- Expediente N.º: EXP202302933

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Con fecha 20 de enero de 2023, se presentó reclamación ante la Agencia Española de Protección de Datos contra DIGI SPAIN TELECOM, S.L., con NIF B84919760 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que su número de teléfono ******TELÉFONO.1***, del que es titular, fue clonado por parte de la mercantil DIGI SPAIN TELECOM, S.L.U. ("DIGI"), ya que el 4 de septiembre de 2021, sin ninguna medida de seguridad tendente a identificar fehacientemente a la persona que lo solicitó, una tercera persona, suplantando la identidad de la reclamante, solicitó la clonación del teléfono, con la finalidad de realizar llamadas a la entidad bancaria BANCO PICHINCHA ESPAÑA, S.A., y así llevar a cabo ciertas operaciones que supusieron un total 50.000 euros trasferidos de su cuenta bancaria a otras cuentas.

Aporta denuncia policial (la causa fue sobreseída provisionalmente, en fecha 24 de noviembre de 2022 por no aparecer debidamente justificada la perpetración del delito) y reclamaciones efectuadas.

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/ALIAS, 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 13 de marzo de 2023, como consta en el certificado que obra en el expediente.

Con fecha 13 de abril de 2023, se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

"La propia reclamante refiere en su escrito el sobreseimiento provisional de la causa penal mediante Auto del Juzgado de Instrucción ******JUZGADO.1*** *al no aparecer debidamente la perpetración del delito. Auto que, contrariamente a lo indicado en el escrito recibido por DIGI, no se encuentra entre la documentación aportada por lo que no ha podido ser objeto de estudio por esta parte. Por tanto, de la información*

disponible, el sobreseimiento provisional se produce ex art. 461.1 LEC y no por el segundo punto del mismo artículo.

*Consecuentemente, no es que no se haya podido identificar al autor o cómplices de un hipotético delito (en la reclamación se citan a un tal **A.A.A.** y un tal **B.B.B.** y presumimos que se pudo instruir, incluso, los códigos IBAN de las cuentas destinatarias y el nombre de sus titulares reales si no fueran aquellos), sino que no se ha podido comprobar la mera existencia de tal delito.*

Por tanto, no apareciendo debidamente justificada la perpetración de delito, deducir la actuación de DIGI acorde con la diligencia debida ya que:

1º) No se ha confirmado el quebranto del principio de integridad y confidencialidad por parte de la actuación de DIGI.

2º) No se ha confirmado la insuficiencia de las medidas de seguridad. No puede aceptar esta parte que sea suficiente para ello que la reclamante indique en su escrito que la Policía pudiera haberlo señalado esto en un atestado, no solo por no aportarse el mismo sino porque tal opinión pudiera estar exenta de crítica y contra-argumentación, máxime cuando no se facilitan los argumentos materiales para su sustento.

3º) No se ha confirmado la brecha de seguridad que pudiera dar lugar a una obligación de notificación ex normativa de protección de datos.

No obstante lo anterior, tan pronto el reclamante informa de tales hechos, DIGI procedió a la adopción de las siguientes medidas encaminadas a solventar la situación y minimizar cualquier posible riesgo que se pudiese originar:

a) Rectificación del elemento causante de la incidencia: suspendiendo la SIM activada de forma presuntamente irregular. Conviene señalar a estos efectos que la línea de móvil estuvo activada en la SIM presuntamente fraudulenta desde la noche del 04-09-21 hasta la tarde del 07-09-21, cuando se inactivó la SIM supuestamente irregular y se entregó a la reclamante el nuevo duplicado SIM generado para recuperar el control de su línea. Cabe mencionar que para la generación de este duplicado también se siguió el procedimiento de identificación doble de la reclamante, primero telefónicamente en el servicio de atención al cliente de DIGI y después presencialmente en un dealer de DIGI, donde la reclamante tuvo que mostrar su documento de identidad.

b) En relación con lo anterior, DIGI procedió de forma interna a la investigación de los hechos acaecidos a efectos de detectar el origen del incidente. Dado que esta compañía es desconocedora de una posible pérdida, por parte del reclamante de su documento identificativo, y/o de otros datos que pudiesen ser utilizados para la obtención del duplicado de la tarjeta SIM, se procedió a la imposición de medidas respecto al Distribuidor implicado por un posible incumplimiento contractual por parte de éste de las políticas establecidas por esta compañía para la identificación de clientes. Por este motivo, tal y como ha sido expuesto, DIGI contactó con el Distribuidor para esclarecer los hechos acontecidos, así como para recordar y reiterar la importancia de cumplir con los procedimientos establecidos.

c) Adicionalmente, DIGI ha estimado los hechos reclamados por la reclamante, facilitándole a estos efectos la información solicitada en su ejercicio del derecho de acceso.

Respecto al ámbito de actuación de la Compañía, la incidencia relatada por la reclamante traería causa en un supuesto caso de duplicado SIM no solicitado por la reclamante.

En concreto se recibió llamada a las 20:43 del 04-09-21 de una persona que, superando el test de identificación (nombre-apellidos, teléfono, documento de identidad y cuatro últimos dígitos del número de cuenta) y por tanto identificándose como la reclamante, solicitaba el duplicado de la tarjeta SIM asociada a dicho número. Superado dicho test se concede el duplicado y se le facilita el código necesario para aportar en la recogida presencial ante un Dealer junto con su Documento de Identidad para recoger la SIM y finalizar el proceso de duplicado. La reclamante contactó indicando que no tenía red el día 06-09-21, solicitando el duplicado SIM una vez superado el test de identidad ya referido. El proceso de duplicado finalizó el día 07-09-21.

Aunque DIGI ha comprobado que se trata de un incidente de carácter puntual, en aras de garantizar y reforzar la seguridad en el tratamiento de los datos personales de sus clientes, esta Compañía ha modificado los procedimientos de emisión de duplicados de tarjeta existentes en la fecha en la que sucedieron los hechos analizados, tal y como se expondrá más adelante.

Así mismo, interesa a esta compañía resaltar que los perjuicios manifestados por la reclamante que han sido ocasionados en el presente caso, derivan concretamente de los procesos de identificación de clientes establecidos por las propias entidades bancarias. En este sentido, tal y como relata la reclamante en su escrito de denuncia, el presunto usurpador lograría superar los protocolos de seguridad de identificación remota de la entidad bancaria y así acometer el consecuente perjuicio. Ha de resaltarse que entre los elementos de seguridad de la entidad bancaria se encontrarían el saldo, importe de la nómina, ingresos, última transferencia, datos de cotitular, que el presunto usurpador no habría contestado satisfactoriamente según lo que se relata en el escrito de la reclamante. Pero aun así la entidad bancaria permitió a dicho presunto usurpador acceder a los datos bancarios de la reclamante. En este sentido, entre los elementos de seguridad de la entidad bancaria no se encontraría el número de cuenta –que si era objeto entonces de uno de los mecanismos de seguridad para la autenticación de DIGI lo que denota la existencia de un incidente de seguridad previo a cualquier actuación de DIGI y ajeno a esta Compañía, puesto que el presunto usurpador pudo acceder al dato del número de cuenta de la reclamante bien a través de la entidad bancaria de ésta, o a través de la propia reclamante. Habida cuenta por tanto de estos daños colaterales que se pueden derivar para los clientes de esta Compañía con motivo de la adquisición de un duplicado de tarjeta SIM, y en virtud de los riesgos detectados, DIGI ha centrado sus principales esfuerzos y objetivos en la mejora de dichos procesos.

Tal y como se ha venido informando por parte de esta compañía, la adquisición de duplicados de tarjeta SIM mediante suplantación de identidad de los clientes es

una problemática actual en la que no sólo se están viendo afectados los propios clientes de forma directa, sino además los propios operadores de telecomunicaciones, en quienes recaen las obligaciones impuestas por la regulación sectorial de telecomunicaciones sobre conservación de datos como la normativa aplicable sobre protección de datos de carácter personal, además de las consecuencias colaterales que ello puede generar, como es la posible pérdida de clientes.

Así pues, en el último año DIGI ha cambiado y reforzado sus procesos internos para la emisión de duplicados de tarjeta SIM en varias ocasiones, atendiendo a su eficacia y a los riesgos detectados, siempre con el objetivo de mitigar la contingencia existente con la solicitud de duplicados de tarjeta SIM realizados bajo suplantación de identidad.

A continuación, incluye de forma detallada, las medidas adoptadas para evitar que se produzca esta suplantación, así como un informe detallado sobre las medidas técnicas y organizativas implementadas por el responsable del tratamiento para acreditar la identidad del titular de una tarjeta SIM en el momento de solicitar un duplicado, bien por el canal presencial, bien por el canal telefónico o cualquier otro establecido a tal efecto (p.ej. la plataforma web).

Para la emisión del duplicado de tarjeta SIM que supuestamente se produjo de forma irregular, el Punto de Venta comprobó el documento de identidad del solicitante y procedió a introducir en el sistema el número de teléfono para el cual se solicita el duplicado, además del número del documento de identidad. Siendo ambos datos coincidentes con los datos contenidos en las bases de datos de DIGI, se autoriza la generación del duplicado SIM, para lo que, en el siguiente paso, el sistema solicita la introducción del ICCID de la nueva tarjeta SIM. A estos efectos, la comprobación del documento identificativo, y la coincidencia entre los datos aportados es la única manera de obtener un duplicado SIM, rechazándose la emisión del duplicado SIM si los datos aportados no coinciden con los datos registrados por DIGI.

Dicho protocolo de segunda identificación ha sido confirmado por el Dealer:

Por tanto, de las comprobaciones que han sido efectuadas por DIGI, se ha podido determinar que la causa que ha motivado la presente reclamación es la emisión presuntamente irregular de un duplicado de tarjeta SIM, tras haberse presuntamente usurpado la identidad del reclamante por parte de un individuo que previamente pudo haber tenido acceso a la información personal del reclamante, por causas ajenas a DIGI, y que, por tanto, dicho individuo era ya conocedor de la misma.

Teniendo en cuenta lo expuesto anteriormente, se puede evidenciar que DIGI contaba con medidas técnicas y organizativas suficientes para la verificación de la identidad de los clientes ante una solicitud de duplicado SIM, de cara a evitar posibles incidencias como la que ha originado la presente reclamación, de forma que razonablemente podían calificarse de idóneos y suficientes, no habiéndose detectado de forma fehaciente un fallo en dichas medidas, sino que el supuesto resultado pernicioso se ha producido como consecuencia de una pérdida de confidencialidad de los datos personales del reclamante con anterioridad y por causas totalmente ajenas a DIGI, además del propio protocolo de seguridad implantado por las entidades

bancarias para la identificación de sus propios clientes, a fin de evitar incidentes como el que nos ocupa.

A mayor abundamiento, las indicaciones que hace la propia reclamante respecto del Auto judicial que conoció de los hechos se deduce que no se ha podido confirmar la mera existencia del delito.

Adicionalmente, en relación al caso que nos ocupa, DIGI ha podido confirmar que una vez se tuvo constancia de la emisión del duplicado de la tarjeta SIM no autorizado por la reclamante, se pusieron en marcha todas las acciones necesarias para reestablecer la irregularidad detectada, así como para frenar posibles emisiones de duplicados de tarjeta SIM no autorizados."

TERCERO: Con fecha 20 de abril de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: Con fecha 24 de abril de 2023, se recibe en esta Agencia nuevo escrito de respuesta indicando lo siguiente:

En el momento de solicitud de duplicado se requería para autenticar en primer lugar por teléfono, aportar el nombre completo, número de teléfono, número de documento de identidad y cuatro últimas cifras del número de cuenta bancaria del titular de la línea. Se aporta como Documento 1 copia de la grabación de llamada.

Tal y como se puede escuchar en la grabación la persona solicitante supera el filtro de seguridad sin mayor problema, quedando identificado como titular de la línea, y así queda reflejado en su histórico de cliente.

En cuanto a la presentación del DNI al recogerse la tarjeta física en el distribuidor implicado, como se ha explicado a la Agencia, el procedimiento establecido por DIGI requería que el titular de la línea (tras la previa identificación telefónica) visitara un distribuidor de DIGI, se identificará mediante la exhibición física y presencial de su documento de identidad original, y finalmente el número de dicho documento de identidad debía ser introducido en el sistema habilitado por DIGI para ello. Se adjunta a continuación captura de pantalla del mencionado sistema, donde se puede comprobar que se describe el procedimiento, y se exige la introducción del número de teléfono para el cual se está pidiendo el duplicado, más el número documento de identidad del titular.

Así pues, el sistema no deja generar un duplicado SIM si (1) el cliente ha solicitado el duplicado telefónicamente, y se ha identificado correctamente por vía telefónica; (2) el cliente se ha identificado (por segunda vez) presencialmente ante un distribuidor de DIGI y mediante su documento de identidad original; (3) se han introducido todos los datos correctamente en el sistema para habilitar la generación del duplicado. Este es el procedimiento que estaba definido y había que seguir para obtener el duplicado de la tarjeta SIM de la reclamante, y no hay argumento alguno (salvo que se hubiera cometido algún delito) para sostener que el procedimiento no se siguió tal y como había sido implantado por DIGI.

En primer lugar, cabe traer aquí los pasos previos tomados para la correcta adecuación de las medidas a tomar para el caso concreto:

1ª) Revisión preliminar acerca de su historial sobre incidencias similares. Esta parte entiende de interés señalar que ni antes, ni después del incidente objeto del presente expediente, el distribuidor ha estado relacionado con ninguna otra situación análoga, habiendo ejecutado su contrato conforme a las normas y protocolos objeto de análisis, y es un distribuidor que sigue actualmente colaborando con DIGI en tanto que cumple con sus obligaciones.

2º) Revisión preliminar del historial y actuación del distribuidor.

3º) Entrevista con el distribuidor para que se pronunciase sobre la situación y, en concreto, sobre su actuación al respecto.

No habiendo ningún elemento que hiciera dudar de la correcta actuación de todos los empleados y colaboradores de DIGI, incluyendo el distribuidor, se impusieron las siguientes medidas en atención meramente al principio de precaución:

• Recordatorio al distribuidor de la importancia de la correcta autenticación por los daños que puede conllevar tanto al cliente, como a DIGI y, por su puesto, a la propia persona del distribuidor.

• Recordatorio al distribuidor de los procesos de verificación contra usurpaciones."

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 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), es competente para resolver estas actuaciones de investigación 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
Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

III
Principios relativos al tratamiento

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

IV
Conclusión

La reclamación se concreta en que la tarjeta del teléfono de la reclamante fue clonada por parte de la mercantil DIGI SPAIN TELECOM, S.L.U. ("DIGI"), ya que el 4 de septiembre de 2021, sin ninguna medida de seguridad tendente a identificar fehacientemente a la persona que lo solicitó, una tercera persona, suplantó su identidad.

La entidad reclamada ha acompañado las medidas de seguridad que tiene implantadas para evitar la suplantación o fraude en las solicitudes de duplicado de tarjetas SIM y que fueron cumplidas en el caso objeto de reclamación: se identificó de forma completa al solicitante por teléfono y se aportó el DNI en la tienda presencial.

Por otro lado, la reclamante también presentó denuncia por estos hechos que fue sobreseída por no aparecer debidamente justificada la perpetración del delito.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

De conformidad con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a DIGI SPAIN TELECOM, S.L. y a la parte reclamante.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

940-020323

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