- **Expediente N.º: EXP202202150**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes:

ANTECEDENTES

PRIMERO: Dña. ***A.A.A.*** (en adelante, la parte reclamante) con fecha 11 de enero 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, la parte reclamada o DIGI). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que el día 7 de enero de 2022 el servicio de su línea móvil ******TELEFONO.1*** no funcionaba, y la parte reclamada le informó que con sus datos se había solicitado un duplicado de la tarjeta SIM.

Tras informar la reclamante durante esa llamada que ella no había contactado con DIGI, ni había solicitado la emisión de un duplicado de su tarjeta SIM, DIGI procedió a cancelar la emisión del duplicado SIM, y a restablecer el funcionamiento de la SIM original que estaba en poder de la reclamante.

Pues bien, el día 9 de enero de 2022, volvió a quedarse sin línea móvil, por haberse solicitado un nuevo duplicado de la tarjeta SIM para su línea de móvil ******TELEFONO.1***.

Posteriormente, pudo comprobar cómo el suplantador había entrado en su cuenta bancaria, haciendo uso de la misma.

Interpuso denuncia ante la Policía Nacional de Logroño el día 8 de enero de 2022 y sus correspondientes ampliaciones, ante los hechos ocurridos el día 9 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 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 21 de febrero de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 22 de marzo de 2022 se recibe en esta Agencia escrito de respuesta indicando que han verificado la existencia de una solicitud de duplicado de tarjeta SIM

relativa a la línea móvil del reclamante. Dicha solicitud, efectuada con fecha 7 de enero de 2022 se realizó a través del canal que el servicio de atención al cliente que DIGI tiene habilitado vía WhatsApp.

La referida solitud fue realizada por una persona que se identificó como la reclamante, aportando sus datos personales y superando el desafío de seguridad establecido por DIGI para poder verificar la identidad del cliente.

Por motivos de seguridad procedieron al bloqueo preventivo de la anterior tarjeta SIM, ya que se había alegado su robo. El mismo día recibieron comunicación telefónica de la reclamante alegando que su línea móvil no funcionaba, tras esa comunicación y las comprobaciones efectuadas procedieron a cancelar el proceso de emisión de duplicado de SIM, y reestablecer el funcionamiento de la SIM original que estaba en poder de la reclamante. Procedieron a establecer una nota de aviso en los sistemas relativa a que la reclamante podría estar inmersa en un caso de usurpación de identidad.

Se manifiesta que por los servicios de atención al cliente existe la obligación de consultar el histórico de clientes para evitar casos similares. Se señala que las medidas adoptadas resultaron adecuadas para conseguir rechazar varios intentos de realizar un duplicado por parte del usurpado.

Sin embargo, consta que con fecha 9 de enero de 2022 en otro intento de obtención de duplicado existió un error humano en el servicio de atención y que a pesar de la nota de aviso se procedió a facilitar el código numérico necesario para tramitar el duplicado SIM.

Tras una llamada de la reclamante, ese mismo día, procedieron a desactivar dicho duplicado.

Manifiesta la entidad que no ha revelado a ningún tercero datos personales de la reclamante, desconociendo como el usurpador pudo conocer sus datos personales para superar los controles de seguridad establecidos.

Se adoptaron una serie de medidas:

Rectificación inmediata del elemento causante de la incidencia cancelando la emisión del duplicado (en el primer intento porque en el segundo se cometió un error y el trámite continuo adelante).

Se detallan las medidas adoptadas por el responsable para hacer frente a situaciones de este tipo.

TERCERO: Con fecha 6 de abril de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE)

2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

(...)

QUINTO: Con fecha 13 de diciembre 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.

SEXTO: Con fecha 27 de diciembre de 2023, DIGI solicita la ampliación del plazo legal conferido para contestar dicho requerimiento y copia del expediente.

SEPTIMO: Con fecha 19 de enero 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 DIGI no ha puesto a disposición de los presuntos delincuentes información personal de la reclamante distinta de la que ya tenían aquellos con anterioridad, tras haberlos obtenido a través del correo electrónico.

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, DIGI manifiesta que queda acreditado que la suplantación de identidad y el acceso a los datos de la reclamante de forma ilegitima se produce mediante una llamada telefónica al servicio de atención al cliente, de forma previa a tener contacto con DIGI, el supuesto suplantador tenía en su poder los datos personales de la reclamante, incluyendo su cuenta bancaria (lo que le permitió, así mismo, acceder a ella).

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.

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 19 de enero de 2023, el instructor del procedimiento acordó practicar las siguientes pruebas: 1. Se dan por reproducidos a efectos probatorios la reclamación interpuesta por Dña. ***A.A.A.*** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento. 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 13 de febrero 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, la parte reclamada solicitó ampliación de plazo para formular alegaciones que le fue concedido, presentó escrito de alegaciones el 6 de marzo 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 la víctima

pierde el control sobre sus datos de carácter personal, y es este hecho el que desencadena y posibilita la comisión del fraude.

Asimismo, manifiesta que ha de tenerse en cuenta que DIGI no participa del proceso de identificación de un usuario ante su banco, sino que éste quien determina el modo en que quiere llevar a cabo esta comprobación, por lo que no cabe trasladar la responsabilidad ante las operadoras de telefonía.

Igualmente, indican que 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, al 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, sin atender a la diligencia utilizada y sin considerar el despliegue de medidas técnicamente adecuadas e implantadas.

DIGI no puede prever ni saber cuál es el deber de diligencia aplicable.

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 nº EXP202202150.

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 formuló reclamación ante esta Agencia el día 11 de enero de 2022, en la que se hace constar que el día 7 de enero de 2022, el servicio de la línea móvil de la reclamante no funcionaba, y DIGI le informó que se había solicitado un duplicado de la tarjeta SIM de su línea móvil. DIGI canceló la emisión del citado duplicado, y procedió a establecer una nota de aviso en los sistemas el citado día relativa a que la reclamante podría estar inmersa en un caso de usurpación de identidad.

El día 9 de enero de 2022, volvió a quedarse sin servicio en su línea móvil, por haberse solicitado un nuevo duplicado de su tarjeta SIM y el suplantador entró en su cuenta bancaria, haciendo uso de la misma.

SEGUNDO. - DIGI acredita, que la parte reclamante se quedó sin línea móvil los días 7 y 9 de enero de 2022. Consta que el día 7 de enero DIGI canceló la emisión del duplicado y alertó de dicha circunstancia en sus sistemas.

TERCERO. - DIGI acredita, las siguientes incidencias el día 9 de enero de 2022:

- Chat correspondiente al desafío de seguridad de un intento de solicitud del 9 de enero de 2022 a las 17:26h, en el cual desde Atención al Cliente se le indica que no se puede proceder por esa vía a gestionar la solicitud y que debe remitir documento de identidad para realizarla, manifestando los representantes de la

parte reclamada que se rechazó al existir una anotación anterior en el histórico del cliente de suplantación de identidad.

- Un tercero contactó el día 9 de enero de 2022 con su servicio de atención al cliente, vía telefónica, solicitando la emisión de un duplicado de la tarjeta SIM de la reclamante y procedió a emitir un código de solicitud de duplicado de la tarjeta SIM, ese mismo día el tercero se presentó en un punto de distribución de DIGI. Allí procedieron a expedir la tarjeta SIM a dicho tercero que no era el titular de la línea, y que en esta ocasión se produjo un error humano por la asesora telefónica, la cual, a pesar de la nota de aviso reflejada en los sistemas y tras aportar la supuesta usurpadora los datos necesarios para superar el desafío de seguridad autorizaron el duplicado de la tarjeta SIM.

CUARTO. - El duplicado se emitió en el establecimiento de un distribuidor de DIGI, el día 9 de enero de 2022 a las 18:46 horas, y al ponerse en contacto la reclamante con el servicio de atención al cliente, procedió DIGI a desactivar el duplicado SIM fraudulento y al día siguiente la reclamante contactó con la compañía para solicitar la baja de todos sus servicios.

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".

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"*.

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

En cuanto a que DIGI no ha puesto a disposición de los presuntos delincuentes información personal de la parte reclamante distinta de la que ya tenían aquellos con anterioridad. En consecuencia, no se ha producido un tratamiento no legitimado de datos personales.

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.

Cabe colegir que DIGI ha facilitado un duplicado de tarjeta SIM a un tercero distinto del legitimo titular de la línea móvil, tras la superación por tercera persona de la política de seguridad existente, lo que evidencia un incumplimiento del deber de proteger la información de los clientes.

Negar la concurrencia de una actuación negligente por parte de 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 que los delincuentes no han conseguido obtener datos personales de DIGI, por lo que no puede hablarse de incumplimiento de medidas de protección, señalar que el acceso al duplicado de una tarjeta SIM que hace identificable a su titular, responde a la definición de dato personal del artículo 4.1) del RGPD.

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.

En el presente caso, resulta acreditado que con fechas 7 y 9 de enero de 2022 DIGI tramitó la emisión de duplicados de la tarjeta SIM de la línea ******TELEFONO.1***, perteneciente a la parte reclamante.

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 la reclamada 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.

Pues bien, entre los dos duplicados emitidos se rechazó otro intento de autorización de duplicado a través del canal que el servicio de atención al cliente de DIGI tiene habilitado vía WhatsApp. No obstante, a pesar de la existencia de la anotación de aviso se autorizó el segundo duplicado de fecha 9 de enero de 2022, por error humano del gestor. 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.

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.

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 de multa. Determinación del importe.

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

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

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

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

b) la intencionalidad o negligencia en la infracción;

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

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

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

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

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

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

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

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

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

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

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

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

a) El carácter continuado de la infracción.

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

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

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

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

f) La afectación a los derechos de los menores.

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

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

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 atenuantes invocadas.

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