- **Expediente N.º: EXP202412168**

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 2 de julio de 2024, se presentó reclamación ante la Agencia Española de Protección de Datos contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF A48265169 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 6 de junio de 2024, se llevó a cabo una portabilidad fraudulenta de su número de teléfono móvil por parte de terceras personas que usurparon su identidad, lo que propició que dichos terceros accedieran a la App de su banco (parte reclamada) cambiando su clave de acceso y realizando diversas compras y transferencias fraudulentas.

Junto a la reclamación, la parte reclamante aporta como documentación relevante la siguiente:

- Copia de la respuesta recibida a una anterior reclamación presentada ante la entidad reclamada, de fecha 26 de junio de 2024, en la que se indica, entre otros, lo siguiente: *"De cara a que situaciones como ésta no vuelvan a repetirse, le recordamos la necesidad de extremar las medidas de seguridad y custodia de sus claves e instrumentos de pago para evitar que terceras personas puedan hacer un uso malintencionado de los mismos y no autorizado por usted [...] No obstante y, tras haber revisado los hechos que nos describe, le informamos que, en esta ocasión, hemos procedido a atender su solicitud de manera favorable, siendo abonados todos los importes reclamados en su cuenta..."*.
- Copia de una reclamación presentada ante el Departamento de Conducta de Entidades del Banco de España, de fecha 24 de junio de 2024
- Dos SMS recibidos relativos a la portabilidad de su número de teléfono móvil
- Copia del contrato de portabilidad recibida por la parte reclamante el 6 de junio de 2024 y certificado de firma.
- Copia de la denuncia de los hechos y ampliación de esta por la parte reclamante ante la Policía Nacional, con fecha de 6, 11 y 13 de junio de 2024.
- Documentos con las operaciones fraudulentas: compra por valor de 868,98€ realizado en la Región de Murcia, transferencia de 2800€, cargo por servicio de taxis en Estonia por valor de 48,65€, compras por valor de 450,00€ y 200,00€ en Madrid, y otra operación en Irlanda por valor de 200€.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 11 de septiembre de 2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 27 de septiembre de 2024 se recibe en esta Agencia escrito de respuesta indicando que las actuaciones fraudulentas llevadas a cabo por terceros en perjuicio de la parte reclamante fueron íntegramente reintegradas no teniendo por ende perjuicio económico alguno que soportar, así mismo se le confirmaba que no había existido filtración de datos alguna por parte de BBVA y se le respondía acerca de su solicitud de indemnización por los supuestos daños sufridos. Es decir, en todo momento se había atendido las reclamaciones de la parte reclamante.

Junto a la respuesta de la parte reclamada se presenta la siguiente documentación:

- *Comunicación remitida a parte reclamante por el Servicio de Atención al Cliente informando, entre otros asuntos, que no ha habido filtración de datos y la posibilidad de comprobar que los dispositivos que se encuentran vinculados a su cuenta aparecen como una opción de Seguridad en la app a modo informativo, pero esto no es limitante en ningún momento, ya que usted u otras personas podrían acceder desde cualquier dispositivo a través de la app y la web con sus claves. Las cuales recomendamos por seguridad cambiarlas cada cierto tiempo. Informan a la parte reclamante de una serie de cuestiones a tener en cuenta para para no ser víctimas de un fraude. Por último, comunican que es carga del reclamante probar los perjuicios alegados, mediante la documentación oportuna, que acredite el daño y la relación de causalidad con la acción u omisión del Banco. Hay que tener en cuenta que, para evaluar los daños y perjuicios causados, no es suficiente que estos se hayan causado efectivamente, sino que es necesario también que hayan provocado un daño o daños y que éstos puedan probarse por medios objetivos y sean cuantificables sobre bases también objetivas.*
- *Comunicación remitida a la parte reclamante por el Servicio de Atención al Cliente informando que tras haber revisado los hechos que nos describe, le informamos que en esta ocasión hemos procedido a atender su solicitud de manera favorable, siendo abonados todos los importes reclamados en su cuenta* ******CUENTA.1*** *con* ******FECHA.1****, por un importe total de 4.767,63 €; quedando así su situación totalmente regularizada.*

TERCERO: Con fecha 2 de octubre de 2024, 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:

La presente reclamación está relacionada con la que presentó la misma parte reclamante señalando la portabilidad fraudulenta investigada durante las actuaciones del expediente ******REFERENCIA.1*** que permitió la realización de las operaciones financieras y comerciales señaladas en la presente reclamación.

Se le ha requerido a la parte reclamada que informara del procedimiento de acreditación de la identidad del cliente en la activación de la aplicación para terminales móviles de la entidad reclamada y el procedimiento para el restablecimiento de contraseña al haber olvidado la actual y verificaciones realizadas durante esta solicitud.

Con fecha de 14 de julio de 2025 se recibe en esta Agencia escrito de respuesta describiendo las operaciones que se llevaron a cabo sobre la cuenta bancaria, aclarando que las operaciones fraudulentas no fueron realizadas a través de la aplicación para móviles como señala la parte reclamante, sino a través de acceso web móvil, y aportando las evidencias recopiladas por el departamento de fraude.

De estas evidencias se desprende la siguiente cronología de los hechos desarrollados todos ellos el 6 de junio de 2024:

5:31:49 horas: Inicio de sesión vía web introduciendo usuario (NIF) y contraseña.

5:32:29 horas: Consulta vía web del Valor del Código de Verificación (CVV) de la tarjeta asociada a la cuenta bancaria de la parte reclamante. Se requiere comprobación mediante envío de SMS al número de teléfono, informado por la parte reclamante a la entidad reclamada, con un código de validación.

5:33:22 horas: Consulta vía web del Número de Identificación Personal (PIN) de la tarjeta asociada a la cuenta bancaria de la parte reclamante. Se requiere comprobación mediante envío de SMS con un código de validación.

5:37:38 horas: Se realiza una compra en comercio por valor 868,98€ en la localidad de Murcia. Se requiere comprobación mediante envío de SMS con un código de validación.

5:55:59 horas: Se realiza una transferencia a través del canal web por importe de 2.800€. Se requiere comprobación mediante envío de SMS con un código de validación. Dado que la operación excedía 1.000€, se envía aviso de operación de alto importe a la parte reclamante mediante correo electrónico y al número de teléfono (notificación PUSH en lo sucesivo).

6:08:48 horas: Dado el alto importe de la operación anterior y la hora inusual de la operación, se produce el bloqueo del usuario multicanal. Se remiten dos correos electrónicos a la dirección de correo informada por la parte reclamante y dos notificaciones PUSH informando de que el usuario había sido bloqueado y el procedimiento a seguir para habilitarlo de nuevo.

6:09:47 horas: Se produce un cambio de contraseña solicitado por el usuario. Se remite correo electrónico informativo a la dirección de correo informada por la parte reclamante y notificación PUSH informando del cambio de contraseña.

Se desprende de esta cronología que la persona que realizó las operaciones fraudulentas conocía previamente las credenciales de la parte reclamante para el acceso web de la entidad reclamada. Es decir, el cambio de contraseña se produjo con posterioridad al bloqueo multicanal del usuario, probablemente, por un intento de desbloquearlo.

Este conocimiento previo de las credenciales de la parte reclamante pudo deberse a una incidencia previa de phishing (por correo electrónico), smishing (por SMS) o cualquier otro método común en la actualidad. Una vez conocidas estas credenciales y haber conseguido la portabilidad del número de teléfono de la parte reclamante (investigada en el expediente citado anteriormente), no existe barrera alguna para operar con normalidad sobre una cuenta bancaria o cualquier otra plataforma que utilice validación de las operaciones mediante el envío de SMS.

***(...)***

## 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 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
Integridad y confidencialidad

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
Presunción de inocencia

La Sentencia del Tribunal Constitucional de 20 de febrero -S 44/1989- indica lo siguiente:

(…) "*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, concurrente 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.*

*Desde la perspectiva constitucional la diferenciación entre la presunción de inocencia y la regla in dubio pro reo resulta necesaria en la medida que la presunción de inocencia ha sido configurada por el artículo 24.2 de la Constitución como garantía procesal del imputado y derecho fundamental del ciudadano protegible en la vía de amparo, lo que no ocurre propiamente con la regla in dubio pro reo, condición o exigencia subjetiva del convencimiento del órgano judicial en la valoración de la prueba inculpatoria existente aportada al proceso.*

*Es cierto que la distinción entre medio probatorio y resultado probatorio no puede ser tan radical en cuanto que la presunción de inocencia es también una regla de juicio a favor de ella que obliga a decidir a favor de la presunción de inocencia cuando no existan pruebas de las que pueda deducirse la culpabilidad, esto es, pruebas de carácter inculpatorio.*

*El que ahora el principio pro reo pueda tener un más sólido fundamento constitucional no permite que pueda confundirse el principio in dubio pro reo con el derecho constitucional a la presunción de inocencia, ni tampoco convertir el proceso de amparo en una nueva instancia en que pueda discutirse el resultado valorativo de una actividad probatoria de cargo realizada en el juicio oral y con todas las garantías"* (…)

Lo anteriormente expuesto, ha de conectarse con la vigencia en nuestro Derecho Administrativo sancionador del principio de presunción de inocencia reconocido en el artículo 24.2 de la Constitución Española, de modo que el ejercicio de la potestad sancionadora del Estado, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

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.

El Tribunal Constitucional (SSTC 131/2003 y 242/2005, por todas) se ha pronunciado en ese sentido al indicar que una de las exigencias inherentes al derecho a la presunción de inocencia es que la sanción esté fundada en actos o medios probatorios de cargo o incriminadores de la conducta imputada y que recae sobre la Administración pública actuante la carga probatoria de la comisión del ilícito administrativo y de la participación en él del denunciado. Por su parte, el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece como uno de los principios de la potestad sancionadora el de la “Responsabilidad”, determinando al respecto 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".*

Igualmente, se debe tener en cuenta lo que establece el artículo 53.2 la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que: *"Además de los derechos previstos en el apartado anterior, 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"*

V
Conclusión

Las razones que han motivado esta reclamación se sustentan en el conocimiento previo de las credenciales de la parte reclamante de acceso a la entidad bancaria. Esta circunstancia junto a la portabilidad fraudulenta investigada en el expediente ******REFERENCIA.1***, hicieron posible el acceso a la cuenta bancaria y validación de las operaciones.

Sin embargo, no se ha podido determinar a través de las actuaciones de investigación realizadas cómo el usurpador pudo tener conocimiento de las credenciales de acceso online a la entidad bancaria reclamada, y las cantidades adeudadas a la cuenta corriente y tarjeta de pago de la parte reclamada han sido restituidas por la entidad en su totalidad y comunicado a la parte reclamante.

En el presente caso, no existen elementos probatorios que permitan concluir que las medidas técnicas y organizativas de la entidad reclamada fueran inadecuadas o que el acceso fraudulento se produjera por una deficiencia atribuible a ésta.

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias 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 BANCO BILBAO VIZCAYA ARGENTARIA, S.A. 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.

940-101025

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