

- **Expediente nº.: EXP202311911**

### RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por DIGI SPAIN TELECOM, S.L.U. (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 8 de noviembre de 2024, y en base a los siguientes:

#### HECHOS

PRIMERO: Con fecha 8 de noviembre de 2024, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202311911, en virtud de la cual se imponía a DIGI SPAIN TELECOM, S.L.U., por una infracción del Artículo 6.1 del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa por un importe de 200.000 euros (doscientos mil euros).

Dicha resolución, que fue notificada a la parte recurrente en fecha 11 de noviembre de 2024, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador quedó constancia de los siguientes:

PRIMERO. – El día 6 de abril de 2021, un tercero se personó ante un punto de venta de DIGI para la realización de un duplicado de la tarjeta SIM del reclamante,

SEGUNDO. – De los dos pantallazos del sistema de DIGI aportados el día 11 de octubre de 2023 en contestación a la solicitud de información de esta Agencia a la parte reclamada y que consta en el expediente se desprende la emisión de dos duplicados de tarjeta SIM del reclamante.

- En el primero de ellos, consta que el duplicado de la tarjeta SIM se realizó el día 6 de abril de 2021 a las 14:21 en un punto de venta de DIGI, quedando el reclamante sin línea.

- En el segundo de ellos, consta que se realizó un nuevo duplicado de SIM de forma que el inicial duplicado quedó inactivo, el día 6 de abril de 2021 a las 16:47 horas, recuperando la línea el reclamante.

TERCERO. – De las impresiones de pantalla aportadas por DIGI, con fecha 11 de octubre de 2023, consta que el proceso de verificación de la identidad del solicitante aplicado al presente caso vigente al momento de los hechos, para la obtención de un duplicado de tarjeta SIM, era el siguiente:

(...)

TERCERO: La parte recurrente ha presentado en fecha 11 de diciembre de 2024, en esta Agencia Española de Protección de Datos, recurso de reposición, fundamentándolo, básicamente, en que la parte recurrente considera que de los hechos acreditados resulta posible concluir que DIGI contaba con un procedimiento al efecto, el cual se siguió escrupulosamente, y que le permitió realizar, conforme sus obligaciones, un tratamiento de datos lícito.

Por otra parte, DIGI manifiesta que extrema sus esfuerzos por identificar y mitigar los intentos de fraude, y no puede imponérsele una responsabilidad absoluta en la detección del mismo; ante un tercero que dispone de los datos telefónicos, identificativos y de los datos bancarios del reclamante, que cumple el protocolo.

Además, señala que la AEPD se basa únicamente en el resultado.

Asimismo, DIGI alega que la AEPD le impone inequívocamente una responsabilidad objetiva, en la cual, independientemente de la diligencia y medidas desplegadas, se declara la culpabilidad de la entidad.

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 EXP202311911, y reseña sanciones impuestas a otras empresas del sector telecomunicaciones con motivo de la concurrencia de los fraudes de tipología Sim Swapping.

Digi solicita que se aprecien las siguientes circunstancias atenuantes:

Procedió la parte reclamada a solventar la incidencia objeto de reclamación de forma efectiva (art. 83.2 c RGPD).

Que en ningún momento se han tratado categorías especiales de datos (Art.83.2g) RGPD).

El grado de cooperación de DIGI con la AEPD.

El inexistente beneficio obtenido por parte de DIGI (art. 83.2 k) RGPD).

Subsidiariamente, en el caso de que la AEPD resuelva en contra de la fundamentación jurídica que sostiene DIGI, se solicita a la AEPD que culmine el procedimiento mediante un apercibimiento y, en última instancia, se modere o module la sanción recogida en la Resolución notificada a DIGI.

## FUNDAMENTOS DE DERECHO

### I

#### Competencia

Es competente para resolver el presente recurso la Presidencia de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123

de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD).

## II

### Contestación a las alegaciones presentadas

En relación con las manifestaciones efectuadas por la parte recurrente, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho II al V, de la Resolución recurrida, tal como se transcribe a continuación:

#### <<II

### Contestación a las alegaciones presentadas

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

*La intervención fraudulenta de un tercero, lo que ha revelado es el deficiente análisis de los riesgos, así como la insuficiente implantación, revisión y control de las medidas de seguridad por parte de la operadora. Tercero ajeno al titular de los datos ha superado las medidas de seguridad establecidas por DIGI. Esto nos muestra que la identificación del titular de los datos no se producía con las suficientes garantías, independientemente de que la identificación se realizara por el propio titular o por un tercero de forma fraudulenta.*

*En suma, una falta de medidas de seguridad apropiadas y un incumplimiento de las obligaciones derivadas de la responsabilidad proactiva, máxime cuando los "errores" persisten en el tiempo.*

*Al respecto hay que señalar que precisamente el que nos encontremos ante el fraude de un tercero hace que sea necesario asegurarse que la persona a la que se expide el duplicado de la tarjeta SIM es quien realmente dice ser y deben adoptarse las medidas necesarias de prevención adecuadas para verificar la identidad de una persona cuyos datos van a ser objeto de tratamiento tal y como se reconoce en el Fundamento Jurídico Séptimo de la SAN, SCA, de 5 de mayo de 2021 ("Por otro lado, en cuanto al hecho de que nos encontramos ante el fraude de un tercero, como dijimos en la SAN de 3 de octubre de 2013 (Rec. 54/2012) -: " Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento...").*

*A lo largo del presente procedimiento DIGI ha manifestado reiteradamente que los duplicados fraudulentos de las tarjetas se han producido tras haber superado los defraudadores su política de seguridad. Considera que es inevitable que a pesar de la existencia de la política de seguridad pueda haber casos en los que a través de ciertos mecanismos dicha política de seguridad pueda ser sobrepasada de forma fraudulenta sin que por ello pueda existir reproche a DIGI.*



*Sin embargo, ha quedado probado que la política de seguridad de DIGI ha resultado insuficiente para la adecuada protección de los derechos fundamentales de la parte reclamante cuya tarjeta SIM ha sido fraudulentamente duplicada.*

*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 y que, 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.*

*No obstante, para poder realizar dichas operaciones a través del teléfono móvil, resulta necesario poder tener acceso al mismo y uno de los medios es, precisamente la obtención de un duplicado de tarjeta. Cuando dicho duplicado se expide a un tercero distinto del de su titular 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.*

*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.*

*En el presente caso, cabe colegir que DIGI ha facilitado un duplicado de tarjeta SIM a un tercero distinto del legítimo titular de la línea móvil, tras la superación por tercera persona de la política de seguridad existente.*

*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".*

*En cuanto a que los delincuentes no han conseguido obtener datos personales a través de DIGI, por lo que no puede hablarse de incumplimiento de medidas de protección, no puede considerarse cierto. Resulta necesario 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.*



*Por lo que respecta 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.*

*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 transcrita 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, cuya concurrencia fue debidamente motivada en el acuerdo de inicio del presente procedimiento.*

*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.*

### III

#### Obligación Incumplida

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

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

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
- f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".*

*La emisión de un duplicado de tarjeta SIM implica necesariamente un tratamiento de datos personales, ya que se realiza sobre la línea y la identidad del titular. Dicho tratamiento debe cumplir con una base jurídica que lo legitime, tal como exige el citado artículo 6.1 del RGPD.*

*En este caso, la emisión del duplicado SIM a solicitud de un tercero sin la intervención o consentimiento del titular constituye una falta de base jurídica válida para dicho tratamiento de datos. Aunque DIGI alega seguir sus propios protocolos, esto no es suficiente para justificar la licitud del tratamiento bajo el RGPD, ya que dichos protocolos no suplen la necesidad de la concurrencia de una base legítima.*

*El procedimiento de verificación de identidad descrito por DIGI, que se basa únicamente en la coincidencia de ciertos datos en su base de datos, no garantiza adecuadamente el cumplimiento del RGPD en tanto:*

- *No acredita la intervención efectiva del titular de los datos en el proceso.*
- *La mera coincidencia de los datos no asegura el consentimiento ni ninguna otra base jurídica del artículo 6.1 que legitime el tratamiento.*

*Por lo tanto, la emisión del duplicado SIM en estas condiciones constituye un tratamiento de datos personales sin base jurídica y, en consecuencia, una infracción del artículo 6.1 del RGPD, dado que se ha realizado sin cumplir con ninguna de las bases legitimadoras para dicho tratamiento. La responsabilidad no reside en la falta de cumplimiento de un protocolo interno de DIGI, sino en la ausencia de una base jurídica válida conforme a las disposiciones del RGPD.*

*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 lo que constituye una 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.”*

*Por lo expuesto, se considera que DIGI ha vulnerado el artículo 6.1 del RGPD*

#### IV

#### *Tipificación y calificación de la infracción*

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

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

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

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

## V

*Sanción de multa. Determinación del importe*

*A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:*

*“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.”*

*“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.”*



Respecto al apartado k) del artículo 83.2 del RGPD, la LOPDGDD, artículo 76, "Sanciones y medidas correctivas", dispone:

"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."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de multa a imponer a la reclamada, como responsable de una infracción tipificada en el artículo 83.5.a) del RGPD, se estiman concurrentes los siguientes factores:

DIGI solicita que se aprecien las siguientes circunstancias atenuantes:

- (I) "Procedió la parte reclamada a solventar la incidencia objeto de la reclamación de forma efectiva" (art. 83.2 c) 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.

La admisión de que opere como una atenuante que la parte reclamada ha solventado la incidencia objeto de reclamación de forma efectiva (artículo 83.2 c) del RGPD), 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. En el presente caso, la resolución de la incidencia no se lleva a cabo por la propia iniciativa de DIGI ni porque esta entidad hubiese advertido el fraude por sí misma, sino



*por la intervención del propio reclamante que, al verse sin servicio, se persona en otro punto de venta para activarlos nuevamente. En ese momento se le entrega un nuevo duplicado de la tarjeta SIM que conlleva la anulación de la anterior obtenida fraudulentamente.*

*El artículo 83.2g) del RGPD se refiere “En ningún momento se han tratado categorías especiales de datos”.*

*Los datos tratados por DIGI, son datos de naturaleza sensible, para identificar a sus clientes en las gestiones que realizan para la obtención del duplicado de la tarjeta SIM son el nombre, apellidos y DNI, son datos personales asociada a una línea de telefonía titular de un usuario, que se obtiene con la finalidad de suplantar su personalidad que se trata de un dato personal cuyo acceso no autorizado es particular grave. Ello, sin perjuicio, de que para la expedición del duplicado de la citada tarjeta se han tratado datos de carácter personal tales como el nombre y apellidos y DNI del titular.*

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

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

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

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

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

- *La circunstancia del artículo 83.2 e) RGPD: “Toda infracción anterior cometida por el responsable o el encargado del tratamiento”.*

*El considerando 148 del RGPD señala que “A fin de reforzar la aplicación de las normas del presente Reglamento [...]” e indica a ese respecto que “Debe no obstante, prestarse especial atención a [...] o a cualquier infracción anterior pertinente [...]”.*

*Así pues, conforme al apartado e) del artículo 83.2. RGPD, en la determinación del importe de la sanción de multa administrativa no podrán dejar de valorarse todas aquellas infracciones anteriores del responsable o del encargado de tratamiento en aras a calibrar la antijuricidad de la conducta analizada o la culpabilidad del sujeto infractor.*

*Además, una correcta interpretación de la disposición del artículo 83.2.e) RGPD no puede obviar la finalidad perseguida por la norma: decidir la cuantía de la sanción de multa administrativa en el caso individual planteado atendiendo siempre a que la sanción sea proporcional, efectiva y disuasoria.*

*Son numerosos los procedimientos sancionadores tramitados por la AEPD en los que la reclamada ha sido sancionada por la infracción del artículo 6.1 RGPD:*

*i. EXP 202104009 Resolución dictada el 15 de marzo de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.*

*ii. EXP202201226. Resolución dictada el 14 de marzo de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.*

*iii. EXP202204881 Resolución dictada el 2 de junio de 2023 en la que se impuso una sanción de 70.000 euros. Los hechos versaron sobre un duplicado de la tarjeta SIM fraudulento sin legitimación.*

- *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 actividad empresarial de la reclamada trata necesariamente datos personales, siendo una compañía de telecomunicaciones muy importante en España. Esta característica de su actividad empresarial repercute, reforzándola, en la diligencia que debe desplegar en el cumplimiento de los principios que presiden el tratamiento de datos de carácter personal y en la calidad y eficacia de las normas técnicas y organizativas que debe tener implementadas para garantizar el respeto del derecho fundamental.*

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

*Procede graduar la sanción a imponer a la reclamada y fijarla en la cuantía de 200.000 € por la infracción del artículo 83.5 a) RGPD, calificada como muy grave a efectos de la prescripción en el artículo 72.1b) de la LOPDGDD>>.*

En cuanto que la Agencia omite en su resolución, tanto el procedimiento de DIGI estipulado al efecto, como la diligencia empleada por la misma en la gestión de los intentos de comisión de fraude. A tal respecto, conviene señalar que en el presente caso la infracción no se fundamenta en la insuficiencia o adecuación de medidas de seguridad, sino en una falta de licitud en el tratamiento de los datos personales que conlleva la emisión de un duplicado de tarjeta y su entrega a un tercero, sin que el titular de la misma tuviera si quiera conocimiento de tales tratamientos.

El artículo 6.1 establece que el tratamiento de datos personales solo es lícito si se cumple al menos una de las condiciones previstas en el mencionado artículo. En este caso, la vulneración del principio de licitud se manifiesta en el tratamiento indebido de los datos personales de la parte reclamada, que no fue la solicitante real del duplicado de tarjeta.

Este tipo de trámites requiere verificar adecuadamente la identidad del solicitante y para ello resulta necesario establecer medidas que aseguren esa correcta identificación. El establecimiento de estas medidas o protocolos, así como su seguimiento y atención por la propia entidad responsable, sirve para valorar la conducta y el grado de diligencia empleado por la misma, pero no son estos los hechos determinantes de la infracción.

DIGI emitió un duplicado de tarjeta SIM sin contar con el consentimiento del titular de la línea y lo entregó a un tercero sin una base jurídica válida. Dicho hecho se traduce en un tratamiento ilícito de datos.

En síntesis, en el presente caso no se está sancionado la existencia o ausencia de medidas técnicas y organizativas, sino el hecho de que, en este caso específico, el tratamiento de los datos personales del reclamante fue llevado a cabo sin cumplir con los requisitos de licitud establecidos en el artículo 6.1 del RGPD. La infracción de este artículo confirma que la parte reclamada permitió un tratamiento no autorizado de los datos, vulnerando de esta forma los derechos de la parte reclamante.

En todo caso, las medidas implantadas por DIGI son las mínimas exigibles a cualquier organización con las características y en el contexto en el que actúa una operadora de telecomunicaciones.

En este sentido, la mera existencia de una política de seguridad no puede justificar una vulneración del principio de licitud previsto del artículo 6.1 del RGPD. Además de existir, estas medidas deben resultar efectivas y el responsable del tratamiento debe de garantizar que se cumplan estrictamente en todo momento. En caso contrario, las medidas adoptadas carecen de virtualidad y pueden conllevar tratamientos ilícitos como ocurre en el presente caso.

Por lo tanto, la parte reclamada no puede pretender quedar exonerada de su responsabilidad apelando a la existencia de medidas mínimas, menos aún cuando el fallo estuvo en la aplicación de esas medidas, permitiendo una infracción de la licitud del tratamiento.

DIGI señala que no consta ni en la reclamación, ni entre las pruebas que figuran en el expediente, que se hubiese accedido a ninguna información personal del titular de la línea como consecuencia de la puesta a disposición del duplicado de la SIM. En este sentido, dicha afirmación no exime de responsabilidad a la parte reclamada, puesto que la simple emisión de una tarjeta SIM y su entrega a un tercero no autorizado implica ya de por sí una vulneración del principio de licitud, en cuanto tienen la consideración de tratamiento de datos personales.

DIGI insiste respecto del grado de responsabilidad que, en su caso, pueda achacárseles, que no puede hacerse depender de una actuación de un tercero que escapa su control, esto es: las medidas de seguridad implementadas por una u otra entidad bancaria o incluso el hecho de que el afectado disponga o no de banca electrónica.

En relación con esta alegación, amén de lo ya indicado anteriormente, el grado de responsabilidad cae dentro de su ámbito y no de terceros, debiendo señalar que la SAN -Sala Contencioso Administrativo- de 5 de mayo de 2021, establece que: *“Por otro lado, en cuanto al hecho de que nos encontramos ante el fraude de un tercero, como dijimos en la SAN de 3 de octubre de 2013 (Rec. 54/2012)-: “ Precisamente por eso, es necesario asegurarse que la persona que contrata es quien realmente dice ser y deben adoptarse las medidas de prevención adecuadas para verificar la identidad de una persona cuyos datos personales van a ser objeto de tratamiento”.*

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.

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, de 19 de diciembre Rec 1274/1988 " (...) 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 transcrita 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 todo caso, la operadora deberá ser capaz de acreditar que los tratamientos de datos realizados cumplen el principio de licitud.

Pues bien, el resultado fue que la reclamada expidió la tarjeta SIM a petición de un tercero que no era el titular de la línea y la entregó a éste.

Sin embargo, DIGI no logra acreditar el respeto de lo establecido en el artículo 6 del RGPD.

Ni siquiera la parte reclamada no ha sido capaz de acreditar que para este supuesto se siguiera el procedimiento implantado por ella misma, quedando en entredicho la diligencia empleada por parte de la reclamada para identificar a la persona que solicitó un duplicado de la tarjeta SIM.

Digi solicita que se aprecien las siguientes circunstancias atenuantes:

(I) *“En ningún momento se han tratado categorías especiales de datos” (art. 83.2 g).*

(II) *“El grado de cooperación de DIGI con la AEPD” (art.83.2 f) RGPD)*

(III) *“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.

Sobre la aplicación del artículo 83.2 g) del RGPD, cabe señalar que las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión 2.1, adoptadas el 24 de mayo de 2023, señalan que: *“En cuanto al requisito de tener en cuenta las categorías de datos personales afectadas (artículo 83, apartado 2, letra g) del RGPD), el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por lo tanto, una respuesta más estricta en términos de multas.”*

De lo expuesto podemos concluir que no tratar categorías especiales de datos no supone una circunstancia atenuante, en todo caso se trataría de una circunstancia neutra.

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 parte reclamada se basa en la contestación a los requerimientos de la Subdirección de Inspección de la presente autoridad para considerar que concurre la mencionada

circunstancia. Sin embargo, ello no puede considerarse como cooperación voluntaria que busque activamente mitigar el impacto de la infracción, sino que se enmarca dentro de su obligación legal de responder a los requerimientos de la autoridad de control.

Según el RGPD, los responsables del tratamiento están obligados a cumplir con las solicitudes de información y a proporcionar la documentación requerida por las autoridades de control. Esta obligación es parte inherente de su responsabilidad y no constituye, en sí misma, una colaboración para remediar o mitigar los efectos de una infracción.

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

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

Por tanto, analizadas las alegaciones efectuadas en el presente recurso potestativo de reposición, se comprueba que no se han aportado en ellas nuevos argumentos jurídicos que permitan reconsiderar el sentido de la resolución sancionadora dictada en fecha 8 de noviembre de 2024.

### III Conclusión

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

### IV Resolución extemporánea

Debido a razones de funcionamiento del órgano administrativo, por ende no atribuibles a la parte recurrente, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de esta Agencia respecto al presente recurso.

De acuerdo con lo establecido en el art. 24 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el art. 21.1 de la citada LPACAP.

Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

Vistos los preceptos citados y demás de general aplicación, la Presidencia de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por DIGI SPAIN TELECOM, S.L.U. contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 8 de noviembre de 2024, en el expediente EXP202311911.

SEGUNDO: NOTIFICAR la presente resolución a DIGI SPAIN TELECOM, S.L.U.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea notificada la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº ES00 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Si la fecha de la notificación se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de

cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-020125

Lorenzo Cotino Hueso  
Presidente de la Agencia Española de Protección de Datos