- Expediente N.º: EXP202201721

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Dña. ***A.A.A.*** (en lo sucesivo la reclamante) con fecha 28/12/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF A48265169 (en lo sucesivo el reclamado). Los motivos en que basa la reclamación son los siguientes: la afectada manifiesta que, tras extraviar su DNI y cursar la correspondiente denuncia el fecha 29/07/2021, un tercero acudió a una sucursal de la reclamada en ******LOCALIDAD.1***, suplantando su identidad siéndole facilitada información bancaria, además de entregarle la totalidad del dinero que se encontraba depositado en la cuenta, sin su autorización ni consentimiento; considera que la entidad reclamada no adoptó las medidas que la diligencia exige al no haber comprobado fehacientemente su identidad (en relación con el parecido físico y la firma).

Aporta:

- Copia de denuncia presentada ante los mozos de escuadra. En ella se señala que el día de la solicitud del extracto y reintegro fue el 26/07/2021 y el de la retirada de fondos el 29/07/2021, en la sucursal número ******SUCURSAL.1***, según indica, de informaciones recabadas del Servicio de Atención al Cliente de la entidad.
- Documento bancario sin firmar (ejemplar para el cliente), de fecha 23/09/2021, en el que se indica que ha recibido una cantidad de dinero correspondiente al montante que fue dispuesto sin su consentimiento, y el compromiso de no reclamar dicha cantidad en el futuro, renunciando a cualquier derecho o acción sobre tal disposición.

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), el 11/02/2022 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 14/02/2022 como consta en el acuse de recibo que obra en el expediente.

El reclamado respondió el 23/02/2022 mediante escrito en el que no aportaba información alguna sobre la reclamación que le fue trasladada.

TERCERO: Con fecha 22/03/2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

El reclamado respondió el 07/04/2022 aportando la siguiente información:

- El 23/08/2021 la reclamante solicitó a la reclamada la devolución de un cargo en su cuenta manifestando que ella no lo había autorizado. Aportan copia del escrito presentado.
- La reclamada resolvió anular el movimiento fraudulento realizada contra el saldo de la cuenta de la reclamante asumiendo el importe defraudado de 9.400 euros.
- El día 22/09/2021 la reclamada contestó a la reclamante indicando que procedía a tramitar el abono correspondiente en su cuenta corriente. Aportan copia del documento.
- El 25/11/2021 la reclamante presentó un nuevo escrito de reclamación a la reclamada, según se acredita mediante aportación de copia del mismo, solicitando la devolución del importe del cargo fraudulento y un 20% adicional como consecuencia de *"la actuación negligente de la sucursal que incumple con la norma en materia de protección de datos, al no verificar mi identidad a efectos de prestar un consentimiento lícito para la entrega de fondos y cesión de datos de naturaleza sensible." La reclamante indicaba en su escrito "esta actuación de la entidad financiera supone una vulneración de mi derecho a la protección de datos, por cuanto, la misma actuó sin la debida diligencia, habida cuenta que no validó correctamente mi identidad (física así como firma propia identificativa) ni adoptó las medidas de seguridad necesarias para verificar mi consentimiento para la retirada de los fondos y entrega de documentación que contiene datos de naturaleza sensible."*
- El 16/12/2021 la reclamada informó a la reclamante, mediante correo electrónico, que procedía a efectuar el abono del cargo efectuado contra su cuenta y, con respecto a la solicitud de indemnización de daños y perjuicios, le informó que debía acreditar los mismos para poder ser evaluados. Aportan copia del correo electrónico.
- Los representantes de la reclamada manifiestan que la reclamante no puso en conocimiento de la entidad bancaria que había perdido el 5/06/2021(casi dos meses antes de la disposición) su DNI, no siguiendo la recomendación del Banco de España para estos supuestos (aportan copia de la referida recomendación titulada "¿Has perdido o te han robado el DNI? Comunícalo a tu banco cuanto antes y denúncialo." Los representantes de la reclamada manifiestan que alertarles de la pérdida del DNI hubiera dado lugar a que la activación del protocolo del que dispone la red de oficinas en estos supuestos. A estos efectos, aportan copia del referido protocolo, que las oficinas deben seguir cuando un cliente les comunica el hurto o extravío del documento identificativo. En el protocolo se comprueba que se indica que *"en el caso de que el cliente comunique el hurto o extravío de su documento identificativo, es obligatorio añadir esa información en el teleproceso mediante bloqueo en cuenta (de texto libre) incluyendo el mensaje «ATENCION: documento robado/extraviado», restringiendo la operativa 0001 Reintegros de manera que sirva de alerta para la Red."*

Realizado requerimiento de información, el reclamado respondió el 30/05/2022 con la siguiente información y documentación:

- Se ha solicitado acreditación documental del procedimiento seguido para la identificación de las personas que solicitan trámites presencialmente en las oficinas, donde consten todos los controles establecidos sobre la acreditación de la identidad de los solicitantes, y copia de las instrucciones facilitadas a los gestores de los trámites a este respecto. En particular se ha pedido aportar el procedimiento de identificación para los trámites de atención de solicitudes de información y retirada de efectivo presenciales en oficina.

La parte reclamada aporta copia del procedimiento (norma interna) de disposiciones de efectivo. La norma interna está a disposición de los empleados de la entidad en la intranet. Han declarado además que comunican diariamente los cambios o actualizaciones que puedan afectar a las normas a través de correo electrónico, aportando copia de la imagen de un correo como ejemplo. También declaran que los empleados disponen de un portal de consultas, aportando como ejemplo impresión de una pregunta sobre identificación del cliente se incluye un enlace a la referida norma interna.

Aportan copia de la referida norma interna, titulada *"Disposiciones de efectivo contra cuentas personales dentro del ámbito de atención universal",* destacando los siguientes aspectos:

"- En el caso de personas físicas, para la comprobación de la firma será suficiente el cotejo con la firma digitalizada del cliente (siempre que se disponga de la misma).
- Atención Universal: Los clientes podrán acudir a cualquier oficina de la Red […] para realizar sus operaciones en Caja y podremos atenderles sin necesidad de ser la oficina propietaria del contrato.
Para ello será muy importante recordar que para verificar la firma del cliente, debemos tener digitalizado el documento de identificación y digitalizada la firma, no siendo necesario en este caso, solicitar la verificación a la oficina propietaria. […]
- Los únicos documentos válidos para una correcta identificación son: DNI español (NIF), pasaporte, […]
- Exclusivamente serán válidos los originales, nunca las fotocopias, y solamente si están en vigor. En ningún caso se aceptarán documentos caducados.
- Tanto el antiguo como el actual modelo español de permiso de circulación (también llamado carné de conducir) NO son válidos como documentos identificativos. […]
Cómo identificar correctamente:
Determinar si la persona que porta el documento es la misma que aparece en la fotografía del documento identificativo.
Verificar que el documento presentado es válido, que es original (nunca fotocopia) y que no esté caducado.
Observar si pudiera existir alguna manipulación o alteración sencilla (fundamental el uso de la lámpara de luz ultravioleta)
Cualquier documento que presente anomalías en su formato como consecuencia de una posible manipulación debe inducir a sospecha.

Observar al propio titular físicamente y determinar si su aspecto y edad coincide con el de la fotografía y la fecha de nacimiento que aparecen en el documento.
Finalmente, utilizar obligatoriamente la lámpara de luz ultravioleta para la validación del documento identificativo."

- Se ha solicitado impresión que acredite el detalle de los trámites realizados a resultas de la solicitud de información sobre los datos y productos bancarios de la reclamante efectuada el 26/07/2021 en oficina, así como la información y documentos que fueron facilitados al solicitante, y documentación acreditativa del detalle de las comprobaciones concretas sobre la identidad del solicitante que se realizaron en este caso. La parte reclamada no ha aportado documentación sobre los trámites realizados ni sobre la información y documentos que fueron facilitados al solicitante, ni de la acreditación documental de las comprobaciones sobre la identidad realizadas en el caso concreto.

- Se ha solicitado impresión que acredite el detalle de los trámites realizados a resultas de la solicitud de reintegro efectuada el 29/07/2021 (oficina ***SUCURSAL.1), así como documentación acreditativa del detalle de las comprobaciones concretas sobre la identidad del solicitante que se realizaron en este caso. Sobre las comprobaciones realizadas sobre la identidad los representantes de la parte reclamada indican que *"En el supuesto que se analiza y de conformidad con la citada norma, la oficina pagadera no realizó una correcta identificación de la persona que dispuso, ya que el reintegro lo llevó a cabo una persona distinta al titular con la documentación robada al cliente".* Aportan justificante de la solicitud de disposición digitalizado con la firma del solicitante, firma que consiste en el nombre y el primer apellido de la reclamante.

Aportan captura de la copia del DNI de la reclamante con su firma (documento digitalizado) indicando que es sobre el que se realiza la verificación previa a la disposición de efectivo (indican que el DNI se encuentra actualizado ya que se ha aportado copia del expedido con motivo del incidente). Indican que como medida de seguridad una vez detectado el fraude documental la oficina recibe las siguientes instrucciones: *"Deben digitalizar la versión actual de su documento de identidad, recomendamos mantener el bloqueo hasta que, bien lo recupere o deje de estar vigente"*.

QUINTO: Con fecha 25/11/2022, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado por la presunta infracción del artículo 6.1 del RGPD, sancionada conforme a lo dispuesto en el artículo 83.5.a) del citado RGPD y del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del citado RGPD.

SEXTO: Notificado el acuerdo de inicio, el reclamado mediante escrito de 12/12/2022 solicitó ampliación de plazo para formular alegaciones, que le fue concedido por el instructor del procedimiento.

El 23/12/2022 el reclamado presento escrito de alegaciones manifestando, en síntesis: que la imputación dirigida contra el reclamado y su fundamentación jurídica es errónea al no haberse vulnerado el artículo 6.1 del RGPD y con respecto a la vulneración del articulo 32.1 es igualmente errónea la interpretación que se realiza, sin

hacer referencia alguna a los procedimientos establecidos por el reclamado para garantizar la validez de las disposiciones de efectivo ni la jurisprudencia existente; la existencia de concurso medial; que en la imputación del artículo 32 del RGPD no se tiene en cuenta la sentencia del Tribunal Supremo de 15 de febrero de 2022 ni la diligencia desplegada por el reclamado.

Posteriormente se aporta copia del audio de la llamada efectuada al Servicio Atención al Cliente por la reclamante.

SEPTIMO: Con fecha/ 19/04/2023, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por la reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por el reclamado y la documentación que acompaña.

-Solicitar al reclamado:

Protocolo, Procedimiento o Instrucciones, etc., establecidas por la entidad para combatir y prevenir el fraude o estafa como en el caso presente, así como las medidas de seguridad o dictámenes para casos de fraude y prevención de fraude y para proceder a una correcta identificación de la clientela.

Acreditación de que dicha regulación junto a las medidas de carácter técnico u organizativas eran conocidas por la oficina donde se produjo la incidencia y eran conocidas por sus empleados.

El reclamado en fecha 09/05/2023 dio respuesta a la prueba practica cuyo contenido obra en el expediente.

OCTAVO: Con fecha 29/06/2023 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancionara al reclamado por infracción del artículo 6.1 y 32.1 del RGPD, tipificadas en el artículo 83.5.a) y artículo 83.4.a) del citado RGPD, con sanción de 50.000 € (cincuenta mil euros) y 20.000 € (veinte mil euros), respectivamente.

La citada Propuesta fue notificada al reclamado el 03/07/2023 dando respuesta a las alegaciones esgrimidas en el escrito presentado al acuerdo de inicio. Transcurrido el plazo legalmente previsto, el reclamado presento escrito de alegaciones el 25/07/2023 reiterando los argumentos esgrimidos a lo largo del procedimiento: que no existía infracción de los artículos 6.1 y 32.1 del RGPD y la existencia de concurso medial de infracciones, solicitando el archivo del procedimiento.

NOVENO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes,

HECHOS PROBADOS

PRIMERO. Con fecha 10/12/2020 tiene entrada en la AEPD escrito de la reclamante manifestando que ha sido objeto de suplantación de identidad; tras extraviar su DNI y cursar la correspondiente denuncia, un tercero acudió a una sucursal de su entidad bancaria siéndole entregada la totalidad del dinero que se encontraba depositado en su cuenta, sin su autorización ni consentimiento, considerando que la entidad reclamada no adoptó las medidas correspondientes al no comprobar fehacientemente su identidad.

SEGUNDO. La reclamante ha aportado copia de la denuncia de 16/08/2021 ante los mozos de escuadra, numero de diligencia ******DILIGENCIA.1*** at Usccorts. En la misma, la reclamante, manifiesta:
"(…)
Que ha estado de vacaciones, fuera en Europa…
Que, al volver a territorio nacional, abrió la aplicación móvil de su entidad bancaria y observó que habían hecho un reintegro, en ventanilla y en persona de 9400 euros, sin su consentimiento ni su autorización.
*Que la denunciante manifiesta que, dicha cantidad de dinero, fue sacada de la entidad BBVA, situada en LOCALIDAD.2 (***LOCALIDAD.1), concretamente de la oficina ***SUCURSAL.1.*
Que la Sra. ***A.A.A****. contacto con Atención al Cliente de su entidad bancaria y la informaron de que se había subido una nueva documentación a su perfil personal, de la cual, ella, no ha realizado ni tiene constancia alguna.*
Qué atención al cliente le facilito dato relativos al hecho, tales como el día en que se solicitó extracto y reintegro y el día en el cual retiraron el dinero.
Que el día de la solicitud fue el día 26/07/2021 y el día que retiraron el dinero fue el día 29/07/2021, ambos realizados en persona en la entidad bancaria de LOCALIDAD.2.,
Que la denunciantes desconoce quien, como y de qué manera han podido acceder a sus datos personales y, especialmente, como han sido capaces de poder sacar dinero, en persona, de la entidad bancaria si estos hacen, supuestamente, la comprobación de la identidad.
(…)"

TERCERO. La reclamante aporta copia de la denuncia realizada en Italia, estación de Venecia-San Marcos en relación con la pérdida de su DNI.

CUARTO. El reclamado ha aportado escrito firmado por la reclamante, sin fecha, en el que solicita la devolución de los sustraído en su cuenta.

QUINTO. El reclamado en escrito de 30/05/2022 ha manifestado que*: "En el supuesto que se analiza y de conformidad con la citada norma, la oficina pagadera no realizó una correcta identificación de la persona que dispuso, ya que el reintegro lo llevó a cabo una persona distinta al titular con la documentación robada al cliente",* y se aporta el justificante de la solicitud de disposición cuya firma no coincide con la que figura en el DNI de la reclamante.

Asimismo, señalaba que *"…ha resuelto anular el movimiento de la disposición fraudulenta realizada contra el saldo de la cuenta corriente de la reclamante asumiendo por tanto BBVA el importe defraudado de 9.400 euros…"*

SEXTO. Consta aportado escrito de fecha 23/08/2021 en respuesta a la solicitud de la reclamante solicitando la devolución del importe del cargo fraudulento en su cuenta, en el que se indica que: *"La solicitud se está gestionando con el número de referencia ***REFERENCIA.1, indicando este número podrá realizar cualquier consulta al respecto",* y la respuesta ofrecida por el reclamado el 22/09/2021 señalando que: *"Hemos recibido el escrito que nos presentó, con fecha 23 de agosto de 2021. Su número de referencia es ***REFERENCIA.1.*
El objeto de la reclamación, expuesto en su comunicación, es solicitar la devolución del dinero (9400 €) que le fue sustraído desde una de las oficinas de BBVA, sin su consentimiento ni autorización, tal y como se explica en la denuncia que adjunta a su escrito.
En este sentido, tras haber revisado los hechos que usted nos describe y la documentación recabada al respecto, le informamos que hemos dado traslado de este asunto a los departamentos oportunos de nuestra entidad que están encargados de analizar y resolver los hechos que nos detalla en su escrito.
Una vez revisado su caso y realizadas todas las comprobaciones necesarias nos informan que se ha atendido su solicitud de manera favorable, por lo que en los próximos días se va a proceder a tramitar el abono en su cuenta del importe objeto de su reclamación.
(…)"

SEPTIMO. Como se señalaba en el hecho quinto consta aportado documento de BBVA *Disposición en Efectivo,* de 29/07/2021 contra la Cuenta: *ES00 0000 0000 0000 0000 0000,* perteneciente a la reclamante en el que se señala: *He recibido del Banco Bilbao Vizcaya Argentaria S.A., con cargo a la cuenta indicada, la cantidad de: 9.400,00 EUROS.*
En el pie del documento aparece la *Firma del Interviniente,* cuya rubrica no coincide con la de la reclamante.

OCTAVO. Consta que la reclamante envió al reclamado el 25/11/2021 una nueva reclamación solicitando junto a la devolución del importe del cargo fraudulento, el 20% adicional como consecuencia de *"la actuación negligente de la sucursal que incumple con la norma en materia de protección de datos, al no verificar mi identidad a efectos de prestar un consentimiento lícito para la entrega de fondos y cesión de datos de naturaleza sensible."*

El reclamado respondía el 12/12/2021 que: *"…Por lo que respecta a su solicitud de compensación por resarcimiento de daños y perjuicios causados, le informamos 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. La acreditación de estos extremos corresponde a la persona que los alega y, en muchas ocasiones, exigen el desarrollo de una fase probatoria que solamente en un procedimiento judicial puede desarrollarse…"*

NOVENO. Consta portado por el reclamado la respuesta ofrecida el 21/02/2022 señalando que: *"Nos dirigimos a usted con relación al nuevo escrito que envió a esta*

entidad, a través de la Agencia Española de Protección de Datos, sobre la cantidad sustraída de su cuenta en una oficina de BBVA sin su consentimiento y la vulneración de su derecho a la protección de sus datos.
*A este respecto, le informamos que analizados de nuevo los hechos objeto de su reclamación, las condiciones concretas de las obligaciones asumidas por las partes y sus particulares circunstancias, esta Entidad considera adecuada la respuesta que se le facilitó a la reclamación ***RECLAMACIÓN.1, cuya copia adjuntamos, por lo que nos ratificamos en la misma.*
Asimismo, hemos podido comprobar que con fecha 16 de diciembre de 2022 fue abonada en su cuenta la cantidad reclamada por usted, por importe de 9.400 €.
No obstante, tal y como le informábamos en nuestra respuesta anterior, si usted no está conforme con esta resolución tiene la facultad de acudir al Departamento de Conducta de Entidades de Banco de España desde la recepción de esta carta…"

DECIMO. La reclamante aporta copia de documento emitido por BBVA, de 23/09/2021 sin firma, en el que se señala que a la reclamante se le ha abonado la cantidad de 9.400 euros comprometiéndose a no reclamar cantidad alguna a BBVA en el futuro, renunciando a cualquiera acción.

UNDECIMO. El reclamado ha aportado copia del audio de la llamada realizada al servicio de atención al cliente del reclamado con ocasión de la retirada de fondos de su cuenta.

DUODECIMO. El reclamado ha aportado documentos relativos a las *Disposiciones de efectivo contra cuentas personales dentro del ámbito de atención universal* en el que se recogen las instrucciones que regulan las disposiciones contra cuentas corrientes, de crédito y libretas de ahorro, así como emisiones de cheques bancarios y transferencias de efectivo; para la *prevención del Fraude y la Estafa* en el que se recogen las instrucciones para la prevención del fraude así como los procedimientos específicos según la modalidad del fraude, dictámenes de seguridad y otras consideraciones sobre fraude y los criterios y pautas de actuación para la *Identificación de la Clientela*.

DECIMOTERCERO. El reclamado ha aportado documentos Fraude por disposiciones de efectivo con DNIs robados y Documentos identificativos falsos en los que se describe el *modus operandi* y cómo actuar en caso de identificar dichas operativas.

DECIMOCUARTO. El reclamado ha aportado correos electrónicos de 25/01/2021 remitidos a las oficinas entre las que se halla donde se produjo la incidencia, asunto: Alerta seguridad 0121-Enero-2021 Fraude por disposiciones de efectivo con DNI robados (importante difusión a todos los compañeros de la oficina).

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y

garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II

Los hechos denunciados se materializan en la suplantación de la identidad de la reclamante por un tercero que acudió a una sucursal de la entidad reclamada, siéndole facilitada información bancaria y la entrega de la totalidad del dinero que se encontraba depositado en la cuenta sin su autorización ni consentimiento, considerando que se ha vulnerado la normativa en materia de protección de datos de carácter personal.

El artículo 58 del RGPD, *Poderes*, señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
(…)"

En primer lugar, el artículo 6, *Licitud del tratamiento*, del RGPD en su apartado 1, establece que:

"1. El tratamiento solo 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".

Por otra parte, el artículo 4 del RGPD, *Definiciones*, en sus apartados 1, 2 y 11, señala que:

"1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

"2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

"11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

III

1. El tratamiento de datos requiere la existencia de una base legal que lo legitime.

De conformidad con el artículo 6.1 del RGPD, además del consentimiento, existen otras posibles bases que legitiman el tratamiento de datos sin necesidad de contar con la autorización de su titular, en particular, cuando sea necesario para la ejecución de un contrato en el que el afectado es parte o para la aplicación, a petición de este, de medidas precontractuales, o cuando sea 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 afectado que requieran la protección de tales datos. El tratamiento también se considera lícito cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, para proteger intereses vitales del afectado o de otra persona física o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

De conformidad con lo señalado en el artículo 6.1, no consta acreditada base de legitimación alguna de las contempladas en el citado precepto para el tratamiento de los datos de la reclamante y cuya personalidad fuera suplantada para vaciar la cuenta de la que era titular, sin que el reclamado desplegara la diligencia que era necesaria para evitar incidencias como la que dio lugar a la reclamación y por ende al procedimiento presente.

2. En el presente caso, se han utilizado los datos de la reclamante para llevar a cabo una operación, disposición del efectivo contenido en una cuenta, por un tercero que no era el titular de la misma sino un suplantador de la identidad de la reclamante y aunque, en términos generales la entidad crediticia tiene legitimación para tratar los datos de la afectada en virtud del contrato suscrito entre ambos, para esta operación concreta no la tenía puesto que quien estaba haciendo uso de los datos era una persona ajena a la relación contractual teniendo que haber verificado la fotografía y la firma del documento que se le presentaba, comprobar que el aspecto del titular de dicho documento y la persona que se tenía enfrente coincidían.

La reclamante ha manifestado desconocer quien fue la persona que acudió a la sucursal de su entidad bancaria siéndole entregada la totalidad del dinero que se encontraba depositado en su cuenta, sin su autorización ni consentimiento y sin adoptar las medidas correspondientes al no comprobar fehacientemente su identidad.

Hay que señalar que, como figura en los hechos probados, el propio reclamado ha manifestado en su escrito de respuesta al requerimiento informativo de la Agencia de 07/04/2021 que *"En el supuesto que se analiza y de conformidad con la citada norma, la oficina pagadera no realizó una correcta identificación de la persona que dispuso, ya que el reintegro lo llevó a cabo una persona distinta al titular con la documentación robada al cliente".*

Además, el propio reclamado ha aportado el justificante de la solicitud de disposición cuya firma no coincide con la que figura en el DNI de la reclamante.

A mayor abundamiento señala que *"…ha resuelto anular el movimiento de la disposición fraudulenta realizada contra el saldo de la cuenta corriente de la reclamante asumiendo por tanto BBVA el importe defraudado de 9.400 euros…"* (los subrayados corresponden a la AEPD.

Por tanto, no se trata como alega el reclamado en la respuesta a la Propuesta de Resolución de un error invencible en la identificación del portador del DNI de la reclamante sino de una grave falta de negligencia que hubiera sido vencida si se hubieran atendido correctamente los procedimientos y protocolos implantados, cotejando y verificando correctamente tanto la fotografía como la firma del documento que se le presentaba junto al de *Disposición en Efectivo*, y que no se compadece con lo señalado por el propio reclamado señalando que no se había realizado una correcta identificación de la persona que dispuso.

Por otra parte, huelga o es inútil señalar que el estado de la técnica permitiría quizás la adopción de medidas identificativas más efectivas como las biométricas, pero que estas son consideradas ilícitas por la AEPD.

De conformidad con lo que antecede, se estima que el reclamado sería responsable de la infracción del RGPD: la vulneración del artículo 6.1, infracción tipificada en su artículo 83.5.a).

IV

En segundo lugar, el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43.
(…)"

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)
g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".
(…)"

V

1. El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

La documentación obrante en el expediente evidencia que el reclamado ha vulnerado el artículo 32 del RGPD, al no tener implantadas y no utilizar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en este tratamiento. Esto es independiente de que, en este caso concreto, además un tercero haya podido suplantar la identidad del reclamante al serle facilitada no solo la totalidad del dinero que existía en cuenta, sino información relativa a la misma.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

2. En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación la AEPD trasladó al reclamado la reclamación presentada para su análisis solicitando la aportación de información relacionada con la incidencia reclamada sin que en un principio aportara información alguna sobre la reclamación trasladada.

No obstante, como se señalaba en fundamento anterior en escrito de fecha 07/04/2021 el reclamado ha reconocido que en este caso concreto que *"la oficina pagadera no realizó una correcta identificación de la persona que dispuso, ya que el reintegro lo llevó a cabo una persona distinta al titular con la documentación robada al cliente",* habiendo reintegrado la cantidad dispuesta a la reclamante, asumiendo la pérdida.

Aporta el reclamado el justificante de la solicitud de disposición en la que figura la firma del disponente, así como la captura de la copia de DNI y firma (digitalizados) que debe verificarse previamente a la disposición de efectivo.

La firma que consta en el justificante de la solicitud de disposición no se corresponde ni parece coincidir con la que figura en el DNI.

3. Como así figura en los hechos probados el reclamado aporto el documento *"Disposiciones de efectivo contra cuentas personales dentro del ámbito de atención universal"* en el que se recogen las instrucciones que regulan las disposiciones contra cuentas corrientes, de crédito y libretas de ahorro, tanto en la oficina en que radique la cuenta como en una oficina diferente.

En el punto 2, *Aspectos de riesgos*, se señala:

"El principal aspecto de riesgo en una disposición es la incorrecta identificación de la persona que va a disponer.

El proceso de identificación está regulado en la norma 80.00.116 "Identificación de la clientela":

Si la persona no se identifica apropiadamente (sea o no cliente), cuando esta identificación sea preceptiva puede y debe denegarse la operación que solicita. Así lo permite la Ley 10/2010 y diversas sentencias que hablan de la "pauta de desconfianza" por la que deben regirse aquellos que tienen a su cargo patrimonio de terceros, como son los empleados de las entidades financieras.

A continuación, señala en el punto 3.2, *Medidas de control de los documentos identificativos,* lo siguiente:

"*Cómo identificar correctamente:*

Determinar si la persona que porta el documento es la misma que aparece en la fotografía del documento identificativo.

Verificar que el documento presentado es válido, que es original (nunca fotocopia) y que no esté caducado.

Observar si pudiera existir alguna manipulación o alteración sencilla (fundamental el uso de la lámpara de luz ultravioleta)

Cualquier documento que presente anomalías en su formato como consecuencia de una posible manipulación debe inducir a sospecha.

Observar al propio titular físicamente y determinar si su aspecto y edad coincide con el de la fotografía y la fecha de nacimiento que aparecen en el documento.

Finalmente, utilizar obligatoriamente la lámpara de luz ultravioleta para la validación del documento identificativo".

También en el documento *Prevención del fraude y la estafa*, contiene instrucciones para evitar este tipo de delitos. A este respecto se señala el procedimiento para realizar una correcta identificación del cliente, documentos válidos, la forma de verificar a la persona y el documento, etc., de manera similar al anterior.

Este documento ya señala que *"La correcta identificación del cliente, tanto si se trata de una persona física individual, como si es apoderada de una persona jurídica, es básica para la prevención precoz de un fraude."*

Asimismo, indica que:

"Los únicos documentos válidos para una correcta identificación son:

** Documento Nacionalidad de Identidad.*

** Pasaporte.*

** Número de Identificación de Extranjeros (NIE), con sus distintas modalidades de Tarjetas (de residencia, asilo, estudiante, etc.).*

** Documento Identificativo nacional de un país de la Unión Europea con fotografía.*

Exclusivamente serán válidos los originales, nunca las fotocopias, y solamente si están en vigor. En ningún caso se aceptarán documentos caducados".

Y que:

"En cuanto a la realización de una correcta identificación, lo primero es determinar si la persona que porta el documento es la misma que aparece en la fotografía del documento identificativo, luego verificaremos que el documento

presentado es válido. Es decir, que esté comprendido entre los que el banco estima como apropiados para la correcta identificación, que sea original (nunca fotocopia) y que no esté caducado.

Lo segundo es observar si pudiera existir alguna manipulación sencilla.

Para ello no basta una mirada superficial del DNI. Hay que observarlo con detalle".

Por tanto, de conformidad con este último documento y el protocolo establecido para la disposición de efectivo la persona que solicita la operación sea o no cliente de la entidad, tiene que identificarse apropiadamente y en caso contrario debe denegarse la misma.

Además, esa persona debe aportar el documento de identificación, que debe ser válido, el original, que no sea fotocopia, que no está manipulado, que no se encuentre caducado, que no presente anomalías, comprobando que el aspecto del titular y la persona que se tiene delante coinciden, es decir, comprobar a través del mismo que es la persona que dice ser.

Sin embargo, en el presente caso no parece que la actuación llevada a cabo por el empleado en la oficina, como así lo confirma el propio reclamado, comprobara fehacientemente y de conformidad con las instrucciones señaladas tanto en el documento *"Disposiciones de efectivo contra cuentas personales dentro del ámbito de atención universal"* como en el de *Prevención del fraude y la estafa*, la personalidad del/la disponente puesto que la cantidad entregada y que provoco el vaciamiento de la cuenta le fue proporcionada a quien no era su titular con vulneración de las medidas correspondientes.

4. A mayor abundamiento, en relación con la disposición de efectivo, el 29/07/2021, un tercero acude a la oficina del reclamado situada en la ******DIRECCIÓN.1***, en ***LOCALIDAD.2 (***LOCALIDAD.1) solicitando la retirada de fondos de la cuenta de la reclamante, incumpliéndose el protocolo de identificación establecido para las retiradas de efectivo.

En el documento aportado por el reclamado consta el nombre y apellidos de la reclamante y la firma que no guarda similitud alguna con la contenida en la copia del DNI, a pesar de lo manifestado por el reclamado en sentido contrario.

Pero lo que resulta paradójico es que la copia del DNI que se aportó en ese momento para realizar la operación fue objeto de digitalización por la misma persona que facilitó el dinero al usurpador/a, es decir, que el DNI aportado en el momento de la disposición fue escaneado y registrado en la base de datos de la entidad como así se informó a la reclamante por el Servicio de Atención al Cliente en su llamada de fecha 04/08/2021, según figura en la copia por la grabación aportada.

Por tanto, lo que antecede evidencia es que el mismo día de la entrega de efectivo, por el empleado de la sucursal se efectuó la digitalización en los sistemas de la entidad del DNI empleado en la operación, sin que se apercibiera de que quien tenía delante no era quien decía ser, no garantizando la seguridad de los datos.

En sus alegaciones a la Propuesta insiste el reclamado en manifestar que se adoptaron las medidas necesarias para acreditar la identidad de la solicitante, llegando a la conclusión de que la persona que acudió a la oficina bancaria era aquélla que decía ser y se correspondía con la reclamante, cuyo documento aportaba, lo que resulta sorprendente a la luz de los hechos acreditados en el procedimiento: la firma no se correspondía con la existente en el DNI y aun así el empleado, como se señalaba anteriormente, procedió efectuó la digitalización en los sistemas de la entidad del DNI empleado en la operación, la afirmación de la propia entidad que ha señalado que no se realizó una correcta identificación de la persona que dispuso, por lo que estamos ante un comportamiento verdaderamente negligente, fácilmente vencible si se hubieran adoptado los protocolos y cautelas establecidas.

Por otra parte, hay que señalar que las medidas de seguridad del tratamiento de datos de la entidad financiera están enfocadas a la seguridad de las transacciones bancarias e indirectamente a garantizar el derecho fundamental de las personas afectadas a la protección de sus datos personales.

5. Por último, es cierto que el Tribunal Supremo en sentencia de 15/02/2022 señalaba que: *“La obligación de adoptar las medidas necesarias para garantizar la seguridad de los datos personales no puede considerarse una obligación de resultado, que implique que producida una filtración de datos personales a un tercero exista responsabilidad con independencia de las medidas adoptadas y de la actividad desplegada por el responsable del fichero o del tratamiento.*

En las obligaciones de resultado existe un compromiso consistente en el cumplimiento de un determinado objetivo, asegurando el logro o resultado propuesto, en este caso garantizar la seguridad de los datos personales y la inexistencia de filtraciones o quiebras de seguridad.

En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".

La diferencia radica en la responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable.

En estas últimas, la suficiencia de las medidas de seguridad que el responsable ha de establecer ha de ponerse en relación con el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados, pero no se garantiza un resultado.”

Sin embargo, también el Tribunal confirma que no resulta suficiente el diseño de los medios técnicos y organizativos necesarios, puesto que también resulta necesaria su correcta implantación y su utilización de forma apropiada.

Y es que la responsabilidad del reclamado viene determinada por el incidente de seguridad puesto de manifiesto por la reclamante, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva que las medidas técnicas y organizativas son apropiadas para garantizar un nivel de seguridad adecuado al riesgo

para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos.

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

VI

1. Alega el reclamado la existencia de un concurso medial de infracciones por concurrir el supuesto a que se refiere el art. 29.5 de la Ley 40/2015, de 1 de octubre, por lo que procedería la imposición de sólo una de las dos sanciones, en concreto, la referente a la infracción del artículo 6.1 del RGPD.

El art. 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que: *"Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida".*

No obstante, tal argumentación no puede ser aceptada; la norma específica en materia de protección de datos, es decir el RGPD, establece en su artículo 83.3 que:

"*3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.*

Ya señalábamos en el FD IV que el tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 6 del RGPD se considera como infracción muy grave, por lo que el único límite vendría establecido por el importe señalado en el artículo 83.5 del RGPD *"20.000.000 € 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".*

2. En alegaciones a la Propuesta el reclamado insiste en la existencia de un concurso medial de infracciones; continuando con lo expresado hay señalar que el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD. Y ello porque el RGPD es un sistema cerrado y completo.

El RGPD es una norma europea directamente aplicable en los Estados miembros, que contiene un sistema nuevo, cerrado, completo y global destinado a garantizar la protección de datos de carácter personal de manera uniforme en toda la Unión Europea.

En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne su finalidad última que es la garantía efectiva y real del derecho fundamental a la

Protección de Datos de Carácter Personal. Lo contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

De hecho, una muestra específica de la inexistencia de lagunas en el sistema del RGPD es el artículo 83 del RGPD que determina las circunstancias que pueden operar como agravantes o atenuantes respecto de una infracción (artículo 83.2 del RGDP) o que especifica la regla existente relativa a un posible concurso medial (artículo 83.3 del RGPD).

A lo anterior hemos de sumar que el RGPD no permite el desarrollo o la concreción de sus previsiones por los legisladores de los Estados miembros, a salvo de aquello que el propio legislador europeo ha previsto específicamente, delimitándolo de forma muy concreta (por ejemplo, la previsión del artículo 83.7 del RGPD). En este sentido, la LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que éste le permite y con el alcance que éste le permite.

Ello es así porque la finalidad pretendida por el legislador europeo es implantar un sistema uniforme en toda la Unión Europea que garantice los derechos y libertades de las personas físicas, que corrija comportamientos contrarios al RGPD, que fomente el cumplimiento, que posibilite la libre circulación de estos datos.

En este sentido, el considerando 2 del RGPD determina que:

"(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas".

Y el considerando 13 del RGPD que:

"(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".

En este sistema, lo determinante del RGPD no son las multas. Los poderes correctivos de las autoridades de control previstos en el art. 58.2 del RGPD conjugado con las disposiciones del artículo 83 del RGPD muestran la prevalencia de medidas correctivas frente a las multas.

Así, el artículo 83.2 del RGPD establece que *"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).".*

De esta forma las medidas correctivas, que son todas las previstas en el artículo 58.2 de RGPD salvo la multa, tienen prevalencia en este sistema, quedando relegada la multa económica a supuestos en los que las circunstancias del caso concreto determinen que se imponga una multa junto con las medidas correctiva o en sustitución de las mismas.

Y todo ello con la finalidad de forzar el cumplimiento del RGPD, evitar el incumplimiento, fomentar el cumplimiento y que la infracción no resulte más rentable que el incumplimiento.

Por ello, el artículo 83.1 del RGPD previene que *"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, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasoria".*

Las multas han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

Para que dicho sistema funcione con todas sus garantías en necesario que varios elementos se desplieguen de forma íntegra y completa. La aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español al permitirlo el propio RGPD-, ya sea por la aplicación de un concurso medial distinto del dispuesto en el RGPD, restaría efectividad al sistema que perdería su sentido, su finalidad teleológica, la voluntad del legislador, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

El RGPD está dotado de su propio principio de proporcionalidad que ha de ser aplicado en sus estrictos términos.

Y ello porque no hay laguna legal, no hay aplicación supletoria del artículo 29 del LRJSP.

Por otra parte, cabe significar que no hay laguna legal respecto de la aplicación del concurso medial. Ni el RGPD permite ni la LOPDGDD dispone la aplicación supletoria de las previsiones del artículo 29 de la LRJSP.

En el Título VIII de la LOPDGDD relativo a *"Procedimientos en caso de posible vulneración de la normativa de protección de datos"*, el artículo 63 que abre el Título se dispone 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."* Si bien existe una remisión clara a la LPACAP, no se establece en absoluto una aplicación subsidiaria respecto de la LRJSP que no contiene en su articulado disposición alguna relativa a procedimiento administrativo alguno.

De igual forma que la AEPD no está aplicando los agravantes y atenuantes dispuestos en el artículo 29 de la LRJSP, puesto que el RGPD establece los suyos propios, por ende, no hay laguna legal ni aplicación subsidiaria del mismo, tampoco cabe la aplicación de apartado relativo al concurso medial y por idénticas razones.

VII

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

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

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, *"Sanciones y medidas correctivas",* establece que:

"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 a imponer en el presente caso por la infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del RGPD de la que se responsabiliza al reclamado, se estiman concurrentes los siguientes factores como circunstancias agravantes:

La naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento; los hechos puestos de manifiesto afectan a un principio básico relativo al tratamiento de los datos de carácter personal, como es el de legitimidad, que la norma sanciona con la mayor gravedad; es evidente que los datos de la reclamante se utilizaron por un tercero que no era titular ni estaba autorizado para llevar a cabo la operación de retirada de efectivo (artículo 83.2.a) del RGPD).

La intencionalidad o negligencia en la infracción. Se observa una grave falta de negligencia al incumplirse los procedimientos implantados al no verificarse la identidad del tercer disponente, sin que se cotejara correctamente tanto la fotografía como la firma del documento que se le presentaba correspondía con el titular de la cuenta. Conectada también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la SAN de 17/10/2007. Si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba 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"* (artículo 83.2, b) del RGPD).

La entidad investigada es una de las grandes empresas dentro de su sector con un volumen de ventas de más de 1.000.000.000€ según datos AXESOR (artículo 83.2.k) del RGPD).

Son circunstancias atenuantes:

Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; una vez detectado el fraude se dictaron instrucciones para evitar dichas incidencias; así consta acreditada las alertas informativas enviadas mediante correo electrónico por el Responsable de Seguridad de la Dirección Territorial Sur a la oficina donde se retiraron los fondos (artículo 83.2. c) RGPD).

- De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción a imponer en el presente caso por la infracción tipificada en el artículo 83.4.a) y artículo 32.1 del RGPD de la que se responsabiliza al reclamado, se estiman concurrentes los siguientes factores como circunstancias agravantes:

Son circunstancias agravantes:

La naturaleza y gravedad de la infracción pues estamos ante el tratamiento de datos de tipo económico, que afectan a la solvencia de las mismas, además de los daños y perjuicios sufridos pues como consecuencia de la negligencia de la entidad los fondos de la cuenta fueron vaciados beneficiando a quien no era su titular (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

La intencionalidad o negligencia en la infracción. Se observa una grave falta de negligencia al incumplirse los procedimientos implantados no verificándose la identidad del tercer disponente, sin que se cotejara correctamente que tanto la fotografía como la firma del documento que se le presentaba correspondía con el

titular de la cuenta. Conectada también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la SAN de 17/10/2007. Si bien fue dictada antes de la vigencia del RGPD su pronunciamiento es perfectamente extrapolable al supuesto que analizamos. La sentencia, después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba 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" (artículo 83.2, b) del RGPD).

Infracción anterior cometida por el responsable o el encargado del tratamiento; existe reincidencia derivada de infracciones en relación con los mismos hechos: constan procedimientos resueltos por infracciones del reclamado con hechos relacionados con los artículos 32.1 del RGPD (PS/362/2021 y PS/420/2021) (artículo 83.2, e) del RGPD).

La entidad investigada es una de las grandes empresas dentro de su sector con un volumen de ventas de más de 1.000.000.000€ según datos AXESOR (artículo 83.2.k) del RGPD).

Son circunstancias atenuantes:

Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados; una vez detectado el fraude se dictaron instrucciones para evitar dichas incidencias; así consta acreditada las alertas informativas enviadas mediante correo electrónico por el Responsable de Seguridad de la Dirección Territorial Sur a la oficina donde se retiraron los fondos (artículo 83.2. c) RGPD).

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

La Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF A48265169, por infracción de los artículos 6.1 y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, multas de 50.000 € (cincuenta mil euros) y 20.000 € (veinte mil euros), respectivamente.

SEGUNDO: NOTIFICAR la presente resolución a BANCO BILBAO VIZCAYA ARGENTARIA, S.A.

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00 0000 0000 0000 0000 0000 (BIC/Código SWIFT: XXXXXXXXXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

Mar España Martí

Directora de la Agencia Española de Protección de Datos