

- **Expediente N.º: EXP202506415**

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 6 de marzo de 2025, se presentó reclamación ante la Agencia Española de Protección de Datos en relación con hechos que podrían ser constitutivos de una infracción imputable a VODAFONE ESPAÑA, S.A.U. con NIF **A80907397** (en adelante, VODAFONE o parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante, cliente de VODAFONE, afirma que un agente de la parte reclamada, durante una gestión realizada por su madre, realizó por error un duplicado de su tarjeta SIM sin su consentimiento.

Junto a la notificación se aporta captura de pantalla de un correo electrónico de fecha 27 de febrero de 2025, dirigido desde la dirección tienda@lowi.es a la dirección *****EMAIL.1**, en la que se le informa del envío de una nueva tarjeta SIM.

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 VODAFONE, 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 29/04/2025 como consta en el acuse de recibo que obra en el expediente.

En respuesta al traslado, VODAFONE informa del procedimiento para emitir duplicado de tarjeta SIM en los siguientes términos:

- Afirma que las vías para solicitar un duplicado de tarjeta SIM son tres: mediante llamada telefónica al servicio de atención al cliente, a través de la aplicación App de la operadora virtual y de forma presencial en una tienda.

Para esta última opción dice el reclamado que *"a través de un número muy limitado de distribuidores autorizados. El solicitante para ello deberá identificarse previamente, aportando su DNI/NIE que permita acreditar su identidad como titular de la línea"* adjuntado documento 1 con el protocolo interno.

En referencia a los hechos ocurridos y que han dado lugar a la reclamación, señala que:

*"[...] se ha constatado que el (reclamante) habría sufrido una incidencia en su línea número *****TELÉFONO.1**, como consecuencia de una solicitud de duplicado SIM realizada por la madre del reclamante en una tienda de Vodafone ubicada en *****DIRECCIÓN.1**, el día 27 de febrero de 2025 a las 20:34 horas. [...]*

(Adjunta captura de pantalla de la aplicación informática del trámite realizado).

El (reclamante) posteriormente y a los efectos de restaurar su línea, acude a otra tienda (del reclamado) y solicita un nuevo duplicado SIM el día 3 de marzo de 2025 a las 15:31 horas. [...]

(Adjunta captura de pantalla de la aplicación informática del trámite realizado).

Por último, el (reclamante) el mismo 3 de marzo de 2025 llama a Atención al Cliente (de la parte reclamada), contando lo ocurrido y solicitando explicaciones."

Continúa la parte reclamada informado que, en las tiendas donde se venden productos de su marca y de la operadora virtual, en su proceso de identificación para realizar duplicados de la tarjeta SIM *"se debe identificar al solicitante mediante la visualización y fotocopia del documento de identidad, que debe quedar custodiado por la tienda, y tras ello, el personal de tienda debe llamar a soporte canal (número específico para el soporte de tiendas) y pasar política de seguridad."*

"La política de seguridad consiste en indicar en relación con la línea afectada por el duplicado SIM: (i)Nombre, Apellidos, documento de identidad del titular de la línea, (ii) línea móvil afectada por el duplicado, (iii) nuevo ICC, (iv) y, por último, solicitar de la tienda confirmación de que se ha verificado la identidad del solicitante correctamente mediante la fotocopia del documento de identidad."

*"Verificados los sistemas, se ha podido comprobar que consta grabación del paso de la política de seguridad." que aporta como archivo adjunto. Sin embargo, señala que "no ha podido conseguir la fotocopia del documento de identidad, dado que la tienda de *****DIRECCIÓN.1** ha cambiado de dueño el 31 de marzo de 2025, habiéndose enviado toda la documentación en papel al proveedor (del reclamado) que almacena y digitaliza dicha documentación, no habiendo sido posible localizar este documento.". Añadiendo en el apartado tercero del escrito que "En el presente caso, dado que fue la madre del reclamante quien solicitó el duplicado SIM se debió también facilitar una*

autorización del reclamante permitiendo la operación, autorizando a su madre a realizar el trámite. Dicho documento tampoco se ha podido localizar."

Así mismo, el duplicado de la tarjeta SIM, informa "no se envió por correo postal porque este se retiró en la propia tienda, por la madre del reclamante", ya que las propias tiendas cuentan con tarjetas SIM.

Por otra parte, indica que debido a que el reclamante estuvo sin servicio como consecuencia del duplicado de la tarjeta SIM, se realizó un abono en compensación, aportando el documento 3 que lo justifica.

Respecto al protocolo de actuación cuando se detecta la emisión de un duplicado de tarjeta SIM fraudulento, la parte reclamada dice que cuando hay un caso de este tipo:

"[...] se incluye un aviso en sistemas y el Departamento de Fraude revisa el caso, y en aquellos casos que se consideran fraude, se restablece el servicio inmediatamente mediante la emisión de un nuevo duplicado SIM, lo que permite desactivar el duplicado SIM fraudulento. Además, se establece una alerta en los sistemas, para que los agentes sepan que ha sido víctima de fraude, mediante el marcado del check víctima de fraude [...], quedando el siguiente mensaje en la ficha del cliente: 'Cliente con intento de fraude. No hacer cambios sin política de seguridad estricta'.

Adicionalmente, se incluyen los datos de la persona afectada en los listados de prevención del fraude para que no puedan realizarse futuras contrataciones por terceros no autorizados.

Por último, se verifica si el fraude ha ocasionado algún tipo de daño o perjuicio económico y se abonan las cantidades que, en su caso, puedan corresponder, bien el coste del duplicado SIM que no se ha solicitado, bien el tiempo que no se ha podido disfrutar del servicio, etc. y se abonan las cantidades correspondientes.

Finalmente, se penaliza a los proveedores que incumplan las políticas de seguridad establecidas, además de requerir la adopción de medidas disciplinarias para los agentes involucrados, según qué casos y el tipo de fraude realizado."

Para el caso en concreto dice la parte reclamada que "El Departamento de Fraude no ha calificado el presente duplicado SIM como un duplicado fraudulento, ya que no se ha realizado por tercero con intenciones fraudulentas, ni tampoco se han producido transferencias bancarias o retiradas de dinero perjudiciales para el reclamante.". Y que, según la grabación aportada "la solicitud de duplicado SIM se presumía lícita al haberse aportado por parte de la tienda la información requerida por la Política de Seguridad".

Por último, aporta el documento 4, carta que envió al reclamante informando de las gestiones realizadas.

En la grabación aportada, se escucha una conversación de dos minutos entre el soporte canal (en adelante soporte) y una persona que se identifica como "(...)" (en adelante vendedor):

- (...).
- (...).
- (...).
- (...).
- (...).
- (...).
- (...).

TERCERO: Con fecha 6 de junio de 2025, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

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:

1) Por la información aportada durante las actuaciones, se ha conocido que en el procedimiento del reclamado para realizar un duplicado de tarjeta SIM en una tienda:

- El cliente, presenta su documentación para verificar que es el titular de la línea.
- Una vez comprobado se fotocopia la documentación y firma una solicitud con tres copias impresas, una para el reclamado, otra para el distribuidor y otra para el cliente.
- Posteriormente el personal de tienda llama a soporte del canal para finalizar el trámite.
- La nueva tarjeta es entregada en la propia tienda al titular. En caso de que la persona que acude a la tienda no es el titular sino un autorizado, la nueva tarjeta no se entrega y se gestiona con atención al cliente el envío al domicilio.

En relación con la documentación generada durante el trámite, la copia para la tienda es custodiada por el distribuidor y la copia para el reclamado la envían los distribuidores a través de *****COMPAÑÍA.1**. Que cuenta con una plataforma para registrar los envíos y la posterior recogida de los documentos en papel en la tienda física.

2) Por la información aportada por el reclamado y el investigado, se ha constatado que el investigado firmó el contrato como encargado de tratamiento con el reclamado, estando vigente hasta el 31/03/2025.

Se ha confirmado que el reclamado es el responsable del tratamiento de datos.

3) Se ha constatado que se realizó un duplicado de la tarjeta SIM de la línea *****TELÉFONO.1** el 27/02/2025. La solicitud se realizó en la tienda del investigado.

Se ha comprobado que, siguiendo el protocolo, el personal de tienda llamó a soporte de canal para finalizar el trámite, y que cuando el agente preguntó al personal de tienda si tenía la fotocopia del documento de identidad del titular y el titular se encontraba en la tienda, obtuvo una contestación afirmativa.

4) No ha sido posible averiguar la persona que realizó el trámite de duplicado de tarjeta SIM porque ni el operador ni el investigado han encontrado la documentación asociada: documento de identidad del titular y solicitud de duplicado firmada por el titular o documento del titular autorizando a realizar el trámite a otra persona.

Según el reclamado y el investigado, ninguno tiene copia de la documentación del duplicado de la tarjeta SIM, aunque el reclamado tampoco puede aportar la documentación de la segunda solicitud de duplicado de la tarjeta SIM que hizo el reclamante.

Tampoco puede el reclamado dar explicaciones del motivo por el que no se encuentra la anterior documentación ni ha indicado si existe información que relacione la activación de la tarjeta SIM con la documentación entregada o pendiente de entrega, en el sistema de gestión con *****COMPAÑÍA.1**.

5) Del mismo modo, no se ha podido comprobar si el duplicado de tarjeta SIM se realizó por error por la madre, titular de dos líneas en el mismo operador virtual de la reclamación, al no constar la documentación asociada al trámite.

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 Presidencia 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 registrarán 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 establece 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

Conclusión

En el presente caso constaría que se ha tramitado el duplicado de la tarjeta SIM del reclamante, afirmando éste que sin su consentimiento ni conocimiento. Dicha solicitud se lleva a cabo en una tienda presencial, colaboradora de VODAFONE, que es además encargada de tratamiento.

Durante las actuaciones previas de investigación, VODAFONE ha acreditado tener protocolos sobre el proceso de solicitud de los duplicados de tarjeta, que incluyen reglas específicas sobre la comprobación de la identidad de que es el titular quien lo tramita.

Por la información obrante en el expediente, no constan evidencias ni documentación suficiente para poder determinar quién realizó la solicitud, con base en qué documentación, ni si, en consecuencia, el encargado de tratamiento (con el que ha dejado de colaborar) siguió las instrucciones anteriormente mencionadas al comprobar la identidad de la persona que solicitó presencialmente la tarjeta.

A este respecto, debe destacarse que en el ámbito administrativo sancionador son de aplicación, con alguna matización, pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones.

El Tribunal Constitucional en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta

“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”.

De acuerdo con este planteamiento, el artículo 53.2 de la LPACAP, establece que, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

“b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.”

Como ha precisado el Tribunal Supremo en Sentencia de 26 de octubre de 1998, la vigencia del principio de presunción de inocencia

“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

Así las cosas, se debe distinguir la verdadera prueba de indicios de las meras sospechas o conjeturas. El Tribunal Constitucional ha manifestado en su Sentencia 24/1997 que

“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que: a) La

prueba indiciaria ha de partir de hechos plenamente probados. b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)."

En definitiva, el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor.

Estrechamente vinculado al principio de presunción de inocencia, se encuentra el principio indubio pro reo, del que la Sentencia del Tribunal Constitucional de 20/02/1989 indica que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

De acuerdo con este principio, aplicable también al ámbito del derecho administrativo sancionador, la carga de la prueba recae en la administración, señalándose que, en caso de duda sobre los hechos o la responsabilidad del investigado/imputado debe realizarse la interpretación más favorable al presunto infractor.

En el presente caso, cabe concluir que se plantean dudas razonables acerca de los hechos reclamados. En consecuencia, procede el archivo de esta reclamación, en aplicación del principio in dubio pro reo, consagrado en el artículo 24.2 de la Constitución española, como garantía esencial que supone una manifestación del principio de presunción de inocencia de acuerdo con consolidada jurisprudencia del Tribunal Constitucional y del Tribunal Supremo (entre otras, la STS Sala 2ª 459/2018 de 10 de octubre).

Por lo tanto, en base a lo indicado en los párrafos anteriores, y con la información de la que se dispone en este momento, no se han encontrado indicios suficientes que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir la responsabilidad por el tratamiento de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a VODAFONE ESPAÑA, S.A.U. y a la parte reclamante.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará 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 Presidencia 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.

1245-101025

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