desafío para identificación telefónica, y confirmar con el mismo los siguientes pasos, DIGI procedió a bloquear la línea como medida de seguridad, hasta que el titular confirmara haber realizado un nuevo duplicado. Igualmente, se le insistió en que debía presentar la correspondiente denuncia, y remitir la misma a DIGI junto con una copia de su documento de identidad. Tras la anterior llamada, a las 19:21 horas, se realizó una cuarta solicitud de duplicado de SIM en el establecimiento de nuestro distribuidor* ***B.B.B. (***DIRECCIÓN.2)****, que fue activado, una vez validada la solicitud, a las 19:47 horas, enviándose un SMS informando de la activación.*

Para la tramitación de esta solicitud, el solicitante y presunto titular de la línea, se identificó como el reclamante, mediante su documento de identidad original, copia del cual se obtuvo en aquel momento.

Se procedió a amonestar al asesor que, incumpliendo sus obligaciones y el procedimiento establecido para la validación de duplicados, validó el tercer duplicado sin comprobar las advertencias y la documentación que ya constaban asociados al ID del reclamante.

Asimismo, se le incluyó en un plan de refuerzo formativo para el debido control de los procedimientos de DIGI, especialmente el relativo a validación de duplicados.

En el caso del segundo duplicado presuntamente fraudulento (el tercer duplicado en el iter de los hechos descritos en el apartado 1 de este escrito), el mismo solo fue posible habiéndose aprovechado el usurpador de la negligencia del asesor de DIGI que validó dicho duplicado, el cual debió cumplir, y no cumplió, con sus obligaciones, y debió haber seguido, y no lo hizo, el procedimiento que DIGI tiene implantado para la validación de duplicados".

TERCERO: De conformidad con el artículo 65 de la LOPDGDD, cuando se presentase ante la Agencia Española de Protección de Datos (en adelante, AEPD) una reclamación, ésta deberá evaluar su admisibilidad a trámite, debiendo notificar a la parte reclamante la decisión sobre la admisión o inadmisión a trámite, en el plazo de tres meses desde que la reclamación tuvo entrada en esta Agencia. Si, transcurrido

este plazo, no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en el Título VIII de la Ley.

Dicha disposición también resulta de aplicación a los procedimientos que la AEPD hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes. En este caso, teniendo en cuenta lo anteriormente expuesto y que la reclamación se presentó en esta Agencia, en fecha 27 de octubre de 2022, se comunica que su reclamación ha sido admitida a trámite, con fecha 27 de enero de 2023, al haber transcurrido tres meses desde que la misma tuvo entrada en la AEPD.

CUARTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad DIGI SPAIN TELECOM, S.L. es una gran empresa constituida en el año 2006, y con un volumen de negocios de 364.201.000 euros en el año 2021.

QUINTO: Con fecha 27 de marzo de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta infracción del Artículo 6.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), tipificada en el artículo 83.5 del RGPD.

SEXTO: Con fecha 10 de abril de 2023, DIGI solicita la ampliación del plazo legal conferido para contestar dicho requerimiento y copia del expediente.

SEPTIMO: Con fecha 26 de abril de 2023, se recibe en esta Agencia, en tiempo y forma, escrito del representante de DIGI en el que en síntesis, se aduce que se reiteran en las alegaciones previamente presentadas, señalando primeramente de manera cronológica como ocurrieron los hechos, indicando el protocolo de seguridad y las medidas adoptadas por estos hechos, manifestando que la suplantación de identidad y el acceso a los datos del titular de forma ilegítima se produce de forma previa a tener contacto con DIGI y es la causa que provoca la incidencia y la emisión del duplicado de la tarjeta SIM.

En consecuencia, señalan, que no resulta posible asociar a DIGI la realización de un tratamiento no legitimado de datos personales, dado que su actuación se reduce al cumplimiento de sus procesos y obligaciones.

Es decir, durante el proceso de solicitud y entrega del duplicado se produce un tratamiento de los datos personales que se facilitan a DIGI con el objeto de que este verifique la identidad del interlocutor, primero por medios telefónicos y posteriormente de forma presencial.

Además, expone que sólo una actuación particular de un empleado, incumpliendo las instrucciones que tenía y por tanto sus obligaciones laborales, sin que DIGI tenga capacidad para evitarlo, permite superar este protocolo.

Por otra parte, señala que la AEPD impone inequívocamente a DIGI una responsabilidad objetiva, en la cual, independientemente de la diligencia y medidas desplegadas, se declara la culpabilidad de la entidad. La AEPD parece confundir el concepto de responsabilidad proactiva con la obligación de resultado que impone la responsabilidad objetiva. En el presente supuesto, se evidencia la existencia de un

estricto control, previo y posterior a la solicitud del duplicado, el establecimiento de medidas previas y a posteriori, así como la existencia de medidas encaminadas a evitar de forma previa estas prácticas.

Es por ello que la parte reclamada considera que el presente Acuerdo de inicio no es ajustado a derecho, pues impone a DIGI una obligación de resultado, basándose únicamente en el resultado lesivo que se produce por la actividad fraudulenta de un tercero, sin atender a la diligencia utilizada y sin considerar el despliegue de medidas técnicamente adecuadas e implantadas.

Por otro lado, manifiesta la falta de proporcionalidad indicando que la AEPD apertura procedimientos sancionadores, durante el año 2021, a las cuatro grandes operadoras de telecomunicaciones del escenario nacional, tras realizar una revisión general de sus procedimientos de duplicados de tarjetas SIM y los consiguientes procedimientos de SIM SWAPPING. Dicha revisión, genérica, derivó en una sanción para cada una de las teleoperadoras, y en el caso de DIGI hasta once procedimientos sancionadores.

En concreto, reseñan la sanción impuesta en el procedimiento sancionador de la AEPD PS/000027/2021, que consideran que es análogo y versa sobre supuestos de hechos idénticos.

Además, señala que concurren en el presente las siguientes circunstancias atenuantes que no han sido consideradas en la adecuada graduación de la sanción:
La inexistencia de infracciones previas cometidas por DIGI (art. 83.2 e) RGPD).
En ningún momento se han tratado categorías especiales de datos (Art. 83.2 g) RGPD)
El grado de cooperación de DIGI con la AEPD con el fin de poner remedio a una supuesta infracción y mitigar sus posibles efectos adversos (art. 83.2 f) RGPD).
El inexistente beneficio obtenido (Art. 83.2 k).

Solicita que se dicte resolución por medio de la cual señale el archivo del procedimiento.

Subsidiariamente apercibimiento y, en última instancia, se modere o module la propuesta recogida en el Acuerdo de Inicio

OCTAVO: Con fecha 27 de abril de 2023, el instructor del procedimiento acordó practicar las siguientes pruebas: *<<1. Se dan por reproducidos a efectos probatorios la reclamación interpuesta por D. **A.A.A.** 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 DIGI SPAIN TELECOM, S.L., y la documentación que a ellas acompaña>>*.

NOVENO: Con fecha 31 de mayo de 2023 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos se sancione a DIGI SPAIN TELECOM, S.L., con NIF B84919760, por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 a) del RGPD, la sanción que correspondería sería una multa por un importe de 70.000 euros (setenta mil euros).

DÉCIMO: Notificada la propuesta de resolución, presentó escrito de alegaciones el 19 de junio de 2023 en el que, en síntesis, se aduce que se reitera en las alegaciones previamente presentadas, y que en el informe emitido por la Agencia de Ciberseguridad de la Unión Europea ratifica que, para realizar un duplicado fraudulento de SIM, el estafador necesita tener acceso a algunos de los datos personales de la víctima, cliente del operador. Es decir, que los ciberdelincuentes, cuentan con datos personales de sus víctimas con carácter previo a acudir ante el Operador de Red Móvil.

Señala, que esto es lo que ocurrió en el presente supuesto, la víctima perdió el control sobre sus datos personales en favor del suplantador de forma previa a que éste contactase con DIGI. "*Es decir, es a través del ataque de "phishing" donde las víctimas, en este caso, el Reclamante y su cónyuge, pierden el control sobre sus datos de carácter personal, y es este hecho el que desencadena y posibilita la comisión del fraude".*

Es por ello que la parte reclamada considera que la Propuesta no es ajustada a derecho, pues impone a DIGI una obligación de resultado, consistente en el establecimiento de medidas infalibles sobre unos riesgos que le son impuestos por terceros que, de manera unilateral, han decidido externalizar, sin la aquiescencia de DIGI, sus propias obligaciones de seguridad como responsables del tratamiento. Llegando a imputar una infracción del artículo 6.1 del RGPD basándose únicamente en el resultado lesivo que se produce por la intervención fraudulenta de un tercero que supera las medidas de seguridad, sin atender a la diligencia utilizada, y sin considerar el despliegue de medidas técnicamente adecuadas e implantadas sobre un tratamiento para el cual DIGI no decide ni la finalidad ni los medios.

Sobre la falta de proporcionalidad de la sanción propuesta y que previos los trámites oportunos se dicte resolución por medio de la cuál señale el archivo del procedimiento EXP202213029.

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

HECHOS PROBADOS

1º. El reclamante formuló reclamación ante esta Agencia en fecha 27 de octubre de 2022, en la que se hace constar que a las 10:30 de la mañana del día 26 de octubre de 2022 su teléfono móvil ******TELÉFONO.1*** se quedó sin servicio tras lo cual recibió un email de DIGI explicándole que con su número había sido activada una segunda tarjeta SIM.

2º DIGI manifestó que, con fecha 25 de octubre de 2022, un tercero que se identifica como el reclamante solicitó un duplicado de tarjeta SIM para la línea móvil ******TELÉFONO.1,*** a través del estand de DIGI ubicado en un centro comercial, exhibiendo el DNI con el número del reclamante y el distribuidor de DIGI procedió a gestionar la solicitud del duplicado de la tarjeta.

Ulteriormente, al contactar el reclamante con DIGI procedió primero a suspender la línea y posteriormente el día 26 de octubre de 2022 la recuperó.

3º DIGI manifestó que, el día 26 de octubre de 2022, el servicio de atención telefónica de DIGI recibió una nueva llamada de un tercero que se identificó como el reclamante y al tratar de confirmar su identidad finaliza la llamada. DIGI dejó registrada dicha incidencia y contactó con el reclamante, para establecer una palabra clave de seguridad para poder solicitar un duplicado de la tarjeta SIM.

4º DIGI manifestó que, el día 26 de octubre recibió en otro establecimiento distinto del primero una tercera solicitud de duplicado de tarjeta SIM, para la línea ******TELÉFONO.1***. Allí proceden a expedir la tarjeta SIM a dicho tercero que no era el titular de la línea.

5º La línea estuvo activada de forma irregular desde las 16:30 horas hasta las 17:44 horas del mismo día, momento en el que el agente de DIGI procede a la suspensión del servicio.

4º El reclamante contactó de nuevo con DIGI, le facilitaron otra SIM la cual recogió en una tienda física de su localidad al igual que la primera y en la que tuvo que identificarse con su DNI original, pero en ningún momento le pidieron el filtro que se estableció el de facilitar la clave para autorizar y facilitarle la tarjeta SIM.

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

Obligación Incumplida

Se imputa a la parte reclamada la comisión de una infracción por vulneración del artículo 6 del RGPD, "*Licitud del tratamiento*", que señala en su apartado 1 los supuestos en los que el tratamiento de datos de terceros es considerado lícito:

"1. El tratamiento sólo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

En respuesta a las alegaciones presentadas por DIGI se debe señalar lo siguiente:

En cuanto a que la suplantación de identidad y el acceso a los datos del titular de forma ilegítima se produce forma previa a tener contacto con DIGI y es la causa que provoca la incidencia y la emisión del duplicado de la tarjeta SIM. En consecuencia, no resulta posible asociar a DIGI la realización de un tratamiento no legitimado de datos personales, dado que su actuación se reduce al cumplimiento de sus procesos y obligaciones.

Efectivamente, 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.

Pues bien, DIGI ha facilitado un duplicado de la tarjeta SIM a un tercero distinto del legitimo titular de la línea móvil, tras la superación por terceras personas 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 DIGI 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.

En cuanto a la responsabilidad de DIGI, debe indicarse que, con carácter general DIGI 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.

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, DIGI cuenta con una red de comerciales, puntos de venta y distribuidores homologados a través de un contrato de distribución para ofrecer los servicios de DIGI. 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 cuanto al incumplimiento del principio de proporcionalidad, el RGPD prevé expresamente la posibilidad de graduación, mediante la previsión de multas susceptibles de modulación, en atención a una serie de circunstancias de cada caso individual.

En cuanto a la imposición de una advertencia, apercibimiento, o la adopción de medidas correctivas conforme al artículo 58 del RGPD, una multa disuasoria es aquella que tiene un efecto disuasorio genuino. A este respecto, la Sentencia del TJUE, de 13 de junio de 2013, Versalis Spa/Comisión, C-511/11, ECLI:EU:C:2013:386, dice:

"94.Respecto, en primer lugar, a la referencia a la sentencia Showa Denko/Comisión, antes citada, es preciso señalar que Versalis la interpreta incorrectamente. En efecto, el Tribunal de Justicia, al señalar en el apartado 23 de dicha sentencia que el factor disuasorio se valora tomando en consideración una multitud de elementos y no sólo la situación particular de la empresa de que se trata, se refería a los puntos 53 a 55 de las conclusiones presentadas en aquel asunto por el Abogado General Geelhoed, que había señalado, en esencia, que el coeficiente multiplicador de carácter disuasorio puede tener por objeto no sólo una «disuasión general», definida como una acción para desincentivar a todas las empresas, en general, de que cometan la infracción de que se trate, sino también una «disuasión específica», consistente en disuadir al demandado concreto para que no vuelva a infringir las normas en el futuro. Por lo tanto, el Tribunal de Justicia sólo confirmó, en esa sentencia, que la Comisión no estaba obligada a limitar su valoración a los factores relacionados únicamente con la situación particular de la empresa en cuestión."

"102. Según reiterada jurisprudencia, el objetivo del factor multiplicador disuasorio y de la consideración, en este contexto, del tamaño y de los recursos globales de la empresa en cuestión reside en el impacto deseado sobre la citada empresa, ya que la sanción no debe ser insignificante, especialmente en relación con la capacidad financiera de la empresa (en este sentido, véanse, en particular, la sentencia de 17 de junio de 2010, Lafarge/Comisión, C-413/08 P, Rec. p. I-5361, apartado 104, y el auto de 7 de febrero de 2012, Total y Elf Aquitaine/Comisión, C-421/11 P, apartado 82)."

Hemos de atender a la circunstancia singular de la reclamación presentada, a través de la cual puede constatarse que, desde el momento en el que la persona suplantadora realiza la sustitución de la SIM, el teléfono de la víctima se queda sin servicio pasando el control de la línea a las personas suplantadoras. En consecuencia, ven afectados sus poderes de disposición y control sobre sus datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos según ha señalado el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre de 2000 (FJ 7). De manera que, al conseguir un duplicado de la tarjeta SIM, se posibilita bajo determinadas circunstancias, el acceso a los contactos o a las aplicaciones y servicios que tengan como procedimiento de recuperación de clave el envío de un SMS con un código para poder modificar las contraseñas. En definitiva, podrán suplantar la identidad de los afectados, pudiendo acceder y controlar, por ejemplo: las cuentas de correo electrónico; cuentas bancarias; aplicaciones como WhatsApp; redes sociales, como Facebook o Twitter, y un largo etc. En resumidas cuentas, una vez modificada la clave de acceso por parte de los suplantadores pierden el control de sus cuentas, aplicaciones y servicios, lo que supone una gran amenaza.

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

DIGI cita en su descargo una serie de resoluciones dictadas por la AEPD, manifestando que en contraposición a la sanción impuesta a DIGI, se le impone a otra operadora de telecomunicaciones, por una infracción del artículo 5.1.f) del RGPD. y calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD, una multa administrativa por importe de 200.000 euros (doscientos mil

euros).

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 la operadora de telecomunicaciones, 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.

El procedimiento sancionador PS/000027/2021, tramitado contra la otra operadora se le imputó la violación del artículo 5.1f), no se le imputa el fraude, ni el tratamiento de datos sin legitimación sino una falta de garantías de las medidas de seguridad que produce una cesión de datos a un tercero.

En el presente procedimiento sancionador, la sanción se impone debido a que DIGI 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 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.

En el presente caso, resulta acreditado que se produjeron dos duplicados fraudulentos, con fechas 25 y 26 de octubre de 2022, la operadora DIGI tramitó la emisión de dos duplicados fraudulentos de la tarjeta SIM de la línea ******TELÉFONO.1***, perteneciente a la parte reclamante.

El primero de los duplicados fraudulentos, se llevó a cabo el día 25 de octubre de 2022, a las 19:39 horas, con la presentación de un documento nacional de identidad que no se corresponde con el original de la parte reclamante.

El 26 de octubre de 2022 el reclamante contacta con DIGI informando de la suplantación de identidad. DIGI procedió a bloquear la línea y se abrió un ticket interno por posible caso de usurpación de identidad, añadiendo al ID del reclamante la siguiente anotación: *"Se ha utilizado un duplicado de SIM fraudulento para este cliente, hemos añadido DNI real al ID//Porfavor revisar DNI antes de validar duplicado"*

El segundo de los duplicados fraudulentos se llevó a cabo el 26 de octubre de 2022, a las 16:19 horas, con la presentación de un documento nacional de identidad que no se corresponde con el original de la parte reclamante. El asesor que tenía asignada esta validación, no llevo a cabo ninguna de las comprobaciones que correspondían y procedió a validar la nueva solicitud.

Ahora bien, debe señalarse que el Sim Swapping es un fraude que permite suplantar la identidad mediante el secuestro del número de teléfono al obtener un duplicado de la tarjeta SIM.

En todo caso, la operadora deberá ser capaz de acreditar que para este caso concreto

haya seguido los protocolos de verificación implementados a la hora de solicitar un duplicado de la tarjeta SIM.

Pues bien, el resultado fue que DIGI expidió la tarjeta SIM a un tercero que no era el titular de la línea.

A la vista de lo anterior, DIGI no logra acreditar que se haya seguido ese procedimiento.

De hecho, conforme al procedimiento de identificación descrito por la parte reclamada, debió haberse comprobado el original del documento identificativo, siendo así que, de haberse efectuado correctamente esta operación, el duplicado debió haber sido denegado.

En definitiva, DIGI reconoce tanto en su escrito de contestación al requerimiento de esta Agencia de fecha 2 de febrero de 2023, como en el de las alegaciones al Acuerdo de Inicio de este procedimiento de fecha 26 de abril de 2023 dichos hechos, manifestando al respecto: *"La mencionada suplantación de identidad, en el primer duplicado de SIM presuntamente fraudulento que se ha relatado en los hechos de este caso, solo pudo producirse a partir de la elaboración y posterior uso, por parte del suplantador, de un documento de identidad con apariencia de original, pero presuntamente falsificado, que se remitió a DIGI para la validación de dicho primer duplicado.*

En el caso del segundo duplicado presuntamente fraudulento, el mismo solo fue posible habiéndose aprovechado el usurpador de la negligencia del asesor de DIGI que validó dicho duplicado, el cual debió cumplir, y no cumplió, con sus obligaciones, y debió haber seguido, y no lo hizo, el procedimiento que DIGI tiene implantado para la validación de duplicados".

En consecuencia, tal como reconoce DIGI: *"el asesor al que se asignó la tarea no siguió el procedimiento que DIGI tiene establecido internamente (y respecto al cual todos sus asesores de BackOffice están informados y formados) para la validación de duplicados SIM conforme al procedimiento actualmente vigente en DIGI.*

Cabe mencionar que este procedimiento, como no puede ser de otra forma, implica, entre otras cosas, la obligación del asesor de DIGI de (1) revisar toda la documentación asociada al ID de la línea para la cual se está solicitando un duplicado, incluyendo los tickets y observaciones que figuran en dicho ID; (2) comprobar si existen solicitudes de duplicado previas, que puedan constituir un indicio de que el titular pudiera estar siendo víctima de algún tipo de fraude por suplantación; y (3) contactar con el cliente para confirmar la palabra clave que este hubiera puesto como medida de seguridad para evitar duplicados no autorizados.

Desafortunadamente, en este caso, por una negligencia, el asesor que tenía asignada esta validación, no llevo a cabo ninguna de estas comprobaciones, incumpliendo sus obligaciones laborales, y procedió a validar la nueva solicitud de duplicado, siendo el mismo activado a las 16:30 horas del 26 de octubre de 2022, enviándose el correspondiente SMS informativo".

Por lo que atañe, a la presentación del DNI por el solicitante del duplicado de la tarjeta SIM en los puntos de venta de DIGI, cuya copia ha aportado la operadora, con apariencia legítima pero claramente falso al compararlo con el original, el cual consta en los sistemas de DIGI. El DNI falso incluye una persona completamente distinta, lugar de nacimiento distinto, padres distintos, fecha de nacimiento distinta, etc, sin que sea posible confundirlos.

En todo caso, la parte reclamada no ha sido capaz de acreditar que para este supuesto se siguiera el procedimiento implantado por ella misma, ya que, de haberlo hecho, se debió haber producido la denegación del duplicado de la tarjeta SIM.

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."*

III

Tipificación y calificación de la infracción

La infracción se tipifica en el artículo 83.5 del RGPD, que considera como tal:

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

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

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

IV

Sanción de multa. Determinación del importe.

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

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

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

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

b) la intencionalidad o negligencia en la infracción;

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

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

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

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

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

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

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

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

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

Dentro de este apartado, la LOPDGDD contempla en su artículo 76, titulado *"Sancio-*

nes 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."

Digi solicita que se aprecien las siguientes circunstancias atenuantes:

(I) *"la inexistencia de infracciones previas"* (art. 83.2 e) RGPD).
(II) *"En ningún momento se han tratado categorías especiales de datos"* (art. 83.2 g).
(III) "*la cooperación con la autoridad de control al haber contestado al traslado de la reclamación y haber facilitado la información* solicitada*",* artículo 83.2 f) del RGPD.
(IV) "*La inexistencia* de beneficios obtenidos a través de la infracción", artículo 83.2 k) del RGPD y 76.2 c) de la LOPDGDD.

No se admite ninguna de las circunstancias invocadas.

Respecto a la (I) y (II), cabe señalar que tales circunstancias solo pueden operar como agravantes y en ningún caso como circunstancias atenuantes.

El pronunciamiento que hace la Audiencia Nacional en su SAN de 5 de mayo de 2021 (Rec. 1437/2020) sobre el apartado e) del artículo 83.2. del RGPD, la comisión de infracciones anteriores:

> "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante";*

(III)El artículo 83.2.f) del RGPD se refiere al *"grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;".* La respuesta de la reclamada al requerimiento informativo de la Subdirección de Inspección no cumplía esas finalidades, por lo que no es encuadrable en esa circunstancia atenuante.

(IV) Sobre la aplicación del artículo 76.2.c) de la LOPDGDD, en conexión con el artículo 83.2.k), inexistencia de beneficios obtenidos, cabe señalar que tal circunstancia solo puede operar como agravante y en ningún caso como circunstancia atenuante.

El artículo 83.2.k) del RGPD se refiere a "*cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."* Y el artículo 76.2c) de la LOPDGDD dice que *"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta: [..] c) Los beneficios obtenidos como consecuencia de la comisión de la infracción."* Ambas disposiciones mencionan como factor que puede tenerse en cuenta en la graduación de la sanción los "*beneficios"* obtenidos, pero no la "*ausencia"* de éstos, que es lo que DIGI alega.

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

La Sala de lo Contencioso Administrativo de la Audiencia Nacional ha advertido que, el hecho de que en un supuesto concreto no estén presentes todos los elementos que integran una circunstancia modificativa de la responsabilidad que, por su naturaleza, tiene carácter agravante, no puede llevar a concluir que tal circunstancia es aplicable en calidad de atenuante. El pronunciamiento que hace la Audiencia Nacional en su

SAN de 5 de mayo de 2021 (Rec. 1437/2020) -por más que esa resolución verse sobre la circunstancia del apartado e) del artículo 83.2. del RGPD, la comisión de infracciones anteriores- es extrapolable a la cuestión planteada, la pretensión de la reclamada de que se acepte como atenuante la "*ausencia"* de beneficios siendo así que tanto el RGPD como la LOPDGDD se refieren solo a "*los beneficios obtenidos*":

> "*Considera, por otro lado, que debe apreciarse como atenuante la no comisión de una infracción anterior. Pues bien, el artículo 83.2 del RGPD establece que debe tenerse en cuenta para la imposición de la multa administrativa, entre otras, la circunstancia "e) toda infracción anterior cometida por el responsable o el encargado del tratamiento". Se trata de una circunstancia agravante, el hecho de que no concurra el presupuesto para su aplicación conlleva que no pueda ser tomada en consideración, pero no implica ni permite, como pretende la actora, su aplicación como atenuante";*

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 solventar la incidencia objeto de reclamación de forma efectiva (art. 83.2 c).

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en su artículo 6.1 del RGPD permite fijar una sanción de 70.000 euros (setenta mil euros).

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 DIGI SPAIN TELECOM, S.L., con NIF B84919760, 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 DIGI SPAIN TELECOM, S.L.

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