- **Expediente N.º: PS/00677/2022**

TABLA DE CONTENIDOS

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 11 de enero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a BBVA a fin de imponerle multas por un importe total de 1.640.000 euros, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta comisión de las siguientes infracciones:

Tres relacionadas con el caso concreto denunciado por la reclamante:

- Por la presunta infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del RGPD, en relación con la contratación no autorizada de productos.
- Por la presunta infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por la falta de medidas de seguridad en relación con los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales
- Por la presunta infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, en relación con la incorporación de datos personales en los sistemas de información crediticia.

Y dos relacionadas con la forma en la que se establecieron los procedimientos implantados por el BBVA y que fueron revelados a través de la información aportada por la entidad financiera durante las actuaciones de investigación:

- Por la presunta infracción del artículo 25 del RGPD tipificada en el artículo 83.4 del mismo Reglamento.
- Por la presunta infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por con la falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros

En el citado acuerdo de inicio se le indicaba al BBVA que tenía un plazo de diez días para presentar alegaciones.

SEGUNDO: Con fecha 10 de febrero de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de BBVA en el que, por una parte, se aduce alegaciones al acuerdo de inicio respecto a la presunta infracción del artículo 25 del RGPD y a la presunta infracción del artículo 32 del RGPD por falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros y, por otra parte, se acepta la responsabilidad en la comisión de las siguientes infracciones recogidas en el acuerdo de inicio relacionadas con el caso concreto reclamado ante la Agencia que dio origen a la investigación realizada:

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del RGPD, con relación a la contratación no autorizada de productos.

- La infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por la falta de medidas de seguridad con relación a los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales,

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, con relación a la incorporación de datos personales en los sistemas de información crediticia.

TERCERO: BBVA procedió al pago de las sanciones impuestas por las infracciones cuya responsabilidad había sido aceptada, en la cuantía de 384.000 euros, haciendo uso de las dos reducciones previstas en el acuerdo de inicio.

CUARTO: El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el acuerdo de Inicio respecto a las infracciones cuya responsabilidad ha sido aceptada por BBVA.

QUINTO: Analizadas las alegaciones presentadas, con fecha 8 de septiembre de 2023, se emitió la siguiente propuesta de resolución:

<<

Expediente N.º: PS/00677/2022

PROPUESTA DE RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 12 de octubre de 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 adelante, la parte reclamada o BBVA). Los motivos en que basa la reclamación son los siguientes:

El día 13/04/2020 la reclamante solicitó a BBVA el bloqueo de su tarjeta número ******TARJETA.1*** al percatarse de la sustracción de esta.

La parte reclamante manifiesta que: "*En fecha de 14 de abril de 2020 BBVA es avisado por teléfono y por mail que, entre los días 10 y 13 de abril, la* ***Sra. A.A.A.*** *ha sido víctima de un robo del bolso (con móvil, tarjeta, y otros enseres personales) por una trabajadora de la Residencia (…), en Barcelona. La* ***Sra. A.A.A.*** *se hallaba temporalmente en dicha residencia para recibir un tratamiento oncológico. Se solicita a*

BBVA el bloqueo inmediato de todos los productos bancarios contratados por ***las Sras. A.A.A. y B.B.B.***.

"*BBVA hace caso omiso y permite que, en las semanas siguientes, con suplantación de identidad, terceros accedan a los productos bancarios de dichas señoras, operen con ellos (vaciando las cuentas, cargando facturas), contraten nuevos productos (préstamo, tarjeta, financiación Carrefour), realicen transferencias internacionales a países latinoamericanos desde dichas cuentas, etc*".

No obstante, según la parte reclamante, se producen cargos, transferencias y movimientos no consentidos en su cuenta, procediéndose a generar una deuda que no le corresponde, y que BBVA le reclama a través de diversas empresas de recobro.

Aporta junto a su escrito de reclamación informe de EXPERIAN de 18 de agosto y 8 de septiembre de 2020 sobre la inclusión de los datos de la parte reclamante a instancias de la reclamada; presentación de demanda ante el juzgado, en fecha 3 de septiembre de 2020; escrito de 31 de octubre de 2020, con reclamaciones de KRUK y de EXPERIAN; y escrito de 21 de septiembre de 2021, con reclamación de AXACTOR.

Junto a la notificación se aporta una demanda presentada por la parte reclamante en Juicio ordinario contra la parte reclamada, de fecha 01/09/2020.

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 10/12/2021 como consta en el acuse de recibo que obra en el expediente.

Con fecha 28/01/2022 se recibe en esta Agencia escrito de respuesta indicando lo siguiente: en primer lugar, incluye un resumen de los acontecimientos acaecidos a partir de abril de 2020:

> *El día 13/04/2020 la parte reclamante solicitó a BBVA el bloqueo de su tarjeta número* ******TARJETA.1*** *al percatarse de la sustracción de la misma según detalla en el escrito de demanda.*
>
> *Ese mismo día BBVA procedió al bloqueo de la tarjeta de manera inmediata, exactamente a las 18:07 h., si bien, esto no impidió que con anterioridad una persona no determinada suplantara la identidad de la Sra.* ***A.A.A.*** *y realizara diferentes operaciones, compras con la tarjeta bancaria y transferencias.*
>
> *El día 6/05/2020 el SAC recibió una comunicación de la Sra.* ***C.C.C.*** *solicitando la retrocesión de cualquier operación bancaria realizada desde el 10 de Abril de*

2020 con cargo a la cuenta, o a cualquier otro producto, titularidad de sus de sus representadas, las Sras. ***A.A.A. y B.B.B.*** *en BBVA.*

El día 3/07/2020 el SAC recibió una segunda carta de la Sra. ***C.C.C.*** *solicitando que se impidiera el acceso, por parte de terceros, a cualquier producto bancario titularidad de las Sras.* ***A.A.A. y B.B.B.,*** *así como el abono de los importes y conceptos reclamados previamente en mayo de 2020.*

El día 09/09/2020 la Sra. ***B.B.B.*** *se dirigió mediante correo electrónico a la Oficina del Defensor del Cliente solicitando la cancelación de diferentes productos titularidad de la Sra.* ***A.A.A.****, así como la retrocesión de los importes sustraídos y reclamados previamente a BBVA.*

El día 13/07/2020 BBVA requirió a la Sra. ***A.A.A.*** *el pago de la deuda derivada de descubierto en cuenta y de las cuotas de un préstamo personal, advirtiendo que "los datos de las deudas ciertas, vencidas, exigibles e impagadas con BBVA cuyo pago ha sido requerido previamente, serán comunicados a ASNEF, sistema de información crediticia en el que nuestra entidad participa, accesible para cualquier persona física o jurídica, todo ello de conformidad con lo establecido por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales".*

Dicha notificación se realizó por medio de la mercantil SERVINFORM, S.A. (en adelante, "Servinform"), empresa subcontratada por BBVA que certifica que dicha comunicación se generó, imprimió y ensobró sin que se generase incidencia alguna que alterase el resultado final del envío. El 13/07/2020 la comunicación número de referencia ******REFERENCIA.1*** *se puso a disposición del servicio de Correos para su posterior distribución, junto con un total de 870 comunicaciones. Se adjunta asimismo el albarán de entrega número* ******ALBARÁN.1.***

En relación al requerimiento indicado, el proveedor del servicio de control de devoluciones (servicio que Servinform tiene subcontratado a EQUIFAX IBERICA S.L) ha certificado con fecha 20/12/2021 que "no consta que la Carta de Certificación de Requerimiento Previo de Pago con ref. ******REFERENCIA.1****, generada en Equifax, en fecha 13/17/2020, procesada en el prestador del servicio SERVINFORM S.A., (antes MFASIS Billing & Marketing Services, S.L.) con fecha 13/07/2020, y puesta a disposición del servicio de envíos postales con fecha 13/07/2020, 15/07/2020; dirigida a* ***A.A.A.,*** *con dirección en* ******DIRECCIÓN.1****, en la localidad de ***LOCALIDAD.1 con Código Postal* ***(…)*** *– TARRAGONA, haya sido devuelta por motivo alguno al apartado de Correos designado a tal efecto". Documentos que se aglutinan todos ellos en el Documento nº 8.*

El día 8/09/2020 BBVA cedió los datos de la Sra. ***A.A.A.*** *al fichero de solvencia Badexcug/Experian por motivo de las referidas deudas.*

El día 22/09/2020 el Juzgado de Primera Instancia 10 de Barcelona notificó a BBVA la demanda prestada por la Sra. ***A.A.A.*** *en el seno del Procedimiento Ordinario* ******PROCEDIMIENTO.1*** *donde solicitaba, entre otros*

pronunciamientos, el abono de 6.090,14 euros por los cargos fraudulentos y 7.000 euros en concepto de lucro cesante o daños y perjuicios inmateriales.

BBVA, tal y como se ha acreditado, procedió al instante, al bloqueo de todos los instrumentos de pago asociados a la Sra. ***A.A.A.****. No obstante, BBVA no ha retrocedido los cargos efectuados con anterioridad puesto que las operaciones fueron validadas con el doble factor de autenticación.*

La parte reclamante sostiene que no ha prestado el consentimiento en las operaciones efectuadas entre el 10 y 13 de abril de 2020. No obstante, no podemos considerar aplicable el artículo 31 del Real Decreto Ley de Servicios de Pago que dispone que "en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada" pues las operaciones fueron autenticadas y registradas con exactitud y contabilizadas, y no se vieron afectadas por un fallo técnico o cualquier otra deficiencia.

El artículo 30 de la Ley de Servicios de Pago establece que "cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia."

A estos efectos, en el marco del procedimiento judicial tramitado por el Juzgado de Primera Instancia N 10 de Barcelona ***(***PROCEDIMIENTO.1****), se está discutiendo la procedencia o no de tal reclamación, donde conforme a las pruebas aportadas por las partes se resolverá si existió por parte de la parte reclamante falta de diligencia en la custodia de los mecanismos de seguridad facilitados por el Banco. BBVA no mantiene en el día de hoy informados los datos de la parte reclamante en ficheros de solvencia patrimonial y crédito.*

Por todo lo anterior, se pone de manifiesto que la actuación de BBVA ha sido diligente y conforme a la normativa de protección de datos, estando pendiente la resolución judicial sobre las cantidades dispuestas, y no realizando cesión de datos en la actualidad a ficheros de solvencia patrimonial y crédito.

TERCERO: Con fecha 12 de enero de 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,

Estas actuaciones tuvieron por objeto investigar los hechos denunciados en la reclamación y, como consecuencia de ello, también analizar el procedimiento que BBVA tiene establecido para las contrataciones de productos financieros y las garantías que en esos procedimientos se establecen para evitar supuestos como el producido. A través de esta investigación se tuvo conocimiento de los siguientes extremos:

Hechos según manifestaciones de la parte reclamante:

- Entre los días 10 y 13 de abril de 2020 la parte reclamante fue víctima del robo de su bolso en el que tenía, entre otras cosas, el teléfono móvil, el documento nacional de identidad, y la tarjeta de crédito.

- El día 13 de abril avisa al reclamado del robo sufrido y el 14 vuelve a solicitar el bloqueo de todos los productos bancarios contratados por la parte reclamante y por su hija. Así mismo, informa de que entre la documentación sustraída se encuentra la tarjeta de crédito, el DNI y el teléfono móvil, entre otros

- Expresa que el reclamado no procede correctamente al bloqueo solicitado lo que permite que terceros suplanten la identidad de las afectadas accediendo a sus productos bancarios y operando con ellos.

- Señala que el reclamado ha inscrito a la parte reclamante en sistemas de información crediticia y ha cedido sus datos a empresas de recobro (cita *"KRUK, EXPERIAN, AXACTOR"*).

Documentación relevante aportada por la parte reclamante:

- Demanda de juicio ordinario (en adelante la demanda) contra el reclamado presentada el 1 de septiembre de 2020 que contiene la descripción de los hechos.

- Escrito de ampliación de la demanda (primera ampliación de la demanda) de fecha 31 de octubre de 2020 (registro de presentación el 2 de noviembre de 2020) con referencia al ***"***PROCEDIMIENTO.1"*** en el que manifiesta que el reclamado ha continuado reclamando importes correspondientes a actos realizados por los delincuentes y ha incluido a la parte reclamante en un "fichero de morosos". Adjunta a varios documentos entre los que se incluye: correo electrónico dirigido el 9 de septiembre de 2020 al reclamado, escrito del 8 de septiembre de 2020 dirigido por Experian a la parte reclamante en el que le comunican la inclusión de una deuda procedente de un préstamo personal por el reclamado en el fichero Badexcug.

- Escrito de ampliación de la demanda de fecha 21 de septiembre de 2021 (segunda ampliación de la demanda) en el que se refiere que la entidad AXACTOR en nombre del reclamado ha contactado con la parte reclamante para gestionar una deuda pendiente de cobro. Adjunta copia de la carta.

El día 18 de enero de 2022 la parte reclamante presenta el escrito de número de registro ***(…)*** (ampliación de la reclamación) facilitando la siguiente documentación adicional en relación con los hechos denunciados:

- Carta dirigida por el reclamado a la parte reclamante para comunicarle la existencia de dos deudas relativas a los contratos ******CONTRATO.1*** y ******CONTRATO.2*** que se han comunicado al área de recobros. Además, le informa de que las deudas ciertas, vencidas, exigibles, e impagadas cuyo pago haya sido requerido pueden ser comunicadas a los sistemas de información crediticia.

- Carta de Equifax de fecha 24 de diciembre de 2021 en la que se informa de que el reclamado, el día 23 de diciembre de 2021, solicitó la inclusión de dos deudas por los conceptos de “préstamos personales” y “tarjetas de crédito”.

- Copia de un burofax de fecha 5 de enero de 2022 dirigido por la parte reclamante al reclamado en el que, en relación con la solicitud del pago de unas deudas recibida el 15 de diciembre de 2021, refiere la existencia de una demanda ***(“***PROCEDIMIENTO.1”)*** interpuesta el 1 de septiembre de 2020 en solicitud de declaración judicial de cierre y cancelación de cuentas y tarjetas bancarias y de exoneración de cualquier deuda por cualquier concepto originado en las mismas desde 10 de abril de 2020 en adelante. Cita que dicho proceso se encuentra pendiente de señalamiento para juicio. Manifiesta, asimismo, que la deuda no resulta atribuible a la parte reclamante y solicita la cancelación de sus datos personales en todos los ficheros a los que los hayan cedido (con inclusión de los ficheros de morosidad).

- Copia de un burofax de fecha 5 de enero de 2022 dirigido por la parte reclamante a Equifax con referencia al escrito previo. Refiere la existencia de una demanda ***(“***PROCEDIMIENTO.1”)*** interpuesta el 1 de septiembre de 2020 en solicitud de declaración judicial de cierre y cancelación de cuentas y tarjetas bancarias y de exoneración de cualquier deuda por cualquier concepto originado en las mismas desde 10 de abril de 2020 en adelante. Cita que dicho proceso se encuentra pendiente de señalamiento para juicio. Manifiesta asimismo que la deuda no resulta atribuible a la parte reclamante y solicita la eliminación de los datos personales de la parte reclamante de todos los ficheros de Equifax.

INTERVINIENTES

Además de los referidos anteriormente, durante las presentes actuaciones han intervenido:

- AXACTOR ESPAÑA PLATFORM, S.A. (en adelante, Axactor).
- EQUIFAX IBÉRICA, S.L. (en adelante, Equifax).
- EXPERIAN BUREAU DE CRÉDITO, S.A. (en adelante, Experian).
- INTRUM SERVICING SPAIN, S.A.U. (en adelante, Intrum)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Sobre el alcance de la investigación

La documentación facilitada por los intervinientes contiene detalles sobre productos vinculados no sólo a la parte reclamante sino también a la hija de la parte reclamante, el marido de ésta, y la empresa de este último. Asimismo, se nombran en algunos de los documentos actuaciones fraudulentas cometidas por los terceros contra la reclamada en relación con otras entidades (Sanitas, Iberia, El Corte Inglés, Movistar, Carrefour, etc.). Además, se cita a alguna de las personas que presuntamente habrían cometido el delito indicándose que se estaría procediendo también judicialmente contra las mismas. Dado que la reclamación ante esta agencia se ha presentado en nombre de la parte reclamante y en contra del reclamado la investigación se ciñe a la relación entre ambos y su impacto en el derecho a la protección de sus datos personales.

Cronología de los hechos

En las comunicaciones que se refieren a continuación el reclamado ha actuado tanto a través de direcciones genéricas asociadas a diferentes departamentos (defensor del cliente, departamento de seguridad, atención al cliente, etc.) como de trabajadores concretos (director de la sucursal y ayudante del mismo a la que se encontraba adscrita la parte reclamante). En esta cronología las del primer tipo se citan como procedentes o dirigidas al reclamado (sin especificación concreta del departamento). En el caso de las segundas se referencia al director de la sucursal o su ayudante.

De la información obtenida se ha obtenido la siguiente cronología de hechos:

- Según expone en la demanda la parte reclamante a principios de abril del año 2020 ingresa en una residencia para recibir un tratamiento médico.

- Añade en la demanda que, entre los días 10 y 13 de abril de 2020 una trabajadora de la residencia le sustrajo *"su móvil, […] tarjeta de crédito, […] y otra documentación personal de carácter esencial (DNI, carnet de conducir, [,,,])".*

- El día 13 de abril de 2020 se bloqueó la tarjeta número ******TARJETA.1*** de la parte reclamante. El reclamado manifiesta que procedió a su bloqueo *"de manera inmediata"* tras la solicitud de la parte reclamante. Facilita una impresión de pantalla en la que se aprecia la ejecución de una operación de bloqueo manual de la tarjeta ******TARJETA.1*** el día 13 de abril de 2020 a las 18:06 horas.

- El día 14 de abril de 2020 la hija de la parte reclamante se dirige por correo electrónico al reclamado -a la dirección de la ayudante del director de la sucursal para comunicar el robo sufrido por la parte reclamante (*"móvil, monedero, tarjetas, etc."*). En el escrito solicita cancelar *"todas"* las tarjetas de la parte reclamante y que le faciliten un número de teléfono al que poder llamar.

- El mismo día 14 de abril de 2020 el reclamado (la ayudante del director de la sucursal) responde al correo anterior señalando que la parte reclamante dispone de una única tarjeta (******TARJETA.1***) que fue bloqueada el 13 de abril.

Además, pregunta si el bloqueo se efectuó como consecuencia de una llamada previa al *"contact center"*. Asimismo, informa de que, con carácter previo al bloqueo, se habían realizado una serie de cargos *"a través de banca online que supongo que no a [sic] realizado ella"* que lista. Le expresa que, si no fueran correctos, necesitan una denuncia ante las fuerzas y cuerpos de seguridad para poder tramitar el fraude.

- El reclamado manifiesta que con anterioridad a la comunicación al banco del robo un tercero ya había suplantado la identidad de la parte reclamante y realizado operaciones. Añade, en relación con éstas, que no ha retrocedido los cargos ya que fueron validadas con doble factor de autenticación. En concreto señala que *"las operaciones fueron autenticadas y registradas con exactitud y contabilizadas, y no se vieron afectadas por un fallo técnico o cualquier otra deficiencia".*

    - Incluye un listado de cargos realizados con la tarjeta ******TARJETA.1*** entre el 11 de abril y el 30 de abril de 2020 por importe de 5.559,88 euros, realizados con posterioridad a la denuncia que realizó la parte reclamante ante el BBVA el 13 de abril.

    - Incluye detalles de movimientos de tipo transferencia y *"bizum"* producidos los días 14 y 24 de abril de 2020 en los que figura la parte reclamante como ordenante, realizados con posterioridad a la denuncia que realizó la parte reclamante ante el BBVA el 13 de abril.

- La parte reclamante en la demanda señala que *"intentaron dar de baja la línea de móvil relativa al aparato sustraído,* ******TELÉFONO.1****, desde la propia página web de Telefónica y realizando infinitas llamadas a la misma."*

- El día 16 de abril de 2020 el reclamado (el director de la sucursal) envía un correo electrónico en el que expresa que es necesaria la denuncia ante las fuerzas y cuerpos de seguridad para realizar la investigación.

- El día 17 de abril de 2020 la hija de la parte reclamante dirige un correo electrónico al reclamado (al director de la sucursal) expresándole que le enviará copia de la denuncia la representante de la parte reclamante. El mismo día 17 de abril de 2020 la representante de la parte reclamante envía un correo electrónico al director de la sucursal en el que se presenta y manifiesta adjuntar la denuncia.

  Adjunta al escrito la denuncia presentada el día 16 de abril de 2020 ante los Mossos d'Esquadra. La denuncia es presentada por ***D.D.D.*** en representación de la parte reclamante. Adjunta escrito en el que la hija de la parte reclamante autoriza a ***D.D.D.*** a interponer la denuncia en nombre de la parte reclamante y su hija. La denuncia se interpone contra la residencia de ancianos en la que se encontraba la parte reclamante cuando acaeció el robo de sus pertenencias. En la denuncia se indica que le habrían sustraído la tarjeta de crédito, el teléfono móvil, y el DNI entre otras pertenencias. En la propia denuncia cita que contactaron con el reclamado y que éste les informó de que se había retirado dinero con la tarjeta con anterioridad.

- El día 20 de abril de 2020 el reclamado (director de la sucursal) dirige un correo electrónico a la representante de la parte reclamante en el que le comunica que ha dado traslado de la denuncia al departamento de seguridad y fraudes. Asimismo, en la denuncia se indica que el director de la sucursal les habría comunicado que alguien habría solicitado la emisión de dos tarjetas a nombre de la parte reclamante.

- El día 1 de mayo de 2020 ***D.D.D.*** presenta ante los Mossos d'Esquadra una ampliación de la denuncia en nombre de la parte reclamante, en la que señala que el director de la sucursal del reclamado les ha comunicado que alguien ha contactado identificándose como la parte reclamante solicitando el alta de un número de teléfono en la base de datos del reclamado como teléfono de contacto de la parte reclamante. Expresa que desde el banco le han comunicado que esa gestión debe hacerse presencialmente.

Productos de la parte reclamante impactados

Manifiesta la parte reclamante que los terceros realizaron operaciones tras el robo sobre los siguientes productos que tenía contratados con el reclamado con anterioridad (expresa no haber realizado ella los movimientos posteriores al 11 de abril de 2020):

- Cuenta número ******CUENTA.1*** de la cual el reclamado especifica que no está cancelada. Facilita la copia de la información precontractual y del contrato. La parte reclamante en la demanda reconoce que era titular de la cuenta con anterioridad al robo.

  La parte reclamante facilita un listado de movimientos sobre esta cuenta realizados entre el 17 de abril y el 7 de julio de 2020, realizados con posterioridad a la denuncia que realizó la parte reclamante ante el BBVA el 13 de abril. Además, en la demanda la parte reclamante expresa que "*todos los movimientos realizados desde 17 de Abril hasta 5 de Mayo de 2020, han sido realizados por los delincuentes, y todos los movimientos realizados desde 17 de Junio hasta 7 de Julio de 2020, han sido realizados por el Banco".* Igualmente en la demanda la parte reclamante expresa que la cuenta *"ha sido bloqueada por el Banco suponemos que durante la primera semana de Junio de 2020".*

  El reclamado facilita una impresión de pantalla en la que se aprecia la ejecución de un bloqueo para cargos en esta cuenta de fecha 31 de agosto de 2020. En las observaciones constan referencias a bloqueos previos realizados el día 4 de mayo de 2020 y el día 11 de agosto de 2020.

- Cuenta número (******CUENTA.2***) -reconocida por la parte reclamante su titularidad con anterioridad al robo en la demanda-. La parte reclamante facilita un listado de movimientos sobre esta cuenta realizados entre el 14 de abril y el 17 de junio de 2020. Según expresa en la demanda *"los movimientos efectuados desde 13 de Abril hasta 4 de Mayo de 2020, han sido realizados por los delincuentes"* y *"Los movimientos realizados desde 5 de Mayo hasta 17*

de Junio de 2020, han sido realizados por el Banco". Igualmente en la demanda la parte reclamante expresa que la cuenta se encuentra bloqueada (*"creemos que desde mediados de Junio de 2020"*).

El reclamado facilita una impresión de pantalla en la que se aprecia la ejecución de un bloqueo para cargos en esta cuenta de fecha 4 de mayo de 2020. Asimismo, proporciona una captura de pantalla que refiere el bloqueo de abonos realizado el día 25 de junio de 2020.

- Tarjeta número ******TARJETA.1*** vinculada al contrato ******CONTRATO.2*** que fue sustraída según lo dispuesto en la demanda.

    - Facilita una impresión de pantalla en la que se aprecia la ejecución de una operación de bloqueo manual de la tarjeta ******TARJETA.1*** el día 13 de abril de 2020 a las 18:06 horas.

    - Adjunta el escrito del día 15 de mayo de 2020 en el que la parte reclamante comunica al reclamado, como titular de la tarjeta, el robo y solicita la devolución del importe de un conjunto de movimientos que lista. El listado incluye cargos producidos entre el 11 de abril y el 30 de abril de 2020. En la demanda expresa que el banco *"ha reconocido responsabilidad sobre los movimientos operados en relación con dicha tarjeta por importe de 5559,88 euros."*

    - En un escrito expresa el reclamado que *"Se ha solicitado información sobre las operaciones realizadas con tarjeta con posterioridad a la fecha del bloqueo, y sobre los cambios en el bloqueo de tarjeta de referencia".*

Igualmente, la parte reclamante manifiesta que los terceros suplantaron su identidad contratando nuevos productos con el banco. A saber:

- Préstamo de 4.000 euros suscrito el 12 de abril de 2020 del cual el reclamado especifica que no está cancelado. Facilita la copia del contrato, en el que figuran el nombre, apellidos, dirección, y DNI de la parte reclamante. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* con fecha 12 de abril de 2020.

- Tarjeta número ******TARJETA.2*** vinculada al contrato ******CONTRATO.3***. Sobre esta tarjeta la parte reclamante señala se solicitó desde su número de teléfono móvil y se envió a su dirección. Asimismo expresa que los terceros la usaron posteriormente para realizar operaciones.

  El reclamado manifiesta que se contrató el día 15 de abril de 2020 y facilita la copia de del contrato, en el que figuran el nombre, apellidos, y DNI de la parte reclamante. Refiere que se firmó electrónicamente la solicitud de la tarjeta a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* el 15 de abril de 2020.

La parte reclamante adjunta el escrito del día 16 de junio de 2020 en el que comunica al reclamado, como titular de la tarjeta, el robo y solicita la devolución del importe de un conjunto de movimientos que lista. El listado incluye cargos producidos entre el 17 de abril y el 3 de mayo de 2020. En la demanda expresa que el banco *"ha reconocido responsabilidad sobre los movimientos operados en relación con dicha tarjeta, por importe de 404,84 euros."*

El reclamado aporta una captura de pantalla que muestra la incidencia con motivo *"robo de tarjeta"* comunicada el día 16 de junio de 2020. En los cometarios figura, para el día 16 de junio de 2020 el siguiente: *"Alta de incidencia/fraude Adjuntamos denuncia presentada y bloqueamos claves de acceso, tarjeta, cuenta, y damos de baja el móvil validado. Informado el departamento de fraudes"*. Facilita además una captura de pantalla de sus sistemas en la que consta el 6 de julio de 2020 como fecha de bloqueo de la tarjeta. Asimismo la tarjeta figura en situación de extravío y el contrato en estado cancelado.

- Cuenta número ******CUENTA.3*** (la parte reclamante cita "una cuenta terminada en ***XX***" en correo del 9 de septiembre de 2020) suscrita el 27 de abril de 2020 de la cual el reclamado especifica que no está cancelada. Facilita la copia de del contrato, en el que figuran el nombre, apellidos, dirección, y DNI de la parte reclamante. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* con fecha 27 de abril de 2020. El reclamado señala además otros detalles de la contratación (dirección IP y validación en la *"app"* del reclamado a través de huella dactilar).

Además de los anteriores, el reclamado ha referido los siguientes productos contratados con posterioridad al 10 de abril de 2020 que se encuentran cancelados (en la demanda la parte reclamante refiere asimismo que el banco expidió dos nuevas tarjetas bancarias a solicitud de los delincuentes):

- Tarjeta número ******TARJETA.3*** vinculada al contrato ******CONTRATO.4*** suscrito el 15 de abril de 2020 de la cual el reclamado especifica que se encuentra cancelada**.** Facilita la copia de del contrato, en el que figuran el nombre, apellidos, DNI de la parte reclamante, y el correo electrónico ******EMAIL.1***. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* con fecha 15 de abril de 2020. La dirección de correo electrónico ******EMAIL.1***, según dispone el escrito presentado ante el juzgado de fecha 18 de mayo de 2020, sería una cuenta de la parte reclamante a la que habrían tenido acceso los terceros.

  Anexa también impresión de pantalla de sus sistemas en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo.

- Tarjeta número ******TARJETA.4*** vinculada al contrato ******CONTRATO.5*** suscrito el 15 de abril de 2020 de la cual el reclamado especifica que se encuentra cancelada**.** Facilita la copia de del contrato, en el que figuran el nombre,

apellidos, DNI de la parte reclamante, y el correo electrónico ***EMAIL.1**. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* con fecha 15 de abril de 2020. La dirección de correo electrónico ***EMAIL.1**, según dispone el escrito presentado ante el juzgado de fecha 18 de mayo de 2020, sería una cuenta de la parte reclamante a la que habrían tenido acceso los terceros.

Anexa también impresión de pantalla de sus sistemas en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo.

Situación del procedimiento judicial

Adjunta la parte reclamante la demanda de juicio ordinario contra el reclamado presentada el 1 de septiembre de 2020 que contiene la descripción de los hechos.

Manifiesta el reclamado lo siguiente en relación con el procedimiento judicial abierto y su responsabilidad en la suplantación de identidad sufrida por la parte reclamante:

"La parte reclamante sostiene que no ha prestado el consentimiento en las operaciones efectuadas entre el 10 y 13 de abril de 2020. No obstante, no podemos considerar aplicable el artículo 31 del Real Decreto Ley de Servicios de Pago que dispone que "en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada" pues las operaciones fueron autenticadas y registradas con exactitud y contabilizadas, y no se vieron afectadas por un fallo técnico o cualquier otra deficiencia.

El artículo 30 de la Ley de Servicios de Pago establece que "cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia.

*A estos efectos, en el marco del procedimiento judicial tramitado por el Juzgado de Primera Instancia N 10 de Barcelona (**PROCEDIMIENTO.1), se está discutiendo la procedencia o no de tal reclamación, donde conforme a las pruebas aportadas por las partes se resolverá si existió por parte de la parte reclamante falta de diligencia en la custodia de los mecanismos de seguridad facilitados por el Banco."*

La parte reclamante ha señalado, con relación a la situación del procedimiento judicial abierto, lo siguiente:

"1.-Proceso penal: ha finalizado recientemente la fase de instrucción. Solicitados los escritos de calificación.
2.-Proceso civil: señalado juicio para el 20 de julio de 2022."

Situación en los sistemas de información crediticia

Señala el reclamado que los vencimientos cuyo impago motivo la inclusión de los datos de la parte reclamante en sistemas de información crediticia derivaron de los contratos de préstamo ******CONTRATO.1*** y de tarjeta ******CONTRATO.2*** (tarjeta número ******TARJETA.1***). A tal efecto aporta (EscritoReclamado#2) la siguiente información:

- Impresión de pantalla de sus sistemas en la que, para el préstamo figura un saldo impagado de 4.466,27 euros con fecha de primer y último vencimientos el 31 de mayo de 2020 y el 9 de diciembre de 2021, respectivamente. Señala que el 6 de septiembre de 2020 procedió al registro de la deuda en el fichero BADEXCUG (importe de alta 937,37 euros) y el 7 de enero de 2022 ordenó su baja (importe de baja 4.493,12 euros). Asimismo, indica que el 23 de diciembre de 2021 procedió al registro de la deuda en el fichero ASNEF (importe de alta 4.485,71 euros) y el 7 de enero de 2022 ordenó su baja (importe de baja 4.485,71 euros).

- Impresión de pantalla de sus sistemas en la que, para la tarjeta figura un saldo impagado de 6.544,43 euros con fecha de primer y último vencimientos el 5 de mayo de 2020 y el 9 de diciembre de 2021, respectivamente. Señala que el 16 de agosto de 2020 procedió al registro de la deuda en el fichero BADEXCUG (importe de alta 5.494,75 euros) y el 7 de enero de 2022 ordenó su baja (importe de baja 6.607,46 euros). Asimismo, indica que el 23 de diciembre de 2021 procedió al registro de la deuda en el fichero ASNEF (importe de alta 6.590,06 euros) y el 7 de enero de 2022 ordenó su baja (importe de baja 6.590,36 euros).

Sobre el motivo por el que se incorporaron las deudas de la parte reclamante a los sistemas de información crediticia a pesar de existir una reclamación judicial que afectaba a las mismas, el reclamado manifiesta lo siguiente:

"Notificada a BBVA una demanda en el que cuestiona la certeza de la deuda el letrado del procedimiento tiene instrucciones de solicitar: (i) la baja, según corresponda temporal o definitiva; (ii) solicitar que el contrato no se informe en sistemas de información crediticia a futuro. En este caso no se solicita la baja o no inclusión de los contratos por un error puntual no intencionado."

Expresa, en relación con el motivo de la exclusión de los datos de la parte reclamante de los ficheros de morosidad, que se solicitó *"en la tramitación del expediente que nos traslada la AEDP [sic]".* Facilita el reclamado una carta de fecha 10 de enero de 2022 en la que manifiesta que en dicha fecha los datos de la parte reclamante y de su hija no se encuentran cedidos por BBVA a sistemas de información crediticia.

Según los datos aportados por Equifax, a día 14 de junio de 2022, no existen deudas informadas por el reclamado en relación con la parte reclamante en sus ficheros de

información crediticia. Sin embargo, sí refiere la inscripción y posterior baja de los siguientes en ASNEF:

- Préstamo personal de código de operación ******CONTRATO.1*** con saldo impagado de 4.485,71 euros. Refiere 18 cuotas impagadas entre los meses de mayo de 2020 y diciembre de 2021. Especifica como fechas de alta y baja en ASNEF el 23 de diciembre de 2021 y el 7 de enero de 2022, respectivamente. Consigna el 22 de enero de 2022 como "fecha de visualización".

- Tarjeta de crédito de código de operación ******CONTRATO.2*** con saldo impagado de 6.590,06 euros. Refiere 7 cuotas impagadas entre los meses de mayo de 2020 y diciembre de 2021. Especifica como fechas de alta y baja en ASNEF el 23 de diciembre de 2021 y el 7 de enero de 2022, respectivamente. Consigna el 22 de enero de 2022 como "fecha de visualización".

Según los datos aportados por Experian no existen deudas informadas por el reclamado en relación con la parte reclamante en sus ficheros de información crediticia. Sin embargo, sí refiere la inscripción y posterior baja de los siguientes en BADEXCUG:

- Préstamo personal de código de operación ******CONTRATO.1*** con fechas de alta y baja en BADEXCUG el 6 de septiembre de 2020 y el 7 de enero de 2022, respectivamente.

- Tarjeta de crédito de código de operación ******CONTRATO.2*** con fechas de alta y baja en BADEXCUG el 16 de agosto de 2020 y el 7 de enero de 2022, respectivamente.

Situación de los procedimientos de recuperación de las deudas

Según la información facilitada por el reclamado se asignó a Axactor la deuda de la parte reclamante para su recuperación el día 12 de julio de 2021. Igualmente especifica que éstas fueron desasignadas el 16 de noviembre de 2021.

Axactor ha confirmado el tratamiento de los datos personales de la parte reclamante por cuenta del reclamado en virtud del contrato de prestación de servicios recuperatorios que mantienen suscrito. Sobre ello facilita la siguiente información:

- Adjunta al escrito el contrato de prestación de servicios recuperatorios suscrito entre el reclamado y Axactor del día 2 de julio de 2021. Incluye la condición general octava y el anexo 8.2 relativos al tratamiento de datos personales. En este último se especifica que Axactor actúa como encargado de tratamiento del reclamado con acceso a los datos de los clientes (nombre, apellidos, dirección postal, email, teléfono y datos económicos) para la ejecución de las prestaciones del contrato.

- Adjunta al escrito el registro de las categorías de actividades de tratamiento que efectúa Axactor por cuenta del reclamado que incluye la información sobre la actividad *"Recuperación de activos impagados"*.

- Adjunta los expedientes de recuperación de deuda gestionados por Axactor para el reclamado en los que la parte reclamante ostenta la posición de deudora. Incluyen lo siguiente:

    - Expediente relativo a un préstamo personal de cuatro mil euros concedido el 12 de abril de 2020 de referencia cliente ******CONTRATO.1******. Consigna las fechas de alta y baja del expediente 15 de julio de 2021 y 17 de noviembre de 2021, respectivamente. Contiene el nombre, apellidos, dirección, y número de DNI de la parte reclamante, además de la información relativa al préstamo. Incluye una única gestión, de fecha 10 de septiembre de 2021, denominada *"101 - Carta Hello. Petición: (…). Dirección: ***DIRECCIÓN.1. BarCode:* ***(…)***".

    - Expediente relativo a una tarjeta de 6.463,10 euros cedidos con fecha de inicio de la deuda 5 de mayo de 2020 y referencia cliente ******CONTRATO.2*****. Consigna las fechas de alta y baja del expediente 15 de julio de 2021 y 17 de noviembre de 2021, respectivamente. Contiene el nombre, apellidos, dirección, y número de DNI de la parte reclamante, además de la información relativa a la deuda. No incluye gestiones realizadas en relación con este expediente.

    - Expediente relativo a un descubierto de 74,23 euros cedidos con fecha de inicio de la deuda 4 de mayo de 2020 y referencia cliente ******REFERENCIA.1******. Consigna las fechas de alta y baja del expediente 15 de julio de 2021 y 17 de noviembre de 2021, respectivamente. Contiene el nombre, apellidos, dirección, y número de DNI de la parte reclamante, además de la información relativa a la deuda. No incluye gestiones realizadas en relación con este expediente.

Entre la información facilitada figura además que Intrum habría accedido a los datos de la parte reclamante por cuenta del reclamado. A este respecto, incluye capturas de pantalla de los sistemas del reclamado con la siguiente información:

- Expediente relativo a una deuda por importe de 12.416,29 euros por el producto *"TARJETAS DE CRÉDITO"* en situación de *"PROCESO FINALIZADO"* a día 18 de noviembre de 2021.

- El día 10 de mayo de 2021 figura la primera anotación. Manifiesta el reclamado que en dicha fecha se *"inicia procedimiento prejudicial y se acompaña la liquidación de la tarjeta".*

- El día 18 de noviembre de 2021 figura la última anotación. Manifiesta el reclamado que en dicha fecha se *"cancela el procedimiento por ser la deuda inferior a 6.000 euros".*

CONCLUSIONES

Según la información recabada existen procedimientos judiciales abiertos en relación con los hechos investigados en las presentes actuaciones. Uno de los procedimientos judiciales se inició a raíz de una demanda de juicio ordinario presentada por la parte

reclamante contra el reclamado el día 1 de septiembre de 2020 (***PROCEDIMIENTO.1**).

Estas actuaciones previas de investigación fueron iniciadas a raíz de una reclamación en la que la parte reclamante expresa que, tras comunicar al reclamado que fue víctima del robo de su bolso el reclamado no procedió correctamente permitiendo que terceros suplantasen su identidad tanto operando con sus productos bancarios como contratando nuevos productos a su nombre. Manifiesta además la parte reclamante que, como consecuencia de las operaciones realizadas por los suplantadores, la entidad le ha reclamado el importe de unas deudas a través de empresas de recobros y ha incluido sus datos personales en sistemas de información crediticia. Entre la información obtenida se señala que los suplantadores habrían podido utilizar tanto la línea de teléfono de la parte reclamante como su dirección de correo electrónico.

La parte reclamante se trata de una persona que fue víctima del robo mientras se sometía a un tratamiento médico en las instalaciones de una residencia de ancianos. Las comunicaciones con el reclamado en nombre de la parte reclamante al objeto de bloquear sus productos y evitar las suplantaciones de identidad fueron realizadas, además de por la propia reclamante, por su hija y por otra persona (su representante) en su nombre. Ello dio lugar a que los distintos departamentos del reclamado (sucursal de la que era clienta, departamento de atención al cliente, etc.) procedieran de formas distintas a la hora de validar la capacidad de representación de estos terceros de la parte reclamante. El detalle de estas cuestiones se ha incluido en un apartado ad hoc del informe de inspección.

La cronología de los hechos extraída de los documentos aportados al presente expediente se ha consignado igualmente en el apartado correspondiente del citado informe de inspección. De ella se extraen los siguientes datos de interés para contextualizar los hechos:

- Los “delincuentes”, por lo que se ha visto, habrían sustraído pertenencias de la parte reclamante que les facilitaron la suplantación de identidad: documento nacional de identidad “físico”, línea de teléfono móvil, y tarjeta de crédito.

- Los “delincuentes”, por lo que se puede deducir de la información obtenida, habrían tenido acceso al buzón de correo electrónico y a la banca online de la parte reclamante.

- La parte reclamante el 14 de abril comunicó a la sucursal del reclamado de referencia el robo con indicación de que le habían sustraído además de la tarjeta, el documento nacional de identidad y el teléfono si bien solicitó únicamente la cancelación de sus tarjetas. La tarjeta que tenía operativa se bloqueó el 13 de abril (alguien se comunicó por teléfono previamente). Sin embargo, esta tarjeta se desbloqueó posteriormente y los “delincuentes” pudieron hacer movimientos hasta el 30 de abril (el reclamado no ha argumentado por qué se produjo el desbloqueo).

Además, los “delincuentes” habrían operado con los productos de la parte reclamante y contratado nuevos productos suplantados su identidad. Se listan a continuación:

- Préstamo suscrito el 12 de abril de 2020 (con anterioridad a la comunicación del robo al reclamado) del cual se ha facilitado la copia del contrato en la que figuran los datos personales de la parte reclamante. Refiere el reclamado que se firmó a distancia electrónicamente a solicitud de la parte reclamante.

- Tarjeta número ******TARJETA.1*** de la cual la parte reclamante reconoce que era titular con anterioridad al robo. Se facilita un listado que incluye cargos producidos entre el 11 de abril y el 30 de abril de 2020. El reclamado aporta información en la que se aprecia la ejecución de una operación de bloqueo el día 13 de abril de 2020. No ha explicado por qué se produjeron cargos con posterioridad.

- Cuenta número ******CUENTA.1*** de la cual la parte reclamante reconoce que era titular de la cuenta con anterioridad al robo. Manifiesta que los movimientos realizados entre el día 17 de abril y el 5 de mayo de 2020 fueron realizados por los suplantadores. El reclamado facilita información en la que consta un primer bloqueo de los cargos sobre esta cuenta el día 4 de mayo de 2020.

- Cuenta número ******CUENTA.2*** de la cual la parte reclamante reconoce que era titular con anterioridad al robo. Manifiesta que los movimientos realizados entre el día 13 de abril y el 4 de mayo de 2020 fueron realizados por los suplantadores. El reclamado facilita información en la que consta un primer bloqueo de los cargos sobre esta cuenta el día 4 de mayo de 2020.

- Tarjeta número ******TARJETA.2*** que se contrató el día 15 de abril de 2020 (en esa fecha consta que se había comunicado el robo sufrido a la sucursal, pero no se había facilitado la denuncia ante las fuerzas y cuerpos de seguridad) con los datos de la parte reclamante y se firmó a distancia electrónicamente. El reclamado señala que se envió a la dirección de la parte reclamante. Se facilita un listado que incluye cargos producidos entre el 17 de abril y el 3 de mayo de 2020. Consta que el robo de la tarjeta fue comunicado el día 16 de junio de 2020.

- Tarjeta número ******TARJETA.3*** que se contrató el día 15 de abril de 2020 (en esa fecha consta que se había comunicado el robo sufrido a la sucursal, pero no se había facilitado la denuncia ante las fuerzas y cuerpos de seguridad) con los datos de la parte reclamante y se firmó a distancia electrónicamente. El reclamado facilita información en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo.

- Tarjeta número ******TARJETA.4*** que se contrató el día 15 de abril de 2020 (en esa fecha consta que se había comunicado el robo sufrido a la sucursal, pero no se había facilitado la denuncia ante las fuerzas y cuerpos de seguridad) con los datos de la parte reclamante y se firmó a distancia electrónicamente. El reclamado facilita información en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo.

- Cuenta número ******CUENTA.3*** (la parte reclamante cita “una cuenta terminada en ***XX***” en correo del 9 de septiembre de 2020) suscrita el 27 de abril de 2020.

Se facilita la copia de del contrato en la que figuran los datos de la parte reclamante. Refiere además que se firmó a distancia electrónicamente.

El reclamado ha facilitado documentación que recoge el procedimiento que sigue en términos de prevención de fraudes y estafas. Incluye instrucciones para las oficinas al objeto de registrar en los sistemas las comunicaciones de hurtos o extravíos de los documentos de identificación de los clientes. Incluye asimismo la obligación del cliente de custodiar tanto la tarjeta como el *"PIN"* y comunicar inmediatamente las incidencias. Indica asimismo que en estos casos lo inmediato es el bloqueo de la tarjeta.

A raíz de las acciones anteriormente descritas se derivaron algunas deudas que el reclamado inscribió en sistemas de información crediticia. El detalle de las inscripciones y posteriores exclusiones se puede consultar en el apartado correspondiente del informe de inspección. La exclusión, según expresa el reclamado, se solicitó en la tramitación del expediente trasladado por la AEPD. Igualmente, el reclamado manifiesta que el procedimiento es por no incluir aquellas deudas cuya certeza se encuentra cuestionada en un procedimiento, si bien en este caso se produjo *"un error puntual no intencionado".* Consta asimismo que las deudas fueron asignadas (y posteriormente desasignadas) a dos entidades de recuperación por el reclamado.

QUINTO: Con fecha 11 de enero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a BBVA a fin de imponerle multas por un importe total de 1.640.000 euros, con arreglo a lo dispuesto en los artículos 63 y 64 de la LPACAP, por la presunta comisión de las siguientes infracciones:

Tres relacionadas con el caso concreto denunciado por la reclamante:

- Por la presunta infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del RGPD, en relación con la contratación no autorizada de productos.
- Por la presunta infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por la falta de medidas de seguridad en relación con los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales
- Por la presunta infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, en relación con la incorporación de datos personales en los sistemas de información crediticia.

Y dos relacionadas con la forma en la que se establecieron los procedimientos implantados por el BBVA y que fueron revelados a través de la información aportada por la entidad financiera durante las actuaciones de investigación:

- Por la presunta infracción del artículo 25 del RGPD tipificada en el artículo 83.4 del mismo Reglamento.
- Por la presunta infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por con la falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros

En el citado acuerdo de inicio se le indicaba al BBVA que tenía un plazo de diez días para presentar alegaciones.

Este acuerdo de inicio, que se notificó al BBVA conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogido en fecha 13 de enero de 2023, como consta en el acuse de recibo que obra en el expediente.

SEXTO: Con fecha 13 de enero de 2023, BBVA presenta un escrito a través del cual solicita la ampliación del plazo para aducir alegaciones, que se le facilite copia de los documentos obrantes en el expediente, así como aclaración sobre el importe de la sanción.

SÉPTIMO: Con fecha 26 de enero de 2023, la Directora de esta Agencia dicta resolución de rectificación de errores, por la cual se corrige el error detectado en la página 42 del acuerdo de inicio del presente procedimiento, concediendo al BBVA un nuevo plazo de diez días hábiles para que formule las alegaciones y proponga las pruebas que considere procedentes y otorgando un nuevo plazo de diez días para el pago voluntario de la sanción.

La citada resolución se notifica a BBVA en fecha 27 de enero de 2023, como consta en el acuse de recibo que obra en el expediente

OCTAVO: Con fecha de 26 de enero de 2023 la secretaria del procedimiento dicta acuerdo de remisión al BBVA copia del expediente.

El citado acuerdo se notifica a BBVA en fecha 30 de enero de 2023, como consta en el acuse de recibo que obra en el expediente.

NOVENO: Con fecha 10 de febrero de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de BBVA en el que, por una parte, se aduce alegaciones al acuerdo de inicio respecto a la presunta infracción del artículo 25 del RGPD y a la presunta infracción del artículo 32 del RGPD por falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros y, por otra parte, se acepta la responsabilidad en la comisión de las siguientes infracciones recogidas en el acuerdo de inicio relacionadas con el caso concreto reclamado ante la Agencia que dio origen a la investigación realizada:

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del RGPD, con relación a la contratación no autorizada de productos.

- La infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por la falta de medidas de seguridad con relación a los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales,

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, con relación a la incorporación de datos personales en los sistemas de información crediticia.

DÉCIMO: Con fecha 13 de julio de 2023, el órgano instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporados a efectos probatorios la reclamación interpuesta por la parte reclamante y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento AI/00068/2022.

Asimismo, se daban por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por el BBVA, y la documentación que a ellas acompaña.

Por último, se daba por reproducida a efectos probatorios, sentencia aportada por la parte reclamante, dictada por el Juzgado de Primera Instancia nº 10 de Barcelona de fecha ***FECHA.1, con ******SENTENCIA.1***.

Ese mismo día, 13 de julio de 2023, esta Agencia requirió a BBVA para que en el plazo de diez días hábiles presentara la siguiente información:

1) La evaluación de impacto de protección de datos (en adelante EIPD), fechada y firmada, en materia del tratamiento de los datos personales de los clientes del BBVA en materia de "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*", vigente el 14/04/2020, fecha en la que la hija de la parte reclamante comunicó al BBVA el robo sufrido por la parte reclamante ("móvil, monedero, tarjetas, etc."), así como toda la documentación previa a la EIPD en la que se haya plasmado la necesidad de la decisión de realizar la EIPD; asimismo se precisa toda la documentación elaborada con ocasión de la realización de la EIPD y justificativa de los resultados obtenidos en la EIPD y de las medidas adoptadas al respecto, incluyendo la documentación relativa a participación del Delegado de Protección de Datos del BBVA en la elaboración de la misma.

En el caso de que se hubiera considerado que no procedía realizar una EIPD, la documentación justificativa (fechada y firmada) en la que se recojan los motivos por los que el BBVA consideraba que no estaba obligado a hacer la EIPD, incluyendo la documentación relativa a la intervención del Delegado de Protección de Datos donde expresó su criterio en esta cuestión. En tal caso, aportar la documentación acreditativa del análisis de riesgos efectuado, incluyendo toda la elaborada, justificativa de los resultados obtenidos y de las medidas adoptadas.

2) Documentación fechada y firmada relativa a las medidas técnicas y organizativas que tenía previstas el BBVA en fecha 14/04/2020 para evitar el fraude por suplantación de identidad, concretamente, en las operaciones a través de "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*", cuando se ha producido la sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, y esta circunstancia ha sido comunicada por el cliente.

3) Documentación fechada y firmada relativa a las medidas técnicas y organizativas que el BBVA tenía implantadas con fecha 14/04/2020, para que las comunicaciones realizadas a la entidad por sus clientes por la pérdida, extravío o sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación)

o las tarjetas de crédito, produzcan efecto en sus diversos canales de relación con el cliente relativos la operativa que este pueda realizar.

El citado acuerdo se notifica a BBVA en fecha 14 de julio de 2023, como consta en el acuse de recibo que obra en el expediente.

En la actualidad, no consta en la AEPD que BBVA hubiera presentado escrito de respuesta al requerimiento de información de esta Agencia.

UNDÉCIMO: Se acompaña como anexo relación de documentos obrantes en el procedimiento.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: A principios de abril de 2020, la parte reclamante tenía dos cuentas abiertas en BBVA, la nº. ******CUENTA.1*** y la nº. ******CUENTA.2***, además de una tarjeta de crédito, número ******TARJETA.1***

SEGUNDO: Conforme a la sentencia ***SENTENCIA.1 de ***FECHA.1, dictada por el Juzgado de Primera Instancia nº 10 de Barcelona, con fecha 10 de abril de 2020, estando ingresada en la residencia (…) la parte reclamante fue víctima del robo de su bolso en el que tenía, entre otras cosas, el teléfono móvil, el documento nacional de identidad, y la tarjeta de crédito número ******TARJETA.1***.

TERCERO: Con fecha 12 de abril de 2020 fue contratado con BBVA un préstamo con código de operación ******CONTRATO.1*** por un importe de 4.000 euros. El BBVA facilita la copia del contrato, en el que figuran el nombre, apellidos, dirección, y DNI de la parte reclamante. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* con fecha 12 de abril de 2020.

CUARTO: Con fecha 13 de abril de 2020 la parte reclamante solicitó a BBVA el bloqueo de su tarjeta número ******TARJETA.1*** al percatarse de la sustracción de esta según detalla en el escrito de demanda. Ese mismo día BBVA procedió al bloqueo de la tarjeta de manera inmediata, exactamente a las 18:07 h.

QUINTO: Con fecha 14 de abril de 2020 se produce el siguiente intercambio de correos entre la hija de la parte reclamante y BBVA:

- Desde el correo electrónico de la hija de la parte reclamante ******EMAIL.2*** (página 257 del expediente), se envió el siguiente mensaje:

> "*Hola*
> *Os escribo desde USA*

Ayer le robaron a mi madre, en la residencia en la que se encuentra ingresada por su tratamiento de cancer, el móvil, el monedero y tarjetas etc. por favor urgente cancelar todas sus tarjetas, creo que tiene 2 pero no tengo los números conmigo aqui
Donde os puedo llamar ¿???
Gracias
--
B.B.B." (el subrayado es nuestro).

- Desde el correo ******USUARIO.1***@bbva.com, se envía el siguiente mensaje:

*"Buenos días **B.B.B.***
Ahora he visto tu e mail.
Solamente tiene una tarjeta y veo que ayer 13/04/2020 a las 18:06 fue bloqueada. Llamasteis vosotros al contact center de BBVA???
Lo que veo que tiene diversos cargos a través de banca online que supongo no ha realizado ella.
Adjunto cargos realizados para que le des un vistazo… Si no fueran correctos necesitamos una denuncia de los mossos para poder tramitar el alta del fraude.

Espero que ella esté bien.
Att,"

- Desde el correo ******EMAIL.2*** se envía el siguiente mensaje:

"*Hola a todos,*
*envío este email para poder conectar a **E.E.E.** y **F.F.F.** del BBVA, con **G.G.G.**, Directora de la residencia (…) en la que se encuentra mi madre, y **D.D.D**, familiar involucrado en el cuidado de mi madre, al estar yo en USA.*

***E.E.E.**, aquí adjunto toda la información de contacto, para que podáis comunicar directamente, al estar yo en USA con 7hs de diferencia horaria.*
*Para que todos estemos informados a la par, saber que **G.G.G.** está tramitando la denuncia con los Mossos, y si todo va bien mañana se podrá finalizar. Faltaban documentos que **G.G.G.** esta consiguiendo.*

*La información bancaria enviada por ti **E.E.E.**, ha sido trasladada a **G.G.G.** y los mossos, a efectos de que el proceso administrativo pueda lanzarse como debido.*
Pero además, la residencia necesita poder disponer de los horarios en los cuales se utilizo la tarjeta, porque nos dimos cuenta al ver los extractos de que le roban la tarjeta unos dias antes que le roban el móvil. O sea que la persona que efectúa esto lo hace en dos momentos distintos.
Por ello, te ruego E.E.E. que puedas ingresar mañana en el sistema del banco, y buscar mas detalle de las operaciones tarjeta VISA. De esta manera, la residencia puede definir con mayor precisión la visualización de todas las cámaras de seguridad de la clínica, dentro del marco de la investigación interna que están efectuando. Es muy posible que la persona que haya realizado el robo siga trabajando ahí, en estos momentos.

Os agradezco a todos desde ya vuestra colaboración, y espero que la conexión directa, no a través de mí, sea mas fácil.
Un abrazo,
B.B.B.*"*

SEXTO: El día 14 de abril de 2020 la identidad de la parte reclamante fue suplantada ante el BBVA en la realización de operaciones en la Cuenta número ******CUENTA.2***, cuenta cuya titularidad era reconocida por la parte reclamante con anterioridad al robo.

SÉPTIMO: Con fecha 15 de abril de 2020 la identidad de la parte reclamante fue suplantada ante el BBVA, con la contratación de los siguientes productos:

- Tarjeta número ******TARJETA.2*** vinculada al contrato ******CONTRATO.3***. El BBVA facilita la copia de del contrato, en el que figuran el nombre, apellidos, y DNI de la parte reclamante, y refiere que que se firmó electrónicamente la solicitud de la tarjeta a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA.* Esta tarjeta fue bloqueada con fecha 6 de julio de 2020. Asimismo, la tarjeta figura en situación de extravío y el contrato en estado cancelado

- Tarjeta número ******TARJETA.3*** vinculada al contrato ******CONTRATO.4.*** El BBVA facilita la copia de del contrato, en el que figuran el nombre, apellidos, DNI de la parte reclamante, y el correo electrónico ******EMAIL.1***. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA".* BBVA aportó impresión de pantalla de sus sistemas (página 439 del expediente) en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo

- Tarjeta número ******TARJETA.4*** vinculada al contrato ******CONTRATO.5.*** BBVA facilita la copia de del contrato, en el que figuran el nombre, apellidos, DNI de la parte reclamante, y el correo electrónico ******EMAIL.1***. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA"* BBVA aportó impresión de pantalla de sus sistemas (página 439 del expediente) en la que consta que el contrato se encuentra cancelado con referencia al 4 de mayo de 2020 como fecha de bloqueo

OCTAVO: Con fecha 16 de abril de 2020, desde el correo electrónico ******USUARIO.2***@bbva.com se envía el siguiente mensaje al correo ******EMAIL.2***:

"*Buenos días* ***B.B.B.****,*
espero que estéis todos bien con el tema coronavirus por EEUU, porque ya veo que se está extendiendo mucho todo lados.
Siento mucho lo que le ha pasado a tu madre, lo primero que tenemos que hacer es presentar la denuncia de los "Mossos d'esquadra" lo más urgente posible. Quien hará la denuncia ?? Entiendo que la presentara la directora de la Residencia ¿o ?? Tan pronto la tenga por favor que nos la haga llegar.

A partir de aquí se abrirá una investigación a ver qué ha pasado. Del tema de las transferencias no podemos hacer nada más que esperar a la investigación.
Para cualquier tema dale el tlf mio ******TELÉFONO.2*** *a la directora de la Residencia para que se ponga en contacto conmigo y podamos tramitar todo esto correctamente y lo más rápido posible.*
Un saludo." (el subrayado es nuestro)

NOVENO: Con fecha 17 de abril de 2020, la representante de la parte reclamante, desde el correo ******EMAIL.3*** envió un mensaje (página 203 del expediente) al correo del director de la sucursal ******USUARIO.2***@bbva.com en el que se presenta y manifiesta adjuntar la denuncia presentada el día 16 de abril de 2020 ante los Mossos d'Esquadra.

La denuncia es presentada por ***D.D.D.*** en representación de la parte reclamante. Adjunta escrito en el que ***(…)*** de la parte reclamante autoriza a ***D.D.D.*** a interponer la denuncia en nombre de la parte reclamante y (…). La denuncia se interpone contra la residencia de ancianos en la que se encontraba la parte reclamante cuando acaeció el robo de sus pertenencias. En la denuncia (página 532 y siguientes del expediente) se indica lo siguiente: *"…**Doña A.A.A.** manifiesta que se siente rara y que, además, en la residencia le han robado: + el móvil*
+ un monedero cuadrado con cremallera donde tenía su tarjeta de crédito, el DNI, su carné de conducir y su tarjeta sanitaria…

*…En resumen, los hechos denunciados son los siguientes: en el período temporal comprendido entre la fecha de 10 de abril de 2020 y 13 de abril de 2020, alguien de la residencia ha realizado varios hurtos a **Doña A.A.A.**, tanto de dinero en efectivo, como de la tarjeta, retirando dinero de la cuenta y de la línea de crédito, y otra documentación personal de carácter esencial, también de su móvil, por valor conocido acumulado a fecha de hoy superior a los 13.500.- Euros. Todo apunta a que, durante este fin de semana del 11 al 13 de abril de 2020, la han sedado o anestesiado, ya que ella me manifestó que, en los últimos dos o tres días, se sentía rara, como mareada, cosa que nunca había manifestado antes, a pesar de la medicación que se estaba tomando…".*

En la propia denuncia cita que contactaron con el reclamado y que éste les informó de que se había retirado dinero con la tarjeta con anterioridad a la comunicación por correo electrónico de la sustracción a BBVA el 14 de abril de 2020.

DÉCIMO: El día 17 de abril de 2020 la identidad de la parte reclamante fue suplantada en la realización de operaciones en la Cuenta número ******CUENTA.1,*** de la cual BBVA especifica que no está cancelada.

DÉCIMO PRIMERO: Con fecha 20 de abril de 2020 desde el correo electrónico ******USUARIO.2***@bbva.com se envía un mensaje al correo electrónico de la representante de la parte reclamante ******EMAIL.3,*** en el que le comunica que ha dado traslado al departamento de seguridad y fraudes la denuncia interpuesta por la parte reclamante con fecha 16 de abril de 2020.

DÉCIMO SEGUNDO: Con fecha 26 de julio de 2020, en contestación al requerimiento de información formulado por esta Agencia, BBVA aporta documento de fecha 27 de abril de 2020 de contratación de la Cuenta número ******CUENTA.3*** de la cual BBVA especifica que no está cancelada. BBVA facilita copia de del contrato, en el que figuran el nombre, apellidos, dirección, y DNI de la parte reclamante. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*. Además, BBVA cita otros detalles de la contratación (dirección IP y validación en la *"app"* del reclamado a través de huella dactilar).

DÉCIMO TERCERO: Con fecha 30 de abril de 2020, desde el correo electrónico ******USUARIO.2***@bbva.com se envía un mensaje (página 205 del expediente) al correo electrónico de la representante de la parte reclamante ******EMAIL.4***, con copia ******EMAIL.3*** y ******EMAIL.2***, con el siguiente contenido (traducción no oficial, original en catalán):

"*Buenos días **D.D.D.**,*
*Según conversación telefónica esta mañana a las 12:22 nos ha llamado el teléfono *****TELÉFONO.1** haciéndose pasar por **A.A.A.**, se ha identificado con el número de DNI correspondiente y nos ha solicitado dar de alta el teléfono móvil en la base de datos para poder acceder a la Banca Online. Evidentemente esta operativa no se puede hacer por teléfono y así les hemos trasladado, para que se personen en la oficina del BBVA para realizar estos trámites. y mirad que pasa con el teléfono ya que sigue activo.*
Saludos"

Con fecha 1 de mayo de 2020 ***D.D.D.***, en representación de la parte reclamante presentó ante los Mossos d'Esquadra una ampliación de la denuncia (página 578 del expediente) en nombre de la parte reclamante con relación a los hechos manifestados por el director de la oficina con fecha 30 de abril de 2020.

DÉCIMO CUARTO: Con fecha 5 de mayo de 2020, la parte reclamante presentó un escrito dirigido a Telefónica de España, S.A., en el que solicita la baja del número de móvil de la parte reclamante ******TELÉFONO.1***. Manifiesta que han intentado desde el 14 de abril de forma infructuosa hacerlo, siguiendo a la fecha del escrito operativo.

DÉCIMO QUINTO: Con fecha 6 de mayo de 2020, la abogada de la parte reclamante remite un escrito a BBVA (página 115 del expediente) en el que se le requiere a que de forma inmediata:

> *"1º).- Paralicen, anulen y retrotraigan cualquier Operación bancaria que se haya realizado o se intente realizar desde la línea de móvil *****TELÉFONO.1** contra cualquier cuenta o producto bancario de mis representadas en BBVA, desde 10 de Abril de 2020.*
> *2º).- Paralicen, anulen y retrotraigan cualquier operación bancaria que se intente de cualquier manera (presencial, telefónica. online, etc.) contra cualquier cuenta o producto bancario de mis representadas en BBVA, desde 10 de abril de 2020.*

3º).- Paralicen y no den curso a cualquier operación bancaria que se intente de cualquier manera (presencial, telefónica. online. etc..) contra cualquier cuenta o producto bancario de la sociedad vinculada a mis representadas ***(…).***

Todo ello con motivo de la sustracción fraudulenta de tarjeta de crédito y de móvil a la ***Sra. A.A.A.****, ocurrida entre los días 10 y 13 de abril de 2020 en la residencia (…) de Barcelona, debidamente denunciada ante la policía el día 16 de abril de 2020, y habida cuenta de que todas las peticiones verbales y escritas dirigidas desde el 14 de abril de 2020 al director de la Oficina de BBVA en ***DIRECCIÓN.2, ***LOCALIDAD.1, han quedado inatendidas por parte de BBVA, hecho que ha permitido a los delincuentes continuar operando desde el móvil y tarjeta sustraídos.*

Igualmente les avanzamos que pediremos la responsabilidad de BBVA por todos los daños y perjuicios causados a mis representadas, desde que se les comunicó la orden de paralización total en fecha de 14 de abril de 2020. en adelante. por todas las operaciones fraudulentas que los infractores han realizado y siguen realizando actualmente contra el patrimonio de mis representadas, ya que tales operaciones delictivas no se habrían podido consumar si BBVA hubiera atendido debidamente nuestra Orden de paralización total dada en fecha de 14 de abril de 2020". (el subrayado es nuestro)

DÉCIMO SEXTO: Con fecha 9 de mayo de 2020, la representante de la parte reclamante dirigió una comunicación a BBVA (página 213 del expediente) en la que solicita la devolución de las cantidades sustraídas a la parte reclamante y su hija entre el 13 de abril y el 5 de mayo de 2020.

DÉCIMO SÉPTIMO: Con fecha 15 de mayo de 2020 la parte reclamante firma un escrito (que dirige a BBVA en el que, como titular de la tarjeta ******TARJETA.1*** comunica la incidencia (robo) y solicita la devolución del importe de un conjunto de movimientos que lista. El listado incluye cargos producidos entre el 11 de abril y el 30 de abril de 2020 y el siguiente el comentario:

"Cliente manifiesta que se encuentre en una residencia de ancianos confinada, y que le ha desaparecido el bolso con todas sus pertenencias dentro, entre ellas las tarjetas. Le han suplantado la identidad durante este mes en varias ocasiones, consiguiendo acceder a la banca online." (el subrayado es nuestro)

DÉCIMO OCTAVO: Con fecha 20 de mayo de 2020 el BBVA contestó (página 226 del expediente) al escrito dirigido por la representante de la parte reclamante de fecha 6 de mayo de 2020, solicitando acreditación de la representación en virtud *"del art. 12 del Reglamento para la Defensa del Cliente en España del Grupo BBVA que exige la identificación y firma de los titulares, y en su caso, de la persona que los representa, debidamente acreditada*". En ese mismo escrito se manifiesta que la acreditación de la representación puede realizarse a través del envío de un documento firmado que contenga nombre completo, NIF, dirección completa y firma tanto del representante como del representado.

DÉCIMO NOVENO: Con fecha 21 de mayo de 2020 la parte reclamante solicitó al Juzgado de Instrucción Nº 33 de Barcelona (en el marco de las Diligencias Previas ***(...)***) la medida cautelar consistente en solicitar la baja de la línea ******TELÉFONO.3***. Ello (página 268 del expediente) ya que *"los investigados habían cambiado el teléfono asociado a la póliza de la **Sra. A.A.A.** al nuevo teléfono utilizado por ellos para delinquir que ya nos había confirmado BBVA".*

VIGÉSIMO: Con fecha 29 de mayo de 2020 el Juzgado de Instrucción Nº 33 de Barcelona requiere, en el marco de las Diligencias Previas ***(...)*** (página 282 del expediente) que se sigue por una denuncia presentada por la parte reclamante por la presunta comisión de un delito de hurto, estafa y usurpación de estado civil, a BBVA el bloqueo de acceso por vías no presenciales a todos los productos de la parte reclamante.

Asimismo, requiere en el marco de las Diligencias Previas (página 283 del expediente) referenciadas a Movistar que bloquee los números de teléfono asociados a la parte reclamante ******TELÉFONO.1*** y ******TELÉFONO.3***. Además, solicita los datos de la persona que dio el alta de la línea ******TELÉFONO.3***.

VIGÉSIMO PRIMERO: Con fecha 4 de junio de 2020 (página 215 del expediente), desde el correo electrónico ******EMAIL.5*** se envía un mensaje a los correos "servicioatencioncliente@grupobbva.com" y a "defensordelclientebbva@grupobbva.com", en el que se indica lo siguiente:

> "*En relación con su comunicado de 20 de mayo de 2020, recibido por correo ordinario, en el que me solicitan me identifique como Abogada de **Doña A.A.A.** y de **Doña B.B.B.**, paso a cumplimentar su petición, remitiéndoles la documentación siguiente: escrito de personación, de 14 de mayo de 2020, presentado telemáticamente al Juzgado de Instrucción nº. 33 de Barcelona, en autos de Diligencias Previas nº. **(...)**, con comprobante de firma por todas las personas que aparecen en el mismo, en el que se acredita la voluntad de mis clientes de designarme como su abogada en este procedimiento, a todos los efectos, así como escrito posterior, de 18 de mayo de 2020.*
>
> *Asimismo, les remito correspondencia mantenida con el Director de la Oficina de BBVA en ***LOCALIDAD.1, Sr F.F.F., quien ha recibido instrucciones tanto verbales como escritas de parte de la **Sra. B.B.B.**, de comunicar conmigo en calidad de Abogada de dichas señoras. Finalmente, pongo en copia **a Doña B.B.B.**, y también al **Sr F.F.F.**, Director de la Oficina indicada, quienes les van a confirmar por mail que estoy actuando en calidad de Abogada de las **Sras. B.B.B.** y **A.A.A.**, a todos los efectos, tal como consta acreditado, desde mediados de abril de 2020.*"

Además, el mismo día 4 de junio de 2020 (página 219 del expediente), desde el correo electrónico ******EMAIL.2*** se envía a "servicioatencioncliente@grupobbva.com" y a "defensordelclientebbva@grupobbva.com", el mensaje transcrito en los dos párrafos anteriores y se manifiesta, con relación a dicho correo, lo siguiente:

> "*Por la presente, confirmamos lo aquí abajo declarado por nuestra abogada **C.C.C.**.*"

VIGÉSIMO SEGUNDO: Con fecha 8 de junio de 2020 desde el correo ***EMAIL.3** se envió un mensaje al BBVA (página 208 del expediente), a las direcciones ***USUARIO.2**@bbva.com y ***USUARIO.3**@bbva.com en la que solicita el reintegro de los cargos efectuados entre el 11 y el 30 de abril a la parte reclamante.

El día 16 de junio de 2020 dirige otro correo electrónico con la misma petición (página 209 del expediente).

VIGÉSIMO TERCERO: Con fecha 16 de junio de 2020 la parte reclamante firma un escrito (página 346 del expediente) que dirige al reclamado en el que, como titular de la tarjeta ***TARJETA.2** comunica la incidencia y solicita la devolución del importe de un conjunto de movimientos que lista. El listado incluye cargos producidos entre el 17 de abril y el 3 de mayo de 2020. Incluye el comentario:

> *"Cliente manifiesta que se encuentra en una residencia de ancianos confinada, y que le ha desaparecido el bolso con todas sus pertenencias dentro, entre ellas las tarjetas. Le han suplantado la identidad durante este mes en varias ocasiones, consiguiendo acceder a la banca online."* (el subrayado es nuestro)

VIGÉSIMO CUARTO: Con fecha 2 de julio de 2020 la representante de la parte reclamante envía un correo electrónico a BBVA (página 326 del expediente) en el que resume los hechos ocurridos hasta la fecha en relación con la parte reclamante y su hija. Así cita la sustracción de dinero ocurrida desde el 12 de abril y expresa que los delincuentes habrían asociado líneas telefónicas a productos de las defraudadas mediante suplantación de identidad. En el correo, además, identifica a una de las delincuentes y solicita que *"impidan nuevos accesos a los mismos por terceros delincuentes con suplantación de identidad de mis dos clientes"*. Igualmente requiere que *"se abstengan de dar de alta cualquier tipo de nuevo producto bancario o financiero asociados a los datos personales y bancarios de mis clientes, ya que no son ellas sino una banda de delincuentes quienes lo están pidiendo"*. (el subrayado es nuestro)

VIGÉSIMO QUINTO: El día 2 de julio de 2020 la representante de la parte reclamante firma un escrito (página 127 del expediente) que dirige mediante burofax al reclamado solicitando la protección frente a la suplantación de identidad para sus representadas, que no se contraten nuevos productos a su nombre, y el abono de los importes reclamados en la misiva del 9 de mayo.

El BBVA expresa haber recibido este burofax el día 3 de julio de 2020.

VIGÉSIMO SEXTO: Con fecha 13 de julio de 2020 (página 111 del expediente), el BBVA requirió a la parte reclamante el pago de la deuda derivada del descubierto de los contratos ***CONTRATO.1** y ***CONTRATO.2** advirtiendo la posibilidad de inscripción en sistemas de información crediticia.

La parte reclamante ha adjuntado en la ampliación de la reclamación presentada ante esta Agencia, la carta del BBVA (páginas 136 y 137 del expediente) en la que le comunica la existencia de dos deudas relativas a los contratos ***CONTRATO.1** y ***CONTRATO.2** que se han comunicado al área de recobros. Además, le informa de

que las deudas ciertas, vencidas, exigibles, e impagadas cuyo pago haya sido requerido pueden ser comunicadas a los sistemas de información crediticia.

VIGÉSIMO SÉPTIMO: Con fecha 17 de julio de 2020 la representación de la parte reclamante presenta escrito (páginas 356 a 359 del expediente) al Juzgado de Instrucción Nº 33 de Barcelona (en el marco de las Diligencias Previas ***(...)***) en el que se facilita al Juzgado un conjunto de documentos recuperados por las fuerzas y cuerpos de seguridad de terceros en el marco de una operación. Entre los documentos recuperados se encuentra información de carácter personal (DNI, dirección, número de teléfono, cuentas bancarias) de la parte reclamante.

VIGÉSIMO OCTAVO: Con fecha 28 de julio de 2020 (página 200 del expediente) *la hija* de la parte reclamante envía un correo electrónico al BBVA (a la dirección del director de la sucursal, ******USUARIO.2***@bbva.com) solicitando el desbloqueo de la cuenta de la parte reclamante *"terminada en **XX**"* al objeto de transferir el saldo a otra cuenta, de la hija de la parte reclamante, *"terminada en **XXXX**"* para que ***"****mi madre pueda disponer de su dinero para vivir."* (página 322 del expediente)

VIGÉSIMO NOVENO: El día 30 de julio de 2020 (página 210 del expediente) *la hija* de la parte reclamante dirige un correo electrónico al BBVA (al director de la sucursal) solicitando, entre otras cuestiones, el cierre de las cuentas ******CUENTA.1*** y ******CUENTA.2*** y la cancelación de las tarjetas ******TARJETA.1*** y ******TARJETA.2*** de la parte reclamante.

TRIGÉSIMO: Con fecha 4 de agosto de 2020 el Servicio de Atención al Cliente del BBVA contestó vía correo electrónico a la representante de la parte reclamante con una carta de respuesta a la comunicación recibida el día 3 de julio (página 128 del expediente).

En ésta le solicita nuevamente la acreditación de la representación para poder actuar en nombre de la parte reclamante. Le indica que esto puede realizarse a través del envío de un documento firmado que contenga nombre completo, NIF, dirección completa y firma tanto del representante como del representado.

TRIGÉSIMO PRIMERO: El día 4 de agosto de 2020 la representante de la parte reclamante dirige un correo electrónico al BBVA (página 374 del expediente) en el que expresa que anexa los poderes otorgados a su favor. Facilita asimismo la copia simple de la escritura de poder a pleitos con facultades especiales otorgado ante notario por la parte reclamante y la hija de la parte reclamante a favor de la representante de la parte reclamante.

TRIGÉSIMO SEGUNDO: Entre los días 16 de agosto y 6 de septiembre de 2020 el reclamado registró dos deudas (correspondientes a los contratos de préstamo ******CONTRATO.1*** y de tarjeta ******CONTRATO.2*** -tarjeta número ******TARJETA.1***-) asociadas a la parte reclamante en el fichero de información crediticia *"Badexcug/Experian*" (página 403 y 404 del expediente).

TRIGÉSIMO TERCERO: Con fecha 3 de septiembre de 2020 la parte reclamante y su hija presentaron una demanda de juicio ordinario (página 6 del expediente) contra el reclamado que contiene la descripción de los hechos.

Según lo señalado en la contestación al requerimiento de información formulado por esta Agencia (página 122 del expediente), el día 22 de septiembre de 2020 el Juzgado notificó al BBVA la demanda (*"Procedimiento Ordinario* ******PROCEDIMIENTO.1****").*

TRIGÉSIMO CUARTO: Con fecha a 8 de septiembre de 2020 Experian dirige a la parte reclamante un escrito en el que le comunican la inclusión de una deuda procedente de un préstamo personal por el reclamado en el fichero Badexcug (página 397 del expediente).

TRIGÉSIMO QUINTO: Con fecha 9 de septiembre de 2020 la hija de la parte reclamante dirigió un correo electrónico al reclamado (página 130 del expediente) en respuesta, según cita, a dos comunicaciones previas. En dicho correo, tras pedir cierta información, se reitera las siguientes peticiones:

"1. *Cierre inmediato de las dos cuentas bancarias abiertas a nombre de mi madre* ******CUENTA.1****y* ******CUENTA.2****.*
2. Ruego procedas también a la cancelación inmediata de las dos tarjetas nº. ******TARJETA.1*** *y nº.* ******TARJETA.2****.*
3. Ruego me transfieras, en las próximas 48 horas, el importe de 6.090,14.-euros sustraído por los delincuentes, a la cuenta abierta a mi nombre, cuyo número de IBAN es el que ya te indiqué en mail anterior, terminado en XXXX
4. Finalmente ruego me confirmes que vuestra entidad va a asumir toda la deuda generada en el pasado y que se genere en el futuro, por los actos realizados por los delincuentes, utilizando tanto los productos bancarios de mi madre, como los míos personales."

Además, indica a la entidad financiera que le parece "*increíble que BBVA ponga a mi madre en un fichero de morosos por una deuda que sabéis perfectamente que ella no ha generado, sino que la han generado los delincuentes y BBVA. Ruego contactéis con vuestro Departamento Jurídico para que arreglen este tema y saquen a mi madre del fichero de morosos inmediatamente*."

TRIGÉSIMO SEXTO: Con fecha 21 de septiembre de 2021 la parte reclamante presenta ante el Juzgado de Primera Instancia Nº 10 de Barcelona ampliación de la demanda con referencia al *"***PROCEDIMIENTO.1"* (página 43 y siguientes del expediente) en la que se refiere que la entidad AXACTOR en nombre del reclamado ha contactado con la parte reclamante para gestionar una deuda pendiente de cobro y adjunta copia de la carta.

TRIGÉSIMO SÉPTIMO: Con fecha 2 de octubre de 2020 (página 132 del expediente) BBVA contestó vía correo electrónico a la hija de la parte reclamante adjuntando una carta fechada el 29 de septiembre de 2020.

En la carta se solicita acreditar la representación de la parte reclamante para poder actuar sobre los productos en que ésta figura como única titular.

Asimismo, en relación con los productos a nombre de la hija de la parte reclamante, solicita mayor concreción en relación con el importe objeto de fraude, así como la denuncia policial efectuada.

TRIGÉSIMO OCTAVO: Con fecha 2 de noviembre de 2020 la parte reclamante presenta ante el Juzgado de Primera Instancia Nº 10 de Barcelona, ampliación de la demanda con referencia al "***PROCEDIMIENTO.1" (página 27 y siguientes del expediente) en la que manifiesta que el reclamado ha continuado reclamando importes correspondientes a actos realizados por los delincuentes y ha incluido a la parte reclamante en un "fichero de morosos".

TRIGÉSIMO NOVENO: Con fecha 24 de diciembre de 2021 Equifax dirige una carta a la parte reclamante (página 110 del expediente) en la que se informa de que el BBVA, el día 23 de diciembre de 2021, solicitó la inclusión de dos deudas en el fichero de información crediticia *"ASNEF/Equifax"* por los conceptos de "préstamos personales" y "tarjetas de crédito".

CUADRAGÉSIMO: Con fecha 5 de enero de 2022 la parte reclamante dirigió una comunicación al reclamado (página 108 del expediente) en el que, en relación con la solicitud del pago de las deudas, refiere la existencia de una demanda *("*****PROCEDIMIENTO.1**")* interpuesta el 1 de septiembre de 2020 en solicitud de declaración judicial de cierre y cancelación de cuentas y tarjetas bancarias y de exoneración de cualquier deuda por cualquier concepto originado en las mismas desde 10 de abril de 2020 en adelante.

Cita que dicho proceso se encuentra pendiente de señalamiento para juicio.

Manifiesta, asimismo, que la deuda no resulta atribuible a la parte reclamante y solicita la cancelación de sus datos personales en todos los ficheros a los que los hayan cedido (con inclusión de los ficheros de morosidad).

CUADRAGÉSIMO PRIMERO: El 5 de enero de 2022 la parte reclamante dirigió una comunicación a Equifax (página 108 del expediente) en la que, en relación a la inclusión de las deudas en el fichero ASNEF, señala que existe una demanda *("*****PROCEDIMIENTO.1**")* interpuesta el 1 de septiembre de 2020 en solicitud de declaración judicial de cierre y cancelación de cuentas y tarjetas bancarias y de exoneración de cualquier deuda por cualquier concepto originado en las mismas desde 10 de abril de 2020 en adelante.

Cita que dicho proceso se encuentra pendiente de señalamiento para juicio.

Manifiesta asimismo que la deuda no resulta atribuible a la parte reclamante y solicita la eliminación de los datos personales de la parte reclamante de los ficheros de Equifax.

CUADRAGÉSIMO SEGUNDO: En la sentencia ***SENTENCIA.1 de ***FECHA.1, dictada por el Juzgado de Primera Instancia nº 10 de Barcelona, en el juicio ordinario sobre reclamación de cantidad con nº ***PROCEDIMIENTO.1**, seguidos a instancia de **DOÑA A.A.A.,** y **DOÑA B.B.B.** contra el BANCO BILBAO VIZCAYA ARGENTARIA, S.A, se indica lo siguiente en su Fundamento de Derecho Cuarto:

"*CUARTO. Teniendo en cuenta la normativa aplicable, el iter cronológico expuesto, y además la testifical de la **Sra. D.D.D.**, se infiere que a la **Sra. A.A.A.** le hurtaron el monedero con toda la documentación y tarjetas de crédito el día 10 de abril de 2020,*

si bien no se apercibieron de ello hasta el día 13 o 14 de abril, en que se presentó la denuncia ante los Mossos d'Esquadra por la Directora de la Residencia, con las correspondientes ampliaciones posteriores que se hicieron a medida que se iban percatando de que por parte de quienes tenían en su poder la documentación personal y bancaria de la ***Sra. A.A.A.*** *estaban suplantando su identidad.*

Por tanto, queda acreditado, que tan pronto como se tuvo conocimiento de la sustracción de las tarjetas se informó a la entidad BBVA para que procediera a bloquear las mismas. Así se desprende de la respuesta que dio BBVA el día 14 de abril de 2020, documento 8 de la demanda cuando responde a la ***Sra. B.B.B.*** *"Solamente tiene una tarjeta y veo que ayer 13/04/2020 a las 18:06 fue bloqueada. Llamasteis vosotros al contact center de BBVA??? Lo que veo que tiene diversos cargos a través de banca online que supongo no ha realizado ella. Adjunto cargos realizados para que le des un vistazo... Si no fueran correctos necesitamos una denuncia de los mossos para poder tramitar la alta del fraude". Y así se desprende de la documentación que consta en las Diligencias Previas, en que por parte de la entidad Bancaria se informa a la* ***Sra. D.D.D.****, que "la baixa on line en del 16/04" y le pasa los datos actualizados y las operaciones realizadas, entre ellas un préstamo online el 12/04, por importe de 4.000€ y el alta de una tarjeta el 15/04 (pág. 34 del testimonio D.Previas* ***(...)****).*

Cuando menos desde el 14 de abril de 2020 BBVA tenía conocimiento del hurto sufrido por la ***Sra. A.A.A.****.*

La ***Sra. A.A.A.*** *cumplió con su obligación de comunicar de forma inmediata con el hurto de sus tarjetas y de su D:N.I:, por lo que todos los cargos habidos con las tarjetas cuya cancelación se solicitó el día 14 de abril de 2020 deben ser reintegrados a la* ***Sra. A.A.A.****, pues cumplió con sus obligaciones, y si los delincuentes hicieron uso de las mismas con impunidad debe imputarse a una falta de diligencia por parte de la entidad bancaria, pues había sido advertida de los hechos, siendo que a tenor de los mail que remite el Director de la sucursal de ***LOCALIDAD.1 se desprende que era consciente de la suplantación de identidad, y así se lo advierte a la* ***Sra. D.D.D.*** *y a la letrada de* ***las actoras*** *al remitir el mail en fecha 30 de abril de 2020, aportado como documento 25.4 de la demanda, en el que le dice*

"Buenos días ***D.D.D.****,*
Según conversación telefónica esta mañana a las 12:22 nos ha llamado el teléfono ******TELÉFONO.1*** *haciéndose pasar por* ***A.A.A.****, se ha identificado con el número de DNI correspondiente y nos ha solicitado dar de alta el teléfono móvil en la base de datos para poder acceder a la Banca Online. Evidentemente esta operativa no se puede hacer por teléfono y así les hemos trasladado, para que se personen en la oficina del BBVA para realizar estos trámites. y mirad que pasa con el teléfono ya que sigue activo.*
Saludos

*De dicho mail se desprende no sólo que la entidad bancaria, o cuando menos el director de la sucursal de ***LOCALIDAD.1, lugar de residencia de la* ***Sra. A.A.A.****, que estaba en Barcelona para un tratamiento oncológico, sabía no sólo del hurto de las tarjetas sino del teléfono móvil de la* ***Sra. A.A.A.*** *y de la suplantación de identidad, motivo por el que se pone en contacto con la hija de la* ***Sra. A.A.A.****,* ***la coactora, Sra. B.B.B.*** *para advertirle del intento de acceder a la Banca Online."* (el subrayado es nuestro)

Por tanto, queda acreditado, según indica la mencionada sentencia, que al menos desde el 14 de abril de 2020 la entidad BBVA tenía conocimiento del hurto sufrido por la ***Sra. A.A.A.***, que había cumplido con su obligación de comunicar de forma inmediata el hurto de sus tarjetas y de su D.N.I., y que hubo falta de diligencia por parte de la entidad bancaria, pues habiendo sido advertida de los hechos, los delincuentes hicieron uso de las mismas con impunidad.

No solamente tenía conocimiento la entidad financiera del robo de las tarjetas, sino también del teléfono móvil de la parte reclamante lo que permitió la suplantación de la identidad de la misma (a tenor de los mails que remite el Director de la sucursal de ***LOCALIDAD.1).

CUADRAGÉSIMO TERCERO: Con fecha de 23 de julio de 2022, recibido en el registro de la AEPD el 26 de julio de 2022, BBVA presentó un escrito de respuesta al requerimiento de información y documentación realizado por la AEPD al que acompañaba varios documentos de los que destacamos:

Documento 1: Este documento consiste en e-mail remitido desde el correo electrónico ******USUARIO.3***@bbva.com (página 308 del expediente). Según se describe en dicho documento el 13 de abril 2020 a las 18:06 la Entidad bloqueó la tarjeta número ******TARJETA.1*** vinculada al contrato de tarjeta nº ******CONTRATO.2***.

A pesar de que el 13 de abril de 2020 se procedió, según la reclamada, a bloquear, la tarjeta bancaria de la parte reclamante, con posterioridad a este bloqueo la parte reclamante aporta un listado que incluye cargos producidos entre el 11 de abril y el 30 de abril de 2020. En la demanda presentada ante el juzgado expresa que el banco *"ha reconocido responsabilidad sobre los movimientos operados en relación con dicha tarjeta por importe de 5559,88 euros."*

Documento 2: Son dos copias de dos burofaxes de fechas 6 de mayo de 2020 y 9 de mayo de 2020 respectivamente, a través de los cuales la parte reclamante comunicaba a la reclamada que, a pesar de haber sido comunicado al banco el robo de tarjetas y terminal móvil, se había producido la sustracción de varias cantidades de dinero de la cuenta de la parte reclamante después de dicha comunicación, utilizando la identidad de ella y solicitaba que se paralizara, anule y retrotraiga cualquier operación realizada con el teléfono móvil de la parte reclamante "*o contra cualquier cuenta o producto bancario de la parte reclamante en BBVA antes del 10 de abril de 2020, fecha en la que se produjo el robo."*

Documento 3: Este documento 3 lleva por título "*PREVENCION DEL FRAUDE Y LA ESTAFA*", fechado el 1 de junio de 2015 y es el procedimiento utilizado por el reclamado para los casos de contrataciones. En el resumen de su contenido se indica que se refiere a "*Instrucciones para la prevención del fraude referidas tanto a aspectos generales como a procedimientos específicos según la modalidad del fraude. Dictámenes de seguridad sobre los casos de fraude y otras consideraciones sobre cuestiones de prevención del fraude*". En dicho documento se dice:

"*Una de las claves de la relación cliente-entidad financiera es la confianza que debe establecerse. Sin duda, desde ese punto de vista, los ataques a la seguridad de determinados productos o servicios pueden deteriorar este principio […]*

La defensa de la confianza en los procesos, el preservar la reputación de las propias entidades, dado que el fraude afectan muy negativamente a la imagen de las mismas, y evitar quebrantos que, una vez producidos, son, en la mayoría de los casos, irrecuperables, hacen necesario potenciar la prevención en este campo mediante la emisión de normas y la actuación formativa […]

Esta norma pretende difundir aquellas medidas básicas de vigilancia que puedan permitir detectar y abortar la gran mayoría de los fraudes que se producen, con un reducido esfuerzo. Esta eficacia está condicionada por un hecho innegable: el mundo del fraude está en continuo cambio y los procedimientos son perfeccionados por los delincuentes constantemente, por lo que habrá que actualizar la información de forma permanente.

Si se consigue un nivel preventivo adecuado, se extenderá dentro de la comunidad delincuencial la opinión de que el grupo BBVA adopta adecuadas medidas que dificultan el fraude con lo que, como efecto secundario, pero no menos importante, tenderán a disminuir las tentativas y los riesgos de futuros ataques. […]

2. Seguridad
2.1. Introducción
2.1.1. Conceptos
A continuación enunciaremos algunos de los conceptos que se manejarán más adelante con el fin de unificar criterios en esta materia: […]

Suplantación de identidad:
Vinculado a las prevenciones sobre identificación, está la suplantación de identidades. En la mayoría de los casos, observar las recomendaciones dadas en cuanto a identificar DI falsos o manipulados y realizar alguna comprobación mediante preguntas que sólo conozca el titular o una llamada al teléfono del cliente que figure en nuestras BD, será suficiente para desenmascarar la mayoría de los intentos.
Pero otro aspecto a tener en cuenta es que, en algunas ocasiones, esta actuación se realiza abusando de una hipotética relación de confianza, por ejemplo, al presentarse una persona para realizar alguna operación con documentación de otra persona sin estar ésta presente.
Hay que tener en cuenta que no son infrecuentes los casos de estafas a familiares directos, manipulación de cuentas de parientes fallecidos (en algunos casos por razones fiscales), o la manipulación indebida de cuentas por razón de herencias, etc. Si el banco no opera correctamente, puede incurrir en una grave responsabilidad, por lo que estas prácticas no deben realizarse. También hay que señalar la utilización de la suplantación para obtener información (números de cuentas, saldo, etc.) que después es utilizada para realizar la estafa mediante, por ejemplo, disposiciones fraudulentas. Hay que extremar las precauciones de identificación, por tanto, a la hora de facilitar determinados datos. […]

Operaciones sin presencia física de la tarjeta.- En estos casos (compras por INTERNET y venta por correo/teléfono), es el comercio el que asume contractualmente la responsabilidad, salvo en el caso de comercio seguro con autenticación del titular. Eso no nos exime de prestar atención a este tipo de fraude ya que redunda indirectamente en la fiabilidad de este producto y, por tanto, en su utilización y rentabilidad. […]

Documento Identificativo (DI): Es aquel que permite comprobar fehacientemente la identidad de una persona, que cuenta con alguna medida de seguridad que evite su alteración y/o manipulación y que incorpora fotografía del titular. Debe ser original (no fotocopia) y estar en vigor. Más adelante se especifican cuáles son.[…]

Medidas de Seguridad:
Son aquellos elementos que, incorporados a un documento (identificativo, de pago, billete, etc.) permiten identificarle como verdadero y, por tanto, distinguirlo del falso o manipulado. […]

2.2.2. Cómo actuar
No hay que olvidar que los estafadores frecuentemente tratan de presionar al empleado, ponerlo nervioso o exigir todo tipo de urgencias con motivos variados y no siempre justificados claramente. Lo hacen para que su víctima cometa un error y les permita hacerse con su botín. No se debe caer nunca en su juego y siempre se debe actuar con calma. A la más mínima duda y para sentirse más respaldado y apoyado, se debe consultar con los compañeros, con el Delegado de Seguridad en el Territorio o con Seguridad Bancaria-Prevención del Fraude.
Como regla general de gran importancia, en caso de mínima duda deberán hacerse siempre fotocopias legibles del Documento Identificativo (de su anverso y reverso si se trata de DNI o similar), además de en los casos que más adelante se especifican, en los que la fotocopia deberá hacerse necesariamente. En el caso de que se llegue a consumar el fraude y en los casos que así se determine, se interpondrá la correspondiente denuncia, que se formulará con el asesoramiento y apoyo del Delegado de Seguridad en el Territorio.[…]

2.2.3. Prevenciones de identificación
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.
Documentos de identificación:
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.
Cómo identificar:
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.
Otras cuestiones a tener en cuenta:
Hurto/extravío del DI / libreta / cheque / pagare:
En el caso de que el cliente comunicase el hurto o extravío de su DI/ libreta / cheque, por ejemplo, al informar de la pérdida o hurto de una tarjeta o de otro documento, es obligatorio añadir esa información en los aplicativos del Banco, de manera que sirva de alerta para la Red.

En estos casos, la oficina es conveniente que recoja del cliente un escrito en el que éste comunique la pérdida de la documentación.
[…] Operaciones a distancia:
Como principio general, para una correcta identificación es imprescindible la presencia física de la persona que va a realizar la operación, además de ser necesaria para contar con su consentimiento y para que se firmen convenientemente todos los documentos requeridos. La experiencia indica que son frecuentes los fraudes en las que se utilizan las comunicaciones por teléfono, e-mail o fax para dar determinadas órdenes.
Se producen deficientes identificaciones, de manera que el estafador se hace pasar por un cliente o, incluso, por un empleado.
Ordenes mediante comunicaciones telefónicas:
Como regla general, NO deben admitirse. Si en casos excepcionales se admiten, deberán restringirse a clientes muy conocidos. En caso de duda, no deben realizarse. Es conveniente realizar preguntas de comprobación para asegurar la identidad del interlocutor o pedir sus datos y llamar a un teléfono obtenido de las bases de datos (BD), nunca al facilitado por el propio comunicante. También se puede contrastar la información a través de las BD. En estos casos excepcionales, inmediatamente se deberán documentar las operaciones.
Remisión de órdenes vía e-mail/fax:
Los procedimientos de escaneado de documentos, por su sencillez y economía, han facilitado el incremento de este tipo de fraude. Por esta razón, como regla general, NO deben admitirse. Se restringirán al máximo, admitiéndose solo en casos excepcionales (exclusivamente clientes muy conocidos), siendo imprescindible cumplir el procedimiento en el que se regula la autorización del uso de la tramitación de órdenes de pago (Nacionales e Internacionales) recibidas por parte de los clientes a través de e.mail/fax el cual obliga a realizar contacto telefónico para verificar la autenticidad de la orden recibida. […]
Es muy frecuente que los estafadores, haciéndose pasar por clientes, llamen a las oficinas (especialmente a otras de la del titular real) repetidas veces para comprobar que su orden se ha cursado. No basta recibir esas llamadas para dar por buena la orden.
[…]
2.2.5. La firma como elemento identificativo
Otro elemento clave en la correcta identificación del cliente es la firma, hasta el punto de que su análisis es una herramienta más de trabajo en la operativa bancaria y, por tanto, constituye un instrumento más dentro del nivel elemental de seguridad. Por estas razones es imprescindible que todos los documentos asociados a los productos estén debidamente firmados y la firma del cliente digitalizada.[…]
2.3.1. Fraudes con Tarjetas[…]
Algunos tipos de fraude son los siguientes:
** Utilización de tarjetas robadas/extraviadas. El cliente tiene la obligación, establecida contractualmente, de custodiar apropiadamente tanto la tarjeta como el PIN y comunicar de forma inmediata cualquier incidencia. Una forma de incumplimiento de la obligación de custodia es que dicho número figure en cualquier momento que lleve junto a la tarjeta.*
*[…] * Hurtos en el envío de la tarjeta. Otro aspecto fundamental es el envío de las tarjetas. En este caso, se deberá seguir lo indicado en la Norma 52.10.026. […] Siempre hay que tener en cuenta que lo que se envía no es un simple plástico, sino un documento de pago equivalente a efectivo por valor del límite de la tarjeta. Se deben*

enviar desactivadas y una vez confirmada la recepción por el cliente, proceden a su activación.
** Operaciones sin presencia física de la tarjeta.- En estos casos (compras por INTERNET y venta por correo/teléfono), es el comercio el que asume contractualmente la responsabilidad, salvo en el caso de comercio seguro con autenticación del titular. Eso no nos exime de prestar atención a este tipo de fraude ya que redunda indirectamente en la fiabilidad de este producto y, por tanto, en su utilización y rentabilidad.*
** Obtención fraudulenta del número personal (PIN). - Los métodos utilizados por los estafadores son variados (engaños, uso de la fuerza, etc.)*
Cómo actuar en caso de fraude:
En caso de que se detecte, por los distintos medios existentes, un fraude con tarjeta de crédito/débito, lo inmediato es el bloqueo de la tarjeta siguiendo instrucciones de la Norma 52.10.026. Esta es una acción preventiva muy importante, porque inmediatamente evita más fraude. En caso de que el cliente dude qué tarjeta fue extraviada o hurtada, se bloquearán todas las de su titularidad.
El proceso continúa, en caso de fraude comprobado, enviándose el expediente completo a Operaciones - Medios de Pago. […]

2.3.8. Créditos al consumo
Para que exista fraude, debe haber un "engaño suficiente" (ver concepto de estafa, punto 2.1.1.), como puede ser la manipulación o falsificación de la documentación presentada. Si no hay tal engaño, seguramente se tratará de mora. En caso de fraude, los estafadores suelen actuar de la siguiente forma:
** Abren una cuenta, en algunos casos con documentación falsa, operando con ella con normalidad. Simulan ingresos periódicos como si se tratase de una nómina.*
** Tras unos meses, solicitan un crédito al consumo para, por ejemplo, comprar un vehículo. Para solicitarlo, presentan nóminas falsas o manipuladas, en algunos casos de empresas reales para las que no trabajan los solicitantes en la fecha de la solicitud, o, en otros casos, de empresas inexistentes o creadas para el fraude. Pueden manipular incluso certificados de la Seguridad Social.*
** Posteriormente disponen en efectivo del dinero o utilizan el dinero del préstamo, revenden el bien y desaparecen.*
** En algunos casos, son grupos organizados que, además de crear empresas con el fin de emitir nóminas ficticias, incluso ponen a nombre del solicitante una propiedad como aparente garantía para luego, antes de desaparecer, volverla a poner a nombre de otra persona de la organización, de forma que el beneficiario del préstamo aparece como insolvente. […]*

2.5. Otras cuestiones relacionadas con la prevención del fraude
2.5.1. Seguridad en la información
La gran mayoría de los fraudes se inicia con una exhaustiva recopilación de información sobre la potencial víctima, por lo que la primera medida preventiva es asegurarse que el acceso a la información lo tenga, exclusivamente, quien lo deba tener.

Esto implica estar vigilantes ante solicitud de datos por vía telefónica por parte de personas desconocidas, aunque digan que son compañeros. En estos casos, conviene confirmar por métodos sencillos, como preguntas de comprobación o, en caso de llamadas recibidas, con llamadas de retorno a teléfonos existentes en

nuestras BD que sepamos que son realmente de la persona que decía llamar (tanto si es cliente como si es empleado). No hay que olvidar que esa confidencialidad, además, viene exigida por la Ley de Protección de Datos, que obliga a tratar con confidencialidad y no facilitar información con datos personales a personas que no sean titulares de productos, salvo ante un requerimiento legal. Para más datos sobre esta materia, ver Norma 62.30.012 (Protección de datos de carácter personal) […]".
Documentos nº 4, 5 y 6: En estos documentos se aportan por la entidad reclamada varias operaciones de compra, disposiciones de cajero y transferencias a través de la con tarjeta ******TARJETA.1*** asociada al contrato ******CONTRATO.2***. En particular, el documento 6 es una comunicación de incidencias relacionados con la tarjeta bancaria, y por medio del mismo se indica que la parte reclamante puso en conocimiento de la reclamada el robo de la tarjeta bancaria y el teléfono y que por la entidad financiera se procedía al adelanto provisional y salvo buen fin de las cantidades reclamadas.

La entidad bancaria no ha aportado ningún otro documento de fecha posterior relativo a la prevención del fraude y la estafa.

CUADRAGÉSIMO CUARTO: La entidad reclamada presentó un escrito el 10 de febrero de 2023 reconociendo su responsabilidad en la comisión de las siguientes infracciones relacionadas con el caso concreto que se presentó ante la Agencia y que fue el origen de la investigación posterior:

- La infracción del artículo 6.1 del Reglamento General de Protección de Datos tipificada en el artículo 83.5 del mismo Reglamento, en relación con la contratación no autorizada de productos, sobre la que el Acuerdo aprecia la posible imposición de una sanción de 70.000 euros.

- La infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, en relación con los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales, sobre la que el Acuerdo aprecia la posible imposición de una sanción de 500.000 euros.

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, en relación con la incorporación de datos personales en los sistemas de información crediticia, sobre la que el Acuerdo aprecia la posible imposición de una sanción de 70.000 euros.

Asimismo, la reclamada procedió al pago de las sanciones correspondientes a las citadas infracciones, efectuadas las deducciones establecidas por el artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

CUADRAGÉSIMO QUINTO: En el anterior escrito de fecha de 10 de febrero de 2023 la parte reclamada presenta escrito de alegaciones al acuerdo de inicio por las dos supuestas infracciones de los artículos 25 y 32 del RGPD, de las que no reconoce su responsabilidad ni realiza el pronto pago, y presenta la siguiente documentación:

Documento nº1: Este documento se denomina "*Valoración de la Seguridad y Privacidad en BBVA*" y en que el BBVA declara que "*BBVA cuenta con una normativa de Security By Design, generada en septiembre del año 2017 y con última revisión*

efectuada en Julio de 2022. La mencionada normativa interna, establece que, al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que estén basados en el tratamiento de datos personales o que, traten datos personales para cumplir su función, debe alentarse a los desarrolladores de los productos, servicios y aplicaciones a que tengan en cuenta los principios básicos establecidos en la normativa de protección de datos en el momento de desarrollar y diseñar estos productos, servicios y aplicaciones…

Entre los diferentes riesgos considerados como parte de los análisis realizados en las fases de diseño y desarrollo de los productos se encuentran:

Categoría de Riesgo ICT	Subcategorías	ID
Riesgos de seguridad de las TIC	Ciberataques y otros ataques ICT externos.	RS.01
	Seguridad ICT interna.	RS.02
	Seguridad ICT física inadecuada.	RS.03
	Incumplimiento Normativo / Regulatorio	RS.04
Riesgos de integridad y privacidad de datos TIC	Tratamiento o manipulación disfuncional de datos ICT.	RI.01
	Controles de validación de datos mal diseñados en sistemas ICT.	RI.02
	Cambios de datos mal controlados en los sistemas ICT de producción.	RI.03
	Arquitectura de datos, flujos de datos, modelos de datos o diccionarios de datos mal gestionados o diseñados.	RI.04
	Incumplimiento con la regulación de protección de datos personales (GDPR, LOPD, LFPDPPP...)	RI.05
Riesgos de cambio de las TIC	Control inadecuado de los cambios en los sistemas ICT y del desarrollo ICT.	RC.01
	Arquitectura ICT inadecuada.	RC.02
	Gestión inadecuada del ciclo de vida y de los parches.	RC.03
Riesgos de disponibilidad y continuidad de las TIC	Gestión inadecuada de la capacidad.	RD.01
	Fallos del sistema ICT.	RD.02
	Planificación inadecuada de la continuidad ICT y de recuperación frente a desastres.	RD.03
	Ciberataques disruptivos y destructivos.	RD.04

[…] *En concreto, el equipo de Fraude emitirá un posicionamiento en las iniciativas analizadas por SeP con el objetivo de prevenir:*
1. Pérdida económica tanto a los clientes como a BBVA
2. Creación de cuentas mula que permitan realizar los ataques de fraude
3. Blanqueo de Capitales
4. Financiación al terrorismo
5. Fuga de información de datos habilitadores de fraude "

BBVA no ha aportado la versión del documento vigente en la fecha de los hechos que se analizan en el presente procedimiento.

Documento nº 2: Este documento se denomina "*Actuaciones Security by Design (BBVA)*". La fecha del documento es de 13 de julio de 2022, por lo que se trata de una

versión posterior a la vigente en el momento de los hechos objeto del presente procedimiento. El documento reproduce la guía de la AEPD sobre protección de datos desde el diseño y por defecto y recoge lo siguiente:

"*Con el objetivo de cumplir con el concepto de Seguridad desde el Diseño y por Defecto, en BBVA se aplican las siguientes normativas y buenas prácticas.*

1. Norma de Desarrollo Seguro y Privacy by Design: Norma interna que recoge los principios de Privacy by Design según el Reglamento orientadas a privacidad y protección de datos durante todo el ciclo de vida del desarrollo de un producto software.

2. Guía Big Data: Glosario de buenas prácticas y consideraciones de la Agencia Española de Protección de Datos en cuanto al tratamiento de datos personales en entornos Big Data.

3. Guía de Anonimización: En esta guía se describen las diferentes posibilidades o técnicas de anonimización que contempla la Agencia Española de Protección de Datos y su finalidad.

4. Norma de clasificación de la información: Normativa interna en cuanto a la clasificación de la información que incorpora consideraciones de GDPR.

5. Framework de medidas de seguridad (versión 3.0): Herramienta que realiza un análisis de riesgo, en base a parámetros de GDPR (volumen de datos, geolocalización y tratamiento de los datos, tipología de datos, etc) y muestra las medidas de seguridad necesarias y recomendables a aplicar.

6. Anexo de seguridad para el contrato con proveedores: Medidas de seguridad con foco en cumplimiento GDPR para el tratamiento de datos en terceros.

Ninguna de las guías a que se refiere este documento se adjunta junto al mismo.

Documento nº 3: En el escrito de alegaciones se denomina: "*Norma de Clasificación de Información Normativa interna (BBVA)"*, en la que "*se proveen las directrices a seguir en el área de Tecnología para la implementación de medidas de seguridad sobre los Sistemas de Información propiedad de BBVA España, basados en la clasificación de la información que manejan, y adecuados a la valoración del riesgo a los que están expuestos*". El documento es de 5 de noviembre de 2019.

Al final del texto se mencionan tres anexos: ANEXO I - Medidas de Protección y Monitorización. ANEXO II - Información Especial. ANEXO III - Excepciones. No pueden ser analizados dichos anexos ya que no se acompaña su texto.

Documento nº 4: Este documento se denomina *"Agile Risk Assessment*" (traducción no oficial, "Evaluación ágil de riesgos"), "*Alertas de seguridad ante bloqueo de usuario*".

La versión aportada es del 24 de julio de 2018. Según el propio documento: *"El objetivo de esta iniciativa consiste en generar alertas proactivas dirigidas a clientes, que les informen ante las siguientes situaciones en Banca Móvil:*

● *Antes de que se bloquee permanentemente su usuario por re-intentos de inicio de sesión fallidos: alerta marcada por la nueva directiva de servicios de pago, PSD2 (Payment Services Directive 2), a partir de la cual se debe informar al usuario antes de que pase a ser bloqueado de manera permanente.*

● *Tras bloquear su usuario permanentemente. Estas alertas deben estar disponibles tanto sobre infraestructura legacy (R1 / SLOD), como sobre R2 (Granting Ticket), y deben comunicarse a través de correo electrónico informado / validado.*

El proceso posterior de desbloqueo del usuario es el mismo que en la actualidad. El alcance geográfico de la iniciativa se circunscribe a España, Portugal y Red Exterior, tanto para Empresas como para Particulares".

Este documento se refiere al establecimiento de una alerta de seguridad ante el bloqueo de usuario antes de que se produzca por reintentos de sesión fallidos y tras el mismo.

Documento nº 5: Este documento se denomina "*Agile Risk Assessment*" (traducción no oficial, "Evaluación ágil de riesgos"), "*Bloqueo Hard Fraude*". La versión aportada (1.0) es de 1 de junio de 2020. Según este documento: "*El objetivo de la iniciativa consiste en implementar una serie de modificaciones en los procesos de bloqueo y desbloqueo de usuario (clientes BBVA) de tipos soft y hard […].*

Descripción del alcance [2020-ES-0901] Bloqueo Hard Fraude
El objetivo de la iniciativa consiste en implementar una serie de modificaciones en los procesos de bloqueo y desbloqueo de usuario (clientes BBVA) de tipos soft y hard. En ambos casos, el bloqueo a nivel operativo para el cliente es el mismo,es decir, no podrá operar con su perfil multicanal. La diferencia es que para el tipo soft se produce un bloqueo en el LDAP y para desbloquearlo se puede hacer desde canales digitales, contact center y oficina y para en el bloqueo tipo hard se bloquea en el IMC y el desbloqueo únicamente se puede realizar desde un cajero u oficinas. Los cambios introducidos serán los siguientes: • Proceso de bloqueo soft. Cuando se lleve a cabo un bloqueo soft (siguiendo los flujos ya establecidos) además de bloquear el usuario multicanal del cliente en el LDAP y cancelar los TSEC asociados al cliente, se notificará el bloqueo al cliente a través de una notificación push. • Proceso de bloqueo hard. Además de los distintos métodos ya existentes para llevar a cabo el bloqueo hard (oficina y contact center) se permitirá la opción a los clientes de bloquear su perfil desde un ATM. En este caso, el cliente tendrá que introducir su tarjeta y su PIN y seleccionar la opción de bloqueo de perfil. Se bloqueará el usuario en el IMC (CPD BBVA) y además se realizará el bloqueo soft (bloqueo en LDAP, cancelación de TSEC y notificación push). • Proceso de desbloqueo hard. Finalmente, cuando un cliente acuda a un cajero para realizar un desbloqueo hard (siguiendo el mismo procedimiento existente actualmente y ya analizado), se procederá a desbloquear al cliente en IMC y además se le desbloqueará en el LDAP. A continuación, se le enviará una OTP que deberá introducir en el cajero para restablecer su contraseña como ya ocurre actualmente. • Proceso de desbloqueo soft. En este caso el proceso es el mismo que actualmente.

[…]
2. Riesgos ICT relevantes identificados
Se identifican los siguientes aspectos de riesgo relevantes asociados a la iniciativa analizada, cuya categorización se encuentra definida en el Anexo I : […]

Riesgos de Seguridad y Antifraude
● *[RS.01] [Antifraude] La funcionalidad analizada (nuevo servicio en ATM que permite a los clientes invocar el bloqueo hard de su propio usuario multicanal) implica cambios en procesos susceptibles de fraude, lo cual podría derivar en pérdidas económicas e impacto reputacional para el Grupo.*

Riesgos de Privacidad e Integridad de Datos
● *No se han identificado riesgos relevantes en el ámbito de Integridad y Privacidad "*

Documento nº 6: Este documento se denomina como: "*Dictamen de medidas técnicas de Seguridad y Fraude Olvido/Desbloqueo de password de usuario multicanal sin tarjeta*", y establece las medidas técnicas de seguridad y prevención del fraude en

caso de solicitud de desbloqueo por olvido de password de usuario Multicanal. La versión aportada (1.0) es de fecha 23 de abril de 2014.

Según el propio documento, "*El objetivo de la presente iniciativa es implementación de un mecanismo que permita la generación de una nueva contraseña de acceso a los canales del segmento de particulares, es decir, bbva.es y .mobi, Banca Móvil y Wallet, Autoservicios y Banca Telefónica, siempre y cuando dispongan de un mail informado y segundo factor de autenticación*.
[…]

5 Riesgos activos
Tras el análisis de la iniciativa, no se han identificado riesgos activos."

BBVA no ha aportado versiones posteriores.

Documento nº 7: Este documento se denomina "*Límites de fraude para operativas < 20 de Bizum sin OTP*" La versión aportada es de fecha 1 de febrero de 2017.
En la página 3 del documento se dice lo siguiente:

"*1. Descripción de la Iniciativa*
De cara a agilizar el proceso de pago con bizum eliminando el 2º factor para operaciones de 20 euros o
menos, con un máximo de 3 operaciones al día de este tipo, esta iniciativa sólo aplica a BIZUM
1.1. Situación Actual
Actualmente, para este tipo de operativas, se está pidiendo siempre clave de firma, independientemente del importe de la operación"

BBVA no ha aportado versiones posteriores.

Documento nº 8: Se trata de un extracto del informe de auditoría emitido por un Deloitte Advisory, S.L. el 01/12/2022, en el que se verifica el cumplimiento por BBVA de los aspectos expuestos en el (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

Documento nº 9: El escrito de alegaciones hace referencia a este documento que se denomina "*Contrato Multicanal*", firmado por la parte reclamante el 04/07/2017.

En este contrato se establecen las condiciones generales de todos los canales y servicios adscritos a dichos canales, concretamente: Banca por internet, Teléfono móvil, Canal Autoservicios: Cajeros Automáticos y Terminales en Oficinas y, por último, Banca Telefónica. La versión es de 27 de noviembre de 2016,

En la cláusula 8.3. del mismo se indica que "*El Cliente se obliga a notificar al Banco la pérdida, robo, o uso indebido del terminal de teléfono móvil y/o sus Tarjetas SIM, o acceso indebido a cualquiera de los mismos, así como cualquier otra causa que le impida acceder a los mensajes que le hayan sido enviados, sin demora indebida en cuanto tenga conocimiento de ello*."

CUADRAGÉSIMO SEXTO: Con fecha 13 de julio de 2023, el órgano instructor del procedimiento acordó la apertura de un período de práctica de pruebas, en el cual esta

Agencia requirió a BBVA para que en el plazo de diez días hábiles presentara la siguiente información:

"*1) La evaluación de impacto de protección de datos (en adelante EIPD), fechada y firmada, en materia del tratamiento de los datos personales de los clientes del BBVA en materia de "BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA", vigente el 14/04/2020, fecha en la que la hija de la parte reclamante comunicó al BBVA el robo sufrido por la parte reclamante ("móvil, monedero, tarjetas, etc."), así como toda la documentación previa a la EIPD en la que se haya plasmado la necesidad de la decisión de realizar la EIPD; asimismo se precisa toda la documentación elaborada con ocasión de la realización de la EIPD y justificativa de los resultados obtenidos en la EIPD y de las medidas adoptadas al respecto, incluyendo la documentación relativa a participación del Delegado de Protección de Datos del BBVA en la elaboración de la misma.*

En el caso de que se hubiera considerado que no procedía realizar una EIPD, la documentación justificativa (fechada y firmada) en la que se recojan los motivos por los que el BBVA consideraba que no estaba obligado a hacer la EIPD, incluyendo la documentación relativa a la intervención del Delegado de Protección de Datos donde expresó su criterio en esta cuestión. En tal caso, aportar la documentación acreditativa del análisis de riesgos efectuado, incluyendo toda la elaborada, justificativa de los resultados obtenidos y de las medidas adoptadas.

2) Documentación fechada y firmada relativa a las medidas técnicas y organizativas que tenía previstas el BBVA en fecha 14/04/2020 para evitar el fraude por suplantación de identidad, concretamente, en las operaciones a través de "BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA", cuando se ha producido la sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, y esta circunstancia ha sido comunicada por el cliente.

3) Documentación fechada y firmada relativa a las medidas técnicas y organizativas que el BBVA tenía implantadas con fecha 14/04/2020, para que las comunicaciones realizadas a la entidad por sus clientes por la pérdida, extravío o sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, produzcan efecto en sus diversos canales de relación con el cliente relativos la operativa que este pueda realizar."

El citado acuerdo se notifica a BBVA en fecha 14 de julio de 2023, como consta en el acuse de recibo que obra en el expediente.

En la actualidad, no consta en la AEPD que BBVA hubiera presentado escrito de respuesta a la práctica de pruebas.

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

De acuerdo con lo dispuesto en los artículos 58.2 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2 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
Antecedentes de hecho relevantes.

1. En relación con las comunicaciones entre las partes reclamante y reclamada.

De cara al análisis de las posibles infracciones cometidas, conviene resumir los antecedentes de hecho relevantes, en su sucesión cronológica:

- El robo de la documentación de la parte reclamante se habría producido en fecha anterior a 13/04/2020 y según la sentencia ***SENTENCIA.1 de ***FECHA.1, dictada por el Juzgado de Primera Instancia nº 10 de Barcelona el día 10/04/2020.

- Con fecha de 13/04/2020 la parte reclamante se habría puesto en contacto con la parte reclamada para anular una tarjeta de crédito de la que era titular

- Con fecha de 14/04/2020, la hija de la parte reclamante envía un correo electrónico a la sucursal en que esta operaba normalmente. En dicho correo se afirma lo siguiente:

  "Ayer robaron a mi madre (…) el móvil, el monedero y tarjetas, etc. Por favor urgente cancelar todas sus tarjetas, creo que tiene 2 pero no tengo los números conmigo aquí"

- En esa misma fecha de 14/04/2020, desde el banco se le contesta lo siguiente al correo anterior:
  "Solamente tiene una tarjeta y veo que ayer 13/04/2020 a las 18:06 fue bloqueada. Llamasteis vosotros al contact center de BBVA???

  Lo que veo que tiene diversos cargos a través de banca online que supongo no ha realizado ella.

Adjunto cargos realizados para que le des un vistazo... Si no fueran correctos necesitamos una denuncia de los mossos para poder tramitar la alta del fraude."

- Con fecha 17/04/2020, se remite un correo desde la abogada de la parte reclamante a la parte reclamada:

  "Te remito ahora la denuncia que nosotros dejamos interpuesta ayer contra la residencia. El proceso seguirá su curso y estimamos que en unas semanas entrará en el Juzgado, donde incoarán una causa penal"

- En fecha de 20/04/2020 se remite un correo desde la parte reclamada a la mencionada abogada:

  "Ya hemos enviado la denuncia al departamento correspondiente para su trámite. En cuanto a las transferencias, no te puedo decir nada más porque esto tiene su proceso natural y del departamento de seguridad y de fraudes entiendo que tendrán que evaluar el tema a través de la denuncia y de la información solicitada"

1. <u>En cuanto a la contratación fraudulenta de diversos productos</u>

Conforme a lo averiguado por la Inspección de esta Agencia, se contrataron los siguientes productos, en las fechas que se detallan (quedan fuera los productos financieros de los que la parte reclamante era titular antes de los acontecimientos):

- Préstamo de 4.000 euros suscrito el 12 de abril de 2020 del cual el reclamado especifica que no está cancelado. El reclamado indica que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*" con fecha 12 de abril de 2020.

- Tarjeta número ******TARJETA.2*** vinculada al contrato ***CONTRATO.3***.*** Sobre esta tarjeta la parte reclamante señala se solicitó desde su número de teléfono móvil y se envió a su dirección. Asimismo, expresa que los terceros la usaron posteriormente para realizar operaciones. El reclamado manifiesta que **se contrató el día 15 de abril de 2020 y** refiere que se firmó electrónicamente la solicitud de la tarjeta a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*" el 15 de abril de 2020

- Cuenta número ***CUENTA.3 (la parte reclamante cita "una cuenta terminada en ***XX***" en correo del 9 de septiembre de 2020) **suscrita el 27 de abril de 2020** de la cual el reclamado especifica que no está cancelada. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*" con fecha 27 de abril de 2020.

- Tarjeta número ***TARJETA.3 vinculada al contrato ***CONTRATO.4 **suscrito el 15 de abril de 2020** de la cual el reclamado especifica que se encuentra cancelada. Refiere que se ha firmado electrónicamente a solicitud de la parte

reclamante a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*" con fecha 15 de abril de 2020.

- Tarjeta número ***TARJETA.4 vinculada al contrato ***CONTRATO.5 **suscrito el 15 de abril de 2020** de la cual el reclamado especifica que se encuentra cancelada. Facilita (documento 12 adjunto al EscritoReclamado#2) la copia de del contrato, en el que figuran el nombre, apellidos, DNI de la parte reclamante, y el correo electrónico ***EMAIL.1. Refiere que se ha firmado electrónicamente a solicitud de la parte reclamante a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*" con fecha 15 de abril de 2020.

Como puede observarse, existió una segunda comunicación a la parte reclamada, en fecha 14/04/2020, ya que el día anterior hubo una primera para el bloqueo de una tarjeta, en que se avisaba de que la parte reclamante había sido objeto de un robo, incluyendo "*el móvil, monedero, las tarjetas, etc*". Con ello, se avisaba al banco de que habían sido sustraídos tanto las tarjetas como el teléfono móvil, con posibilidad incluso de que se hubieran apoderado de documentos identificativos. El robo del teléfono móvil, por lo demás, apunta a la posibilidad de que los delincuentes podrían tener acceso a la banca a distancia de la parte reclamante.

Pero no solo eso, sino que, en el correo electrónico de la parte reclamada, de fecha 14/04/2020, de contestación al aviso de robo por la parte reclamante, el banco afirma:

"*Lo que veo que tiene diversos cargos a través de banca online que supongo no ha realizado ella.*

Adjunto cargos realizados para que le des un vistazo... Si no fueran correctos necesitamos una denuncia de los mossos para poder tramitar la alta del fraude."

Manifestando con ello conocimiento de evidencias de posibles cargos fraudulentos. Con posterioridad, en fecha 17 de abril de 2020 se remitió al banco la denuncia interpuesta por la representación de la parte reclamante con fecha 16 de abril de 2020, tal y como se recoge en el Hecho Probado Noveno, en la que se denuncia la sustracción: "***Doña A.A.A.*** *manifiesta que se siente rara y que, además, en la residencia le han robado:*
+ el móvil
+ un monedero cuadrado con cremallera donde tenía su tarjeta de crédito, el DNI, su carné de conducir y su tarjeta sanitaria…".

A pesar de ello, como se ha detallado más arriba, los defraudadores tuvieron la posibilidad de continuar contratando, hasta una fecha tan lejana como 27/04/2020, diversos productos desde los cuales pudieron operar, efectuando movimientos, realizando transferencias y, en general, sustrayendo los activos dinerarios de que era titular la parte reclamante.

III
Contestación a las alegaciones aducidas al acuerdo de inicio

En relación con las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por la parte reclamada:

Con relación a las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por el BBVA:

1.- "*PREVIA. - SOBRE LA RESPONSABLIDAD ACEPTADA POR BBVA Y EL PAGO VOLUNTARIO"*

En esta primera alegación, BBVA atribuye los hechos objeto del este procedimiento a "*una serie de errores producidos en el presente caso, y deducidos en gran parte del hecho de que la persona que suplantó la identidad (en adelante, la "Usurpadora") de quien formuló la reclamación que da inicio al presente procedimiento (en adelante, la "Reclamante") pudo acceder a la información referida a sus claves de contratación electrónica como consecuencia de la sustracción de sus efectos, entre los que se encontraban su Documento Nacional de Identidad, su teléfono móvil y su tarjeta de crédito.*

BBVA continúa en su razonamiento señalando que "*como consecuencia de dichos errores, los sucesivos bloqueos de los productos financieros contratados por la Reclamante con mi mandante, así como los reintegros de fondos realizados a su cuenta pudieron ser objeto de levantamiento…*

Sin embargo, mi mandante no puede reconocer, y de hecho niega categóricamente, que no haya aplicado en la política de admisión y contratación de sus clientes los principios de privacidad desde el diseño (en adelante, por sus siglas en inglés, "PbD") y las medidas técnicas y organizativas adecuadas encaminadas a la garantía y protección de los derechos fundamentales de sus clientes, y en particular de su derecho fundamental a la protección de datos personales.

En este sentido, considera mi mandante que la AEPD pretende aplicar a lo que no es sino un desafortunado incidente, que mi representada no niega reconocer, una suerte de doctrina general, según la cual mi mandante no estaría impidiendo, con carácter general, la posible usurpación de la identidad de sus clientes como consecuencia de la existencia de una serie de errores en el caso concreto al que se está haciendo referencia en el presente procedimiento. Es decir, la AEPD no sólo imputa a mi mandante los hechos concretos acaecidos y probados, sino que extiende dicha imputación más allá de las circunstancias del caso concreto, negando el establecimiento de unas medidas que, lamentablemente, han fallado en el presente supuesto, o que por parte de BBVA se apliquen los principios de protección de datos personales en el desarrollo de su actividad y en las relaciones derivadas de la actividad de sus clientes con la misma".

En contestación a esta alegación, cabe señalar que las infracciones que se le imputan a BBVA no tienen como fundamento "*una suerte de doctrina general*", sino que las conductas que motivaron el presente procedimiento derivan de unos hechos concretos ante los cuales se ha puesto de manifiesto, por un lado, que en el documento para la gestión de incidentes aportado por el BBVA denominado "Prevención del fraude y de la

estafa", no aplica el principio de protección de datos desde el diseño y por defecto en el tratamiento de datos personales de sus clientes, esto es, que, en lo relativo a dicho principio, BBVA no tiene medidas de técnicas y organizativas apropiadas para evitar sucesos como el acontecido en la contratación de productos financieros como para la realización de operaciones, especialmente a través del canal "*BANCA A DISTANCIA TELEFONÍA MÓVIL/TARJETA*", una vez que el cliente ha comunicado de forma reiterada y por diversos canales a BBVA la pérdida o sustracción de su DNI, teléfono móvil o tarjeta de crédito.

En efecto, como se desarrollará más adelante, ha quedado acreditado que BBVA no tenía analizado el riesgo que se produce, desde el punto de vista del derecho fundamental a la protección de datos personales, en supuestos de pérdida o sustracción de documentación identificativa o de dispositivos o terminales (teléfonos móviles, tarjetas de crédito) que pueden dar lugar al uso de datos personales con objeto de causar un perjuicio patrimonial a su titular y un enriquecimiento ilícito a los defraudadores. Esto ha propiciado que, en ausencia de medidas técnicas u organizativas que hubieran sido implantadas ante el análisis de riesgos mencionado y que habrían evitado que, una vez sustraída la documentación a un cliente, los suplantadores pudieran haber continuado, durante semanas contratando productos financieros a nombre del cliente, con el consiguiente perjuicio patrimonial para este.

Desde BBVA se argumenta que estos hechos se han producido por una "*serie de errores"*. No cabe sino discrepar de esta visión de los hechos. La sustracción de los medios de identificación (DNI) o autentificación (teléfono móvil) de los clientes de BBVA, no puede considerarse un error, sino un riesgo cierto por el cual los clientes del BBVA pueden sufrir una pérdida de control sobre sus datos personales. Este riesgo debe preverse por el responsable del tratamiento. Desde el momento en el que el cliente comunica al BBVA la sustracción de los medios de identificación o autenticación, la cautela ha de presidir en la entidad bancaria, puesto que puede no ser el cliente quien efectivamente está realizando las operaciones. De la lectura de los Hechos Probados de este documento se comprueba que las continuas peticiones realizadas por la parte reclamante para que sus datos personales dejaran de ser tratados de forma ilegal han sido desatendidas por el BBVA. En este caso, BBVA dar por buenas las operaciones por el sólo hecho de utilizar el doble factor de autenticación, cuando éste se produce a través de un medio (el teléfono móvil), cuya sustracción ha sido comunicada por el cliente de BBVA, por lo que se producen tantos errores continuos, concatenados que ponen de manifiesto una falta absoluta de procedimiento para evitar el tratamiento ilegal de datos personales. Esta entidad ha reconocido que se ha producido la contratación de productos bancarios, pero, lejos de ser un hecho puntual, nos encontramos que de forma sistemática se ha podido vulnerar el derecho a la protección de datos de la parte reclamante. De la documentación aportada por BBVA, recogida en los Hechos Probados Cuadragésimo Tercero y Cuadragésimo Quinto, y que se analizará posteriormente en esta contestación a las alegaciones, se constata la inexistencia de procedimientos respecto a la prevención del fraude en operaciones online, sobre todo en supuestos de robo o pérdida de información que puede ser utilizada para cometer fraude y en general de procedimientos para la gestión de incidentes en relación con el fraude, con unas directrices no actualizadas, no adaptadas al RGPD y no enfocadas en los riesgos para los derechos y libertades de los clientes.

En consecuencia BBVA, en primer lugar, tiene que realizar un diseño de sus tratamientos de datos personales aplicando el principio de protección de datos desde el diseño y por defecto, que tenga en cuenta los riesgos para los derechos y libertades de las personas físicas y, en segundo lugar, debe tener medidas que garanticen la seguridad de los datos en cuestión y los derechos y libertades de las personas físicas, máxime cuando un cliente comunique la sustracción de dichos elementos de forma reiterada, y por los diversos canales de relación con sus clientes que el BBVA dispone, y sabiendo que los datos sustraídos se deben utilizar para la banca online .

2.- "*PRIMERA. - SOBRE LA SUPUESTA VULNERACIÓN POR BBVA DEL PRINCIPIO DE PROTECCIÓN DE DATOS DESDE EL DISEÑO, CONCULCADO EN EL ARTÍCULO 25 DEL RGPD".*

Esta alegación, a su vez, se divide en los siguientes subapartados:

"1. Sobre el contenido del Acuerdo de Inicio y el alcance de la infracción que pretende imponerse a mi mandante "

Según BBVA, en el acuerdo de inicio se hace una "*argumentación aparente*" por cuanto en ningún momento se acredita si en realidad BBVA ha dado cumplimiento a las obligaciones derivadas del citado precepto, sino que el citado fundamento de derecho consiste única y exclusivamente en una descripción de lo que a juicio de la AEPD debe considerarse que implica el principio de protección de datos desde el diseño.

En primer lugar, hemos de significar que el acuerdo de inicio de un procedimiento sancionador se encuentra regulado en el artículo 64 de la LPACAP, el cual dispone que debe contener al menos, entre otras cuestiones, *"2. b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción".* Por ello, no es el acto administrativo en el que debe de acreditarse si se ha cometido una infracción administrativa, tal y como pretende la parte reclamada, sino en el que se consignan los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, tal y como se ha hecho, sin perjuicio de lo que resulte de la instrucción.

En segundo lugar, y entrando en el fondo del asunto, en respuesta al argumento esgrimido por BBVA, hay que señalar que el cumplimiento del principio de responsabilidad proactiva, y en particular de la protección de datos desde el diseño y por defecto (en adelante "PDDD"), se materializa, tanto en el momento de determinar los medios del tratamiento como en el momento del propio tratamiento, en la adopción de medidas técnicas y organizativas apropiadas, de todo tipo, concebidas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados.

Tal y como se fundamentaba en el Fundamento de Derecho V del acuerdo de inicio en cuanto a la infracción del artículo 25 del RGPD, en primer lugar, el cumplimiento de la PDDD conlleva que *"el responsable del tratamiento llevará a cabo un ejercicio de análisis y detección de los riesgos durante todo el ciclo de tratamiento de los datos,*

con la finalidad primera y última de proteger los derechos y libertades de los interesados, y no sólo cuando efectivamente se produce el tratamiento", de acuerdo con lo que establece expresamente el artículo 25.1 del RGPD: "*Teniendo en cuenta… los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas…".*

Asimismo, se indicaba que "*Examinado el documento, se observa que tienen un enfoque eminentemente empresarial o de "negocio". Su finalidad es tratar de evitar prácticas fraudulentas de las que se derive un perjuicio para la entidad. Con ello indirectamente se podrá evitar un perjuicio patrimonial para el usuario, pero no se protege su Derecho Fundamental a la Protección de Datos Personales, no se protegen sus derechos y libertades, que es la finalidad última que persigue el RGPD a través de la protección de datos desde el diseño. No se trata, por lo tanto, de un documento concebido para el cumplimiento del principio de responsabilidad proactiva (artículo 5.2 RGPD), ya que para ello debería haberse partido del mencionado análisis de riesgos que llevara a la adopción de medidas para la protección de los derechos y libertades, a partir siempre del diseño del tratamiento. (…) Así, examinado el procedimiento establecido por la entidad bancaria respecto a la gestión de incidentes en relación con el fraude, se observa que está totalmente desactualizado, no adaptado al RGPD y no enfocado en los riesgos para los derechos y libertades de los clientes, lo que muestra que no se ha cumplido con la obligación dispuesta en el artículo 25 del RGPD en relación con el diseño y la integración de la protección de datos en el sistema de detección del fraude de la organización*".

Pues bien, de conformidad con la literalidad del documento, tal y como se dispone en el Hecho Probado Cuadragésimo Tercero (documento 3), este documento tiene un enfoque en los riesgos para la entidad y no para proteger los derechos y libertades de los clientes de la parte reclamada en materia de protección de datos, tal y como propugna el RGPD.

Así, se puede comprobar del contenido del citado documento que dispone que:

> *"Una de las claves de la relación cliente-entidad financiera es la confianza que debe establecerse. Sin duda, desde ese punto de vista, los ataques a la seguridad de determinados productos o servicios pueden deteriorar este principio.*
> *…*
> *La defensa de la confianza en los procesos, el preservar la reputación de las propias entidades, dado que el fraude afecta muy negativamente a la imagen de las mismas, y evitar quebrantos que, una vez producidos, son, en la mayoría de los casos, irrecuperables, hacen necesario potenciar la prevención en este campo mediante la emisión de normas y la actuación formativa.*
> *…*
> *Si el banco no opera correctamente, puede incurrir en una grave responsabilidad, por lo que estas prácticas no deben realizarse".* (el subrayado es nuestro)

De igual forma podemos ver ese enfoque en los riesgos en la entidad bancaria en los activos que se protegen, como la recepción de billetes falsos, o sobre el sujeto de la

estafa, la entidad bancaria, como acontece en lo que se recoge en el documento relativo a los créditos al consumo.

Examinado el citado documento no se identifican los riesgos en los derechos y libertades de los interesados, ni se evalúan, ni se determinan medidas técnicas y organizativas para garantizar el Derecho Fundamental a la Protección de Datos de Carácter Personal.

Además, en 2015, cuando se elaboró este documento de la parte reclamante, estaba vigente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que no contenía disposición alguna en relación con el diseño del tratamiento, con el enfoque en los derechos y libertades de los interesados, con la implantación de medidas técnicas y organizativas de todo tipo y apropiadas para garantizar dichos derechos y libertades. Se limitaba a hacer mención a las medidas de seguridad, lo que ahora constituyen una parte de la totalidad de las medidas técnicas y organizativas de todo tipo recogidas en el artículo 25 del RGPD y que el responsable del tratamiento debe implementar. Se trata de un documento que no recoge un procedimiento para evitar los fraudes, estafas y suplantaciones de identidad en las operaciones online, ni siquiera se prevén los riesgos de suplantación en estas operaciones. Tampoco contiene procedimientos para detectar operaciones fraudulentas. Es de resaltar que el documento es anterior al Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera que traspuso parcialmente la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 sobre servicios de pago

Curiosamente, desde 2015 a 2023, pasando por la aplicabilidad del RGPD en mayo de 2018 (y habiendo transcurrido cinco años desde entonces), dicho documento no ha sido adaptado a las premisas del RGPD, ni mudado ninguno de sus aspectos en relación ni con el enfoque del riesgo, ni con los riesgos mismos.

Por todo ello, no puede tenerse por bueno el enfoque de riesgos previstos en un documento elaborado en el año 2015, antes de la propia existencia del RGPD y, consecuentemente, de la PDDD como una obligación propia del responsable del tratamiento derivada de la responsabilidad proactiva, sin tener en cuenta, a mayores, la propia evolución de la tecnología y los riesgos que pueden aparecer o mudar por el mero transcurso del tiempo.

Ni una mención en el documento que *"pretende difundir aquellas medidas básicas de vigilancia que puedan permitir detectar y abortar la gran mayoría de los fraudes que se producen, con un reducido esfuerzo"* a la operativa online entre los clientes y la entidad que hoy en día está generalizada. Ni una mención al fraude online.

Tan sólo una mención a las compras a distancia con tarjeta (por internet, correo o teléfono) y, para, de nuevo, hacer referencia a los riesgos que puede o no soportar la entidad y ninguno del cliente:

> *"* Operaciones sin presencia física de la tarjeta.- En estos casos (compras por INTERNET y venta por correo/teléfono), es el comercio el que asume contractualmente la responsabilidad, salvo en el caso de comercio seguro con autenticación del titular. Eso no nos exime de prestar atención a este tipo de*

fraude ya que redunda indirectamente en la fiabilidad de este producto y, por tanto, en su utilización y rentabilidad".

Añadiremos que el citado documento se basa únicamente en la seguridad de la información (que puede contener o no datos personales) como premisa primera y única que fundamente la conformación del mismo.

A mayor abundamiento, todo esto no es una "*argumentación aparente*", sino una argumentación fundada de la infracción atribuible a BBVA, como responsable del tratamiento en cuestión.

En segundo lugar, BBVA no explica en qué medida el contenido de cada documento aportado en sus alegaciones está relacionado con el cumplimiento del PDDD respecto al tratamiento de los datos personales objeto del presente procedimiento, tan sólo enumera un listado de documentos sin motivar como contribuyen a cumplir con el PDDD.

De la lectura de dichos documentos, no se puede decir que ni el documento "Prevención del fraude y de la estafa", elaborado en el año 2015 como ya se dijo anteriormente, aportado por BBVA en la contestación al requerimiento de información formulado por esta Agencia, como los documentos aportados en el trámite alegaciones a que se refiere el Hecho Probado Cuadragésimo Quinto, cumplan con el PDDD por los siguientes motivos:

- Documento nº 1: Este documento recoge una normativa interna de "seguridad desde el diseño", que se describe como un proceso en el que se "alienta" a los desarrolladores de productos, servicios y aplicaciones a que tengan en cuenta los principios básicos establecidos en la normativa de protección de datos en el momento de desarrollar y diseñar estos productos, servicios y aplicaciones.

Se categorizan una serie de riesgos, principalmente tecnológicos, y se establece un proceso por el que dicen considerar las medidas técnicas y/o organizativas necesarias para garantizar la seguridad y privacidad de los datos. El área de Data Security interviene en este proceso, no se dice nada del Delegado de Protección de Datos a los efectos de realizar sus funciones de asesoramiento e información en cuanto al cumplimiento del RGPD. Posteriormente se habla de la "Estrategia antifraude" donde se relacionan los mecanismos de autenticación y firma de operaciones.

En este documento se hace referencia a riesgos tecnológicos (véase el cuadro recogido en el documento 1 del Hecho Probado Cuadragésimo Quinto), el enfoque no está en los riesgos a los derechos y libertades de los interesados, como el riesgo de pérdida financiera. Las medidas a las que hacen referencia son medidas de seguridad tecnológica que no están dirigidas a evitar o minimizar los riesgos en los derechos y libertades de las personas. Así, en la página 3 determinan los objetivos, algunos de los cuales no son riesgos en los derechos y libertades de los interesados sino riesgos de la organización.

Según indica el propio documento, la normativa que denomina de "Security By Design", fue generada en septiembre del año 2017 y la última revisión efectuada en julio de 2022, con posterioridad a los hechos.

- Documento nº 2: Con el título "*Actuaciones Security by Design*", en primer lugar, hay que señalar que este documento es posterior a los hechos que se analizan. La reclamación es de octubre de 2021, el robo se produjo el 10/04/2020 y el 14/04/2020 existe constancia en el expediente que la entidad financiera tenía conocimiento de los hechos.

Segundo, este documento relaciona una serie de principios para el cumplimiento del artículo 25 del RGPD, y una serie de "normas y guías de buenas prácticas" en materia de seguridad que copia, básicamente, la guía de la AEPD de privacidad desde el diseño, sin mayores concreciones. Además, el documento cuando habla de medidas de seguridad desde el diseño en BBVA, se limita a intercalar una serie de enlaces dirigidos a otros documentos.

Documento nº 3: Con el título "*Norma de Clasificación de Información Normativa interna (BBVA)"*, el documento es de 5 de noviembre de 2019.

Esta "norma" provee unas directrices a seguir en el área de Tecnología para la implementación de medidas de seguridad sobre los Sistemas de Información propiedad de BBVA. Establece directrices en cuanto a evaluación de riesgos (sin llevar a cabo dicha evaluación), clasificación de la información, uso correcto de activos, gestión de medios extraíbles y destrucción de medios físicos, transferencia por medios físicos (directrices de transferencia de información en formato papel y formato electrónico dentro de BBVA) y medidas de protección y monitorización de la información.

Sin embargo, a pesar de que existen varias versiones sólo se hace referencia a la última, desconocemos por tanto las anteriores. Incluyen básicamente riesgos en la organización y riesgos tecnológicos, faltando el enfoque en los riesgos referido a los derechos y libertades en cuanto a la protección de datos de los clientes. En su texto se clasifica información y activos, que es en lo que está focalizado en el documento, y no en la protección de los datos personales Esto supone que, incluso aunque pudiera considerarse que de manera indirecta se protejan los datos personales, dado que se incluyen en la información y en los activos, el enfoque no es el correcto. En este sentido, la evaluación de los riesgos y las medidas a adoptar puede ser errónea debido justo a este enfoque.

Debe tenerse en cuenta que los riesgos no se producen sólo en relación con la seguridad de los sistemas de información de la entidad, sino que también pueden existir riesgos en el entorno virtual relacionados con los derechos y libertades de las personas físicas, en particular en casos en que el titular de los datos ha perdido el control sobre información que puede ser utilizada para suplantar su identidad.

Al final del texto se mencionan tres anexos: ANEXO I - Medidas de Protección y Monitorización. ANEXO II - Información Especial. ANEXO III - Excepciones. No pueden ser analizados dichos anexos ya que no se acompaña su texto.

- Documento nº 4: Bajo el título *"Agile Risk Assessment*" (traducción no oficial, "Evaluación ágil de riesgos"), "*Alertas de seguridad ante bloqueo de usuario*", el

documento realiza una valoración de riesgos en materia de alertas de seguridad ante bloqueo de usuarios. En el documento no se realizan consideraciones sobre el nivel de riesgo, siendo el único riesgo asociado el incumplimiento de la normativa en materia de pagos, un riesgo de la organización. Por otra parte, se identifica en estos procesos riesgos relacionados con el fraude tecnológico.

Se mezclan, además en este documento, riesgos de la organización con los de los interesados (hablan de riesgo tecnológico) y solo se refiere al establecimiento de una alerta de seguridad ante el bloqueo de usuario antes de que se produzca por reintentos de sesión fallidos y tras el mismo.

- Documento nº 5: Bajo el título "*Agile Risk Assessment*" (traducción no oficial, "Evaluación ágil de riesgos"), "*Bloqueo Hard Fraude*", el objetivo de la iniciativa consiste en implementar una serie de modificaciones en los procesos de bloqueo y desbloqueo de usuario de los clientes del BBVA que la reclamada divide en dos tipos: soft y hard. En ambos casos, el bloqueo a nivel operativo para el cliente es el mismo, es decir, no podrá operar con su perfil multicanal.

Parece que existe un defecto en el diseño de los procedimientos que han se seguirse en caso de riesgo de fraude y suplantación. Lo que se puso de manifiesto en este caso que se solicitó el bloqueo de la cuenta y los suplantadores de la identidad de la parte reclamante continuaron operando con la misma. La entidad reclamada no ha aportado ningún documento en el que se recojan los procedimientos implementados por la entidad para proceder al bloqueo en el caso de que terceros no autorizados tengan acceso a las claves del primer factor de autenticación, o a información personal que permita suplantar la identidad del cliente, una vez que BBVA tiene conocimiento de ello.

Además, en dicho documento, se indica en la página cinco en cuanto a los riesgos de privacidad e integridad de datos que no se contemplan riesgos, habiéndose puesto de manifiesto en el caso al que se refiere este expediente, la existencia de riesgos, por lo que sí existía un riesgo cierto, que se ha materializado y que BBVA no ha sido capaz de identificar.

- Documento nº 6: Bajo el título "*Dictamen de medidas técnicas de Seguridad y Fraude Olvido/Desbloqueo de password de usuario multicanal sin tarjeta*", el objetivo del dicho documento es definir los requisitos de seguridad asociados a la iniciativa "Olvido/desbloqueo de password de usuario multicanal sin tarjeta" y describe las tareas a realizar, así como los costes asociados al proyecto, por parte de las áreas de Protección de Datos y IT Risk Fraud & Security.

Al respecto de este documento hay que indicar que su fecha es anterior a la de la entrada en vigor del RGPD. Es la versión inicial y desconocemos si hay versiones posteriores que, en todo caso, no han sido aportadas por la reclamada. Además, no se categorizan los riesgos en cuanto a la protección de datos personales , por lo que el documento está encaminado a evitar el fraude económico y no a proteger a los clientes de la entidad respecto al tratamiento sus datos personales,

- Documento nº 7: Bajo el título "*Límites de fraude para operativas < 20 de Bizum sin OTP*", el objetivo de esta iniciativa consiste en una aplicativa que solo afecta a BIZUM,

utilizada para agilizar el proceso de pago con eliminando el segundo factor para operaciones de 20 € o menos, con un máximo de 3 operaciones al día de este tipo.

Respecto de este documento hay que indicar que la fecha es anterior a la entrada en vigor del RGPD y en la fecha que acontecieron los hechos, por tanto, estaba desactualizado. Además, en este caso, no hubo ningún aviso que alertara al BBVA de que terceros no autorizados estaban realizando operaciones a través de Bizum con los datos de la parte reclamante.

- Documento nº 8: Del informe de auditoría emitido por un Deloitte Advisory, S.L. hay que indicar que los hechos investigados suceden a lo largo del año 2020 y esta auditoría es de finales del 2022, dos años después. En dicho informe se recogen la metodología, el modelo y los índices de fraude notificados del Reglamento Delegado 2018/389, no del cumplimiento del RGPD.

- Documento nº 9: En el "*Contrato Multicanal*" se establecen las condiciones generales de todos los canales y servicios adscritos a dichos canales, concretamente: Banca por internet, Teléfono móvil, Canal Autoservicios: Cajeros Automáticos y Terminales en Oficinas y, por último, Banca Telefónica y que se basa en un modelo de la versión de 27 de noviembre de 2016, y que lo único que demuestra es que la parte reclamante tenía un contrato suscrito con la reclamada para la contratación de productos o servicios bancarios. La parte reclamante cumplió debidamente, tal y como se recoge en el Hecho Probado Quinto, con la obligación establecida en la cláusula 8.3 de dicho contrato, notificando a BBVA la sustracción del teléfono móvil sin demora indebida en cuanto tuvo conocimiento de ello.

En consecuencia, por los motivos expuestos anteriormente, ha quedado desacreditada la afirmación de BBVA de que "*ha llevado a cabo respecto de la totalidad de sus tratamientos de datos personales, y en concreto respecto de los referidos a la utilización por parte de sus clientes de los canales on-line, el pertinente análisis de riesgos, determinando las medidas técnicas y organizativas pertinentes para garantizar el respeto de los derechos de los interesados*".

"2. Sobre el alcance del principio de protección de datos desde el diseño"

En este punto, BBVA realiza una interpretación acerca del alcance de la PDDD, según el cual considera que ha analizado y valorado plenamente todas las medidas que correspondía adoptar para garantizar el cumplimiento de los principios establecidos en el artículo 25 del RGPD, sin perjuicio de que no sea considerado suficiente por parte de la autoridad de control.

En respuesta a este argumento, de la documentación aportada por BBVA, analizada de forma pormenorizada anteriormente, no se acredita que se hayan tenido en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de sus clientes en el procedimiento establecido por la entidad bancaria respecto a la gestión de incidentes en relación con el fraude, ante la falta de protección de los derechos la parte reclamante que ha quedado en evidencia ante las constantes desatenciones a las comunicaciones realizadas por la parte reclamante de la ilegalidad del tratamiento de sus datos personales con la suplantación para el acceso a sus productos,

realización de operaciones y contratación de productos nuevos ante el BBVA, especialmente a través del canal “BANCA A DISTANCIA TELEFONÍA MÓVIL/TARJETA”,

Analizada toda la documentación aportada, en las distintas fases de este procedimiento, por BBVA, se observa que esta entidad no cumplía con el principio de privacidad desde el diseño. En primer lugar, no existía un análisis de riesgos adecuado. Ni uno solo de los documentos aportados abordaba el riesgo derivado de la pérdida o sustracción de determinada documentación identificativa, (o los métodos o dispositivos para el acceso a su banca online) al quedar al descubierto los datos personales que permiten la contratación a distancia de productos financieros.

Los documentos aportados no contienen ningún análisis de este riesgo y, con ello, no arbitraban medidas técnicas u organizativas que podrían evitar la lesión del derecho fundamental a la protección de datos e, indirectamente con él, los bienes y derechos patrimoniales de que son titulares los clientes de la entidad bancaria. Por el contrario, estos documentos se centran en la evitación de riesgos esencialmente para la propia entidad. Abordan riesgos tecnológicos, organizacionales o de negocio que pueden concluir en un perjuicio patrimonial para el banco.

A este respecto, debe recordarse que conforme al artículo 25 del RGPD:

“Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, c*omo la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.”* (el subrayado es nuestro)

Es decir, la protección del derecho fundamental a la protección de datos no consiste en una mera espera “reactiva” a que pueda producirse un problema que lo lesione, sino que los responsables del tratamiento deben diseñar (“protección de datos desde el diseño”) con carácter previo al inicio del tratamiento, las políticas adecuadas para la protección de dicho derecho fundamental. Y ello incluye todos los aspectos regulados en el RGPD, comenzando por las obligaciones de transparencia, el respeto al ejercicio de los derechos establecidos en el Reglamento, y el establecimiento de todas medidas técnicas y organizativas necesarias para garantizar el cumplimiento de dicha norma. Y asimismo las medidas de seguridad. Y todo ello debe estar planificado e implementado con carácter previo al inicio del tratamiento por el responsable.

Derivado de las actuaciones de inspección llevadas a cabo por esta Agencia, así como del resto de documentación y alegaciones presentadas por BBVA en este procedimiento, ha podido constatarse que dicho principio (y en consecuencia el artículo 25 del RGPD) no se cumplían por la entidad bancaria. No existía un análisis de riesgo que hubiera identificado el riesgo de contrataciones mediante suplantación

cuando algún cliente extraviara y le fuera sustraída su documentación identificativa o su teléfono móvil.

A este respecto, el análisis de riesgo es una pieza clave del principio de privacidad desde el diseño, ya que es lo que permite el establecimiento de medidas técnicas y organizativas que los eviten o, en caso de producirse, los palíen. Como se ha señalado, el artículo 25 hace especial referencia a "los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas", como presupuesto para el establecimiento de dichas medidas.

Se ha comprobado que ni el riesgo estaba establecido ni con ello las medidas implantadas. Y todo ello queda corroborado por el caso que dio lugar a este expediente. En efecto, como ha quedado ampliamente narrado en los hechos probados de esta propuesta, desde el 14 de abril de 2020, y en reiteradas ocasiones, se había notificado a BBVA la sustracción del teléfono móvil número ******TELÉFONO.1*** y la documentación identificativa de la parte reclamante***.*** Sin embargo, BBVA mantuvo este dato personal de la parte reclamante como medio a través del cual se producía la autenticación de la identidad de la parte reclamante, lo que evidencia una falta de medidas adecuadas aplicables a estas situaciones.

Además, la aplicación del PDDD, a diferencia del argumento planteado por BBVA, no se limita a la adopción de unas medidas determinadas, que pueden ser consideradas adecuadas o no por la autoridad de control, sino que estas medidas deben ser efectivas. Es decir, que el RGPD no establezca unas medidas concretas en materia de PDDD, ya que estas dependen el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad, esto no significa que cualquier medida adoptada sea apropiada.

Cabe traer a colación las consideraciones realizadas por el Comité Europeo de Protección de Datos (CEPD), el cual, en cumplimiento del objetivo de garantizar la aplicación coherente del Reglamento General de Protección de Datos (según le atribuye el artículo 70 del RGPD), con fecha 20 de octubre de 2020 adoptó las Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto (https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf). En los apartados 7 y siguientes de dichas directrices se establece que:

"7. *En un sentido amplio, cabe entender que las medidas técnicas y organizativas y las garantías son cualquier método o medio que el responsable pueda emplear en el tratamiento. Para que sean adecuadas, las medidas y las garantías necesarias deben ser adecuadas para conseguir el fin previsto, es decir, deben aplicar los principios de protección de datos de forma efectiva.*

8…

13. La efectividad es la base del concepto de protección de datos desde el diseño. El requisito de aplicar los principios de manera efectiva implica que los responsables del tratamiento deben aplicar las medidas y garantías necesarias para proteger dichos principios, a fin de garantizar los derechos de los interesados

14. Primero, significa que el artículo 25 no requiere la aplicación de ninguna medida técnica u organizativa específica, salvo en el sentido de que las medidas y garantías elegidas deben ser específicas para la aplicación de los principios de protección de datos en el tratamiento en cuestión. Para ello, las medidas y garantías deben concebirse para que sean sólidas y el responsable debe poder aplicar medidas adicionales a fin de adaptarlas a cualquier incremento del riesgo. Las medidas y garantías aplicadas deben conseguir el efecto deseado en términos de protección de datos, y el responsable del tratamiento debe disponer de documentación sobre las medidas técnicas y organizativas aplicadas

15. Segundo, los responsables del tratamiento deben ser capaces de acreditar que estos principios se han mantenido." (el subrayado es añadido).

Por lo tanto, la PDDD pretende garantizar que se apliquen de forma efectiva los principios de protección de datos, tales como licitud, lealtad, transparencia, exactitud, integridad y confidencialidad, por lo que su alcance no depende, a diferencia del argumento que plantea BBVA de que sea considerado suficiente por esta Agencia. Los Hechos Probados ponen de manifiesto que estos principios no se garantizan mediante las medidas adoptadas por el BBVA.

"3. Sobre las exigencias adicionales de seguridad establecidas por la normativa sectorial aplicable a BBVA y su implementación en el supuesto que genera el presente procedimiento"

BBVA sostiene que *"la propia Directiva PSD2 y sus normas de desarrollo y transposición la que determina los criterios de PbD que deben ser tenidos en cuenta para garantizar, no sólo la prevención del fraude y la seguridad de las operaciones en línea, sino los derechos de los interesados y, en particular, su derecho a la protección de datos personales."* En base a las medidas adoptadas para el cumplimiento de la Directiva (UE) 2015/2366, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y al Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, "RDL de servicios de pago"), así como por aquellas medidas adoptadas en cumplimiento del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros (en adelante, "Reglamento Delegado"), BBVA entiende que ha implementado la PDDD en los tratamientos de datos de sus clientes.

Sin embargo, el enfoque de tales medidas, adoptadas para el cumplimiento del RDL de servicios de pago, pudiendo tener relación con los principios del RGPD, no suponen el cumplimiento de este, el cual está centrado en el riesgo para los derechos y libertades de los interesados. Partimos de la base de que la Directiva que transpone el RDL de servicios de pago, del año 2015, es anterior al RGPD que es del año 2016, y que su cumplimiento no excluye la observancia de los principios que consagra el RGPD. Cabe recordar que en la PDDD el análisis de los riesgos es continuo y no se cumple con el RGPD si estos no se revisan.

Del análisis de la documentación aportada por BBVA, se pone de manifiesto que BBVA no tiene procedimientos internos para evitar riesgos que puedan producirse en circunstancias tales como que el cliente comunica la sustracción del documento de identidad o del teléfono móvil. Recordemos que la protección de datos de carácter personal en el uso de la informática es un derecho fundamental reconocido en el artículo 18 de la Constitución Española de 1978.

A este respecto, la falta de respeto al principio de PDDD viene ilustrado por el caso concreto que se produjo, pero sobre todo en el procedimiento utilizado que es el mismo con independencia del número de personas que pudieran estar afectadas tal y como se desprende de la documentación aportada por el reclamado e indicada en los Hechos Probados Cuadragésimo Tercero y Cuadragésimo Quinto.

Subsidiariamente, cabe señalar que el apartado b) del artículo 41 "*Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas"*, del RDL de servicios de pago, dispone que:

"El usuario de servicios de pago habilitado para utilizar un instrumento de pago:

a…

b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello".

En los Hechos Probados se recogen una serie de comunicaciones, la primera de ellas el 14 de abril de 2020 (Hecho Probado Quinto), enviadas por la parte reclamante y por su representante en las que pone en conocimiento de BBVA la sustracción de, entre otros objetos, un medio de pago (tarjetas) y del factor de autenticación (teléfono móvil con número de teléfono ******TELÉFONO.1)***. En estas comunicaciones se solicitan la paralización de las operaciones realizadas con instrumentos de pagos cuya sustracción había sido comunicada, o que habían sido contratados ilegalmente, por lo que la parte reclamante cumplió con la obligación establecida por el artículo 41.b) del RDL de servicios de pago.

Sin embargo, no puede decirse que BBVA, a la vista de los Hechos Probados, haya cumplido con las obligaciones del proveedor del servicio de pagos establecidas en el artículo 42 del RDL de servicios de pago, concretamente, en su apartado a) se establece que el prestador de servicios de pago "s*e cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41"* y el apartado e) de dicho artículo dispone que *"impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b)".*

En el presente caso, consta en los Hechos Probados que, pese a la comunicación realizada por la parte reclamante de la sustracción de su DNI, de su tarjeta y de su teléfono móvil el cual es un factor de autenticación para operar con cuentas bancarias,

tarjetas de crédito y operaciones de BIZUM, son múltiples las operaciones que quienes suplantaron la identidad de la parte reclamante pudieron realizar utilizando ilegalmente sus datos personales. En la documentación aportada por el BBVA no se recoge la posibilidad de que un número de teléfono deje de ser factor de autenticación para operar en "*BANCA A DISTANCIA TELEFONÍA MÓVIL/TARJETA*" cuando su titular haya comunicado la sustracción del teléfono móvil.

Hay que tener en cuenta que el documento "*Prevención del fraude y de la estafa*" aportado por BBVA, es del año 2015, previo al propio RDL de servicios de pago, del año 2018, por lo que no es posible que en aquel se hayan recogido las obligaciones de esta norma. Tampoco se realiza una evaluación del riesgo para los derechos y libertades de los clientes del BBVA con relación a las operaciones de fraude, una vez que aquellos hayan cumplido con la obligación establecida en el artículo 41.b) del RDL de servicios de pago.

Por todo lo expuesto, se desestima la presente alegación.

"SEGUNDA. - SOBRE LA AFECTACIÓN A LOS PRINCIPIOS DEL DERECHO SANCIONADOR DERIVADOS DE LA INTERPRETACIÓN EFECTUADA POR LA AEPD"

1. Vulneración del principio non bis in idem

Desde BBVA se realiza una interpretación errónea de las infracciones que se le imputa, al afirma que: "…*la AEPD considera que en este caso, la supuesta insuficiencia de las medidas de seguridad que, a su juicio, resultan exigibles en este supuesto implica una doble vulneración del RGPD: (i) por una parte, entiende que mi mandante no ha adoptado las medidas técnicas y organizativas adecuadas, exigidas por el artículo 32.1 del RGPD en el procedimiento de identificación de sus clientes y; (ii) por otra, que la ausencia o insuficiencia de esas medidas conduce a la apreciación de que mi mandante no ha cumplido las exigencias derivadas del cumplimiento del artículo 25.1 del mismo texto legal.*

En primer lugar, la infracción del artículo 32 del RGPD no se refiere a que no se hayan adoptado medidas técnicas y organizativas adecuadas en el procedimiento de identificación de clientes. Los hechos que suponen la infracción del artículo 32 del RGPD se definen en el acuerdo de inicio de la siguiente forma: "*ni de la documentación o información aportadas por el reclamado, ni mucho menos de los resultados producidos en este caso puede deducirse que BBVA dispusiera de un procedimiento adecuado referido a la implementación y aplicación de medidas de seguridad de datos personales apropiadas, técnicas u organizativas, para evitar sucesos como el acontecido en una contratación ni tampoco para la inclusión o el mantenimiento de los datos de los clientes en sistemas de información crediticia cuando la deuda es controvertida."* (el subrayado es nuestro)

En segundo lugar, la infracción del artículo 25 del RGPD, no puede relacionarse como hace BBVA, las medidas de seguridad del artículo 32 del RGPD *("…la ausencia o insuficiencia de esas medidas…"),* con las medidas a que se refiere el artículo 25 del

RGPD, ya que en este se contempla la adopción de medidas, no sólo de seguridad, sino de todo tipo.

El art. 25 del RGPD relativo a la privacidad desde el diseño determina que, *"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados"* (el subrayado es nuestro)

Reiteramos que hay múltiples medidas técnicas u organizativas que no son de seguridad y que puede implementar el responsable del tratamiento como cauce para garantizar este principio.

Sin embargo, el art. 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo, tan sólo de seguridad.

Entrando ya de lleno en el examen del non bis in idem, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que *"(…) Conforme a la legislación y jurisprudencia expuesta, el principio non bis in ídem impide sancionar dos veces al mismo sujeto por el mismo hecho con apoyo en el mismo fundamento, entendido este último, como mismo interés jurídico protegido por las normas sancionadoras en cuestión. En efecto, cuando exista la triple identidad de sujeto, hecho y fundamento, la suma de sanciones crea una sanción ajena al juicio de proporcionalidad realizado por el legislador y materializa la imposición de una sanción no prevista legalmente que también viola el principio de proporcionalidad.*

Pero para que pueda hablarse de "bis in ídem" debe concurrir una triple identidad entre los términos comparados: objetiva (mismos hechos), subjetiva (contra los mismos sujetos) y causal (por el mismo fundamento o razón de castigar):

a) La identidad subjetiva supone que el sujeto afectado debe ser el mismo, cualquiera que sea la naturaleza o autoridad judicial o administrativa que enjuicie y con independencia de quién sea el acusador u órgano concreto que haya resuelto, o que se enjuicie en solitario o en concurrencia con otros afectados.

b) La identidad fáctica supone que los hechos enjuiciados sean los mismos, y descarta los supuestos de concurso real de infracciones en que no se está ante un mismo hecho antijurídico sino ante varios.

c) La identidad de fundamento o causal, implica que las medidas sancionadoras no pueden concurrir si responden a una misma naturaleza, es decir, si participan de una misma fundamentación teleológica, lo que ocurre entre las penales y las

administrativas sancionadoras, pero no entre las punitivas y las meramente coercitivas."

Tomando como referencia lo anteriormente expuesto, no se ha vulnerado el principio non bis in idem, puesto que, si bien entendido grosso modo los hechos se detectan como consecuencia de la ausencia y deficiencia de las medidas de seguridad (solo de seguridad), que suponen una infracción del artículo 32 del RGPD, a su vez, tanto de los hechos como de la documentación aportada por el BBVA se ha constatado el incumplimiento del artículo 25 del RGPD en el diseño y la integración de la protección de datos en el sistema de detección del fraude de la organización.

Respecto de la aplicación de idénticos agravantes en ambas infracciones, hemos de significar que las circunstancias previstas en el art. 83.2 del RGPD y las dispuestas en el art. 76.2 de la LOPDGDD son las únicas que se pueden aplicar por la AEPD para cualquier infracción.

Por último, en el artículo 73, "*Infracciones consideradas graves*", de la LOPDGDD se constata la diferencia de las conductas infractoras, cuando a los efectos de prescripción, "*la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679*" se recoge en el apartado d) del citado artículo, mientras que en su apartado f) se estipula *"la falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".*

2. Subsidiariamente, existencia de concurso medial entre las dos conductas imputadas a BBVA objeto de las presentes alegaciones

Según BBVA, *"…no cabría duda de que el Acuerdo de Inicio identifica (y pretende sancionar) una pluralidad de infracciones que, supuestamente, habría cometido mi mandante (lo que nuevamente se niega de plano) cuando, en realidad, una de ellas se encontraría subsumida y embebida en la otra, dando lugar un concurso medial en los términos previstos en el artículo 29.5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público…"*

En respuesta a esta alegación, cabe señalar, en primer lugar, que en este punto vuelve a confundir la reclamada la tipificación de las infracciones con la calificación de estas a los solos efectos de la prescripción. Ambas infracciones están tipificadas en el art. 83.5 del RGPD, no hay una supuestamente más grave y otra supuestamente más leve.

Segundo, que el artículo 29 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) no resulta de aplicación al régimen sancionador impuesto por el RGPD por los siguientes motivos:

1. El RGPD es un sistema cerrado y completo.

El RGPD es una norma comunitaria 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 DDFF 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 (art. 83.2 del RGDP) o que especifica la regla existente relativa a un posible concurso medial (art. 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 art. 83.7 del RGPD). La LOPDGDD sólo desarrolla o concreta algunos aspectos del RGPD en lo que este 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".* (el subrayado es nuestro)

Sigue indicando 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". (el subrayado es nuestro)

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 art. 83 del RGPD muestran la prevalencia de medidas correctivas frente a las multas.

Así, el art. 83.2 del RGPD dice 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 art. 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 art. 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-, 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, 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.

2. Al no haber laguna legal, no hay aplicación supletoria del art. 29 del LRJSP.

Amén de lo expuesto, 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 art. 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 art. 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.

El artículo 29.5 de la LRJSP 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*".

Pues bien, el concurso medial tiene lugar cuando en un caso concreto la comisión de una infracción es un medio necesario para cometer otra distinta. Los hechos constados determinan la comisión de dos infracciones distintas, sin que la conculcación del artículo 32 del RGPD, tal y como asevera BBVA, sea el medio necesario por el que se produce la infracción del artículo 25 del RGPD (protección desde el diseño y por defecto).

Por todo lo expuesto, se desestima la presente alegación.

"TERCERA. - SOBRE LA PRETENDIDA VULNERACIÓN POR BBVA DEL ARTÍCULO 32 DEL RGPD"

1. Sobre el contenido del Acuerdo de Inicio

El primer motivo de oposición del BBVA a la infracción del artículo 32 del RGPD es que "*yerra el Órgano Sancionador al interpretar el alcance del documento aportado, ya que, sin perjuicio de que las medidas contenidas en el mismo, como se analizó, redundan favorablemente en la protección de los derechos de los clientes de BBVA, dicho documento no tiene por objeto establecer la Política de BBVA en relación con la adopción de medidas de seguridad exigidas por la normativa de protección de datos, siendo por el contrario una Guía de actuación interna utilizada en los casos en los que acontezcan situaciones respecto de las que pudieran existir indicios o evidencias de fraude. En este sentido, cabe reiterar lo ya indicado en cuanto al hecho de <u>que en ningún momento se ha requerido a mi mandante la aportación de los documentos acreditativos de las medidas de seguridad adoptadas en relación con el tratamiento de</u>*

los datos personales de sus clientes, como tampoco se le solicitó el análisis de riesgos referido a dichas actividades de tratamiento."(el subrayado nuestro)

Este documento fue aportado por BBVA el 23 de julio de 2022, en contestación al requerimiento de información formulado por esta Agencia, en el cual se le solicitaba, entre otra documentación, en su punto segundo, el "*Procedimiento establecido por la entidad para evitar suplantaciones de identidad cuando una persona comunica haber perdido el control de sus posesiones (documento de identidad, teléfono móvil, tarjetas bancarias)*". Por lo tanto, no puede afirmarse, como hace BBVA, que no se le solicitasen las medidas de seguridad relativas, al menos en ese punto, en materia de suplantación. Posteriormente, como consta en el Antecedente Décimo, el instructor del procedimiento requirió diversa documentación a BBVA relativas a medidas técnicas y organizativas para evitar el fraude por suplantación en las operaciones a través de "*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*", cuando se ha producido la sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, y esta circunstancia ha sido comunicada por el cliente, así como las medidas técnicas y organizativas que el BBVA tenía implantadas con fecha 14/04/2020, para que las comunicaciones realizadas a la entidad por sus clientes por la pérdida, extravío o sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, produzcan efecto en sus diversos canales de relación con el cliente relativos la operativa que este pueda realizar, sin que se haya tenido respuesta por parte de BBVA.

El segundo motivo de oposición a la infracción del artículo 32 del RGPD es que, según BBVA "*no puede imputársele el acceso a unos dispositivos en los supuestos en los que una determinada persona accede a este servicio habiendo verificado su identidad mediante el procedimiento de autenticación reforzada previsto en la vigente legislación de servicios de pago PSD2 y mediante el uso de las credenciales de la Reclamante."*

Es responsabilidad de BBVA que las constantes comunicaciones que se recogen en los Hechos Probados, de la parte reclamante a BBVA poniendo en conocimiento a través de los diversos canales de relación con el cliente (por correo electrónico remitido al director de la oficina y escrito remitido al servicio de atención al cliente), la sustracción sufrida y las diversas operaciones fraudulentes realizadas por terceras personas no autorizadas no impidieran que, de forma reiterada, se siguieran realizando operaciones ilegales con los datos personales de sus clientes, lo que pone de manifiesto la ausencia de medidas de seguridad implementadas que eviten que, comunicada por un cliente la sustracción de información, impidan que se sigan haciendo tratamientos ilegales de sus datos personales, como un procedimiento de autenticación de los usuarios para estos supuestos.

Afirma BBVA que "*la AEPD yerra al considerar que la vigente normativa de Protección de Datos impone, en lo que respecta a la adopción de medidas de seguridad, una obligación de resultado, entendiendo esta parte que el evidente espíritu del legislador, al establecer el Principio de Responsabilidad Proactiva, es promulgar una obligación de medios."* En el presente caso, tal y como se ha señalado anteriormente, BBVA ni siquiera ha probado que existan los medios, pese a la documentación que se le requirió tanto en el requerimiento de información y en la apertura del período de

prueba a los que nos hemos referido en la contestación al primer apartado de esta alegación.

Por último, BBVA considera que resulta contradictorio que en el acuerdo de inicio se diga que "*no dispone de medidas de seguridad y que las medidas de que dispone son insuficientes por estar desactualizadas, cuando evidentemente ambas afirmaciones son, a juicio de esta parte, contradictorias*". De la documentación aportada por BBVA se constata la existencia de diversas medidas, adoptadas generalmente en aplicación de normativa distinta del RGPD (RDL de servicios de pago y Reglamento Delegado), pero no se ha probado la existencia de medidas de seguridad tal y como exige el artículo 32 del RGPD. Además, estas medidas, tal y como se ha reflejado en el análisis de los documentos aportados BBVA, están desactualizadas (anteriores al RGPD) y no prevén medidas que garanticen la seguridad de los datos en casos de riesgo de fraude y suplantación, por lo que no prueban la existencia de verdaderas medidas de seguridad. Lo que sí resulta contradictorio es que BBVA afirma que no ha aportado medidas de seguridad porque no les han sido requeridas ("*en ningún momento se ha requerido a mi mandante la aportación de los documentos acreditativos de las medidas de seguridad adoptadas en relación con el tratamiento de los datos personales de sus clientes*"), pero, a su vez, quiere dar por acreditadas tales medidas de seguridad.

2. Sobre las medidas de seguridad aplicadas por BBVA durante los procesos de contratación financiera a través de la banca on-line

Sobre la existencia de medidas de seguridad en procesos de contratación en banca online, BBVA alega que "*debe hacerse referencia a los Documentos 1 a 8 aportados junto al presente escrito, de los que se desprende que mi representada ha proveído las directrices a seguir por las distintas áreas de negocio para la implementación de medidas de seguridad sobre los Sistemas de Información propiedad de BBVA*". Se trata de documentación de diverso contenido, con la que se pretende justificar la existencia de medidas de seguridad, pero sin precisar en qué punto estas medidas de seguridad están relacionadas con los hechos objeto del presente procedimiento, y garantizan un nivel de seguridad adecuado al riesgo en cuestión.

En este punto, en ninguno de los documentos aportados por BBVA se detallan las concretas medidas de seguridad que la entidad bancaria tuviera implantadas en previsión del riesgo de extravío o sustracción de documentación identificativa o de dispositivos que permitieran el acceso a la banca online o a distancia.

Seguidamente BBVA recoge una serie de webs donde se aporta información a sus clientes sobre la seguridad en el uso de la banca online y las tarjetas de crédito.

BBVA considera que "*el acceso por el cliente a la banca on-line de BBVA exige la utilización de un primer factor de autenticación cuya custodia y control no le corresponde, recayendo sobre el cliente*". Cabe plantear entonces qué tipo de solución aporta BBVA al cliente en caso de que un tercero tenga acceso al primer factor de autenticación, cuando es evidente que esto se ha producido, y el cliente avisa a BBVA con carácter previo que ha perdido el control sobre sus datos personales. En este procedimiento ha quedado acreditado que BBVA no dispone de ninguna medida de seguridad de gestión de contraseñas, de autenticación o de otro tipo en supuestos de

alto riesgo de fraude, para la protección de los usuarios y evitar, entre otros, el uso recurrente del primer factor de autenticación por parte de persona distinta del titular.

No se trata, como dice BBVA de la "*imposición a mi mandante de una responsabilidad de la que carece, pues en modo alguno puede estar bajo su control la evitación de que las credenciales de todos sus usuarios de banca on-line puedan serles sustraídas a sus clientes por terceros*". Como se ha dicho, la responsabilidad recae desde el momento en que, BBVA carece de medida de seguridad alguna de gestión de contraseñas, autenticación de los usuarios, de bloqueo o de algún otro tipo, para evitar accesos no autorizados en supuestos de pérdida o robo de datos que pueden ser utilizados para cometer un fraude, ni siquiera para evitar que el fraude continúe cometiéndose, una vez que la pérdida o robo les ha sido comunicada.

Por todo lo expuesto, se desestima la presente alegación.

"*CUARTA. - SOBRE LA VULNERACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD EN DETRIMENTO DE LOS DERECHOS DE BBVA"*

La proporcionalidad de las sanciones propuestas ha quedado fundamentada en el acuerdo de inicio, habiéndose tenido en cuenta todas las circunstancias concurrentes para graduar dichas sanciones, del mismo modo que se ha motivado la responsabilidad de BBVA en los hechos constitutivos de las infracciones. Que la incoación del presente procedimiento tenga como origen una sola reclamación y que afecte a dos personas, no es óbice para que entender que los hechos son de menor gravedad.

Según el artículo 83.4 del RGPD, en el caso de las empresas, las infracciones se sancionarán con una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, por lo que la cuantía de las sanciones propuestas queda muy lejos del importe máximo que permite dicho artículo.

A diferencia de lo expresado por BBVA de que la causa de la tramitación del presente procedimiento se trata de "*un hecho puntual, ajeno al control de BBVA, cual es la sustracción de las pertenencias de la reclamante*", la no aplicación del PDDD en el tratamiento de los datos personales de los clientes en situaciones como la ocurrida en este caso, así como la ausencia de medidas de seguridad, suponen una vulnerabilidad para todos los clientes del BBVA, en una situación tan cotidiana como pueda ser la sustracción de la documentación de identidad y del teléfono móvil.

Los agravantes aplicados a las infracciones responden a las circunstancias recogidas en el RGPD y en la LOPDGDD a efectos de graduar la sanción, según los criterios, no ya de esta Agencia, sino los expresados por el Comité Europeo de Protección de Datos en las Directrices 04/2022 sobre el cálculo de las multas bajo el RGPD, adoptadas el 24 de mayo de 2023, y por los Tribunales de Justicia.

La proporcionalidad de las sanciones que se proponen ha quedado motivada tanto en el Acuerdo de Inicio y en la presente propuesta de resolución.

Por todo lo expuesto, se desestima la presente alegación.

IV
Artículo 25.1 RGPD
Principio de protección de datos desde el diseño

El artículo 25.1 del RGPD establece lo siguiente:

"Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."

En consonancia con estas previsiones, el considerando 78 del RGPD dispone:

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

En concreto, a la luz del considerando 78 del RGPD, el principio de protección de datos desde el diseño es la clave a seguir por el responsable del tratamiento para demostrar el cumplimiento con el RGPD, ya que *«el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto».*

El principio de privacidad desde el diseño es una muestra del paso de la reactividad a

la proactividad y manifestación directa del enfoque de riesgos que impone el RGPD. Parte de la responsabilidad proactiva, impone que, desde los estadios más iniciales de planificación de un tratamiento debe de ser considerado este principio: el responsable del tratamiento desde el momento en que se diseña y planifica un eventual tratamiento de datos personales deberá determinar todos los elementos que conforman el tratamiento, a los efectos de aplicar de forma efectiva los principios de protección de datos, integrando las garantías necesarias en el tratamiento con la finalidad última de, cumpliendo con las previsiones del RGPD, proteger los derechos de los interesados.

Así, y respecto de los riesgos que pueden estar presentes en el tratamiento, el responsable del tratamiento llevará a cabo un ejercicio de análisis y detección de los riesgos durante todo el ciclo de tratamiento de los datos, con la finalidad primera y última de proteger los derechos y libertades de los interesados, y no sólo cuando efectivamente se produce el tratamiento. Así se expresa en las Directrices 4/2019 del CEPD relativas al artículo 25 Protección de datos desde el diseño y por defecto, adoptadas el 20 de octubre de 2020.

En las citadas Directrices se indica al respecto que:

> *"35. El «momento de determinar los medios de tratamiento» hace referencia al período de tiempo en que el responsable está decidiendo de qué forma llevará a cabo el tratamiento y cómo se producirá este, así como los mecanismos que se utilizarán para llevar a cabo dicho tratamiento. En el proceso de adopción de tales decisiones, el responsable del tratamiento debe evaluar las medidas y garantías adecuadas para aplicar de forma efectiva los principios y derechos de los interesados en el tratamiento, y tener en cuenta elementos como los riesgos, el estado de la técnica y el coste de aplicación, así como la naturaleza, el ámbito, el contexto y los fines. Esto incluye el momento de la adquisición y la implementación del software y hardware y los servicios de tratamiento de datos.*
>
> *36. Tomar en consideración la PDDD desde un principio es crucial para la correcta aplicación de los principios y para la protección de los derechos de los interesados. Además, desde el punto de vista de la rentabilidad, también interesa a los responsables del tratamiento tomar la PDDD en consideración cuanto antes, ya que más tarde podría resultar difícil y costoso introducir cambios en planes ya formulados y operaciones de tratamiento ya diseñadas".*

Para ello debe recurrir al diseñar el tratamiento a los principios recogidos en el artículo 5 del RGPD, que servirán para aquilatar el efectivo cumplimiento del RGPD. Así, las citadas Directrices 4/2019 del CEPD disponen que *"61. Para hacer efectiva la PDDD, los responsables del tratamiento han de aplicar los principios de transparencia, licitud, lealtad, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, y responsabilidad proactiva. Estos principios están recogidos en el artículo 5 y el considerando 39 del RGPD".*

La Guía de Privacidad desde el Diseño de la AEPD afirma que *"La privacidad desde el diseño (en adelante, PbD) implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso). Por ciclo de vida*

del objeto se entiende todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada".

La Guía dispone que *"La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña (…) La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento y debe garantizarse a lo largo de todo el ciclo de vida de los datos".*

Por ello, la privacidad desde el diseño, obligación del responsable del tratamiento que nace antes de que el sistema esté en funcionamiento, no son parches que se van asentando sobre un sistema construido de espaldas al RGPD. Ligado a la edificación de una verdadera cultura de protección de datos en la organización, implica también por mor de la responsabilidad proactiva la capacidad de documentar todas las decisiones que se adopten con un enfoque "privacy design thinking", demostrando el cumplimiento del RGPD también en este aspecto.

El enfoque de riesgos hace referencia directa e inmediata a un sistema preventivo tendente a visualizar, respecto de un tratamiento de datos personales, los riesgos en los derechos y libertades de las personas físicas. Ha de excluirse, por tanto, del enfoque de riesgos de protección de datos otra serie de riesgos a los que puede encontrarse sometida la organización y que afecten a su ámbito de negocio.

En relación con los riesgos en los derechos y libertades de las personas físicas, han de identificarse los riesgos, evaluar su impacto y valorar la probabilidad de que aquellos se materialicen. Se protegen pues, no los datos, sino a las personas que están detrás de ellos.

Los riesgos para los derechos y libertades de las personas físicas, derivados del tratamiento de datos personales, pueden ser de gravedad y probabilidad variables y provocar daños y perjuicios físicos, materiales o inmateriales, consecuencias tangibles o intangibles, en los derechos y las libertades de las personas físicas. El considerando 75 del RGPD y el artículo 28.2 de la LOPDGDD recopilan ejemplificativamente algunos de los considerados por el legislador, mas no son los únicos. Dependerá del tratamiento y el contexto en el que este se realiza, de los datos personales tratados, de las personas involucradas, de los medios utilizados, etc.

A este respecto, la parte reclamada ha aportado, para la gestión de incidentes como el que se refiere este expediente, un documento denominado "Prevención del fraude y de la estafa". Dicho documento lleva fecha de 01/06/2015, con lo que claramente fue elaborado antes de la aprobación del RGPD. Y ya hemos comentado que el principio de privacidad desde el diseño es una muestra del paso de la reactividad a la proactividad y es un reflejo del enfoque de riesgos que impone el RGPD. Ello aparte de la desactualización del documento frente a un entorno de continua sofisticación de los mecanismos de fraude, como reconoce el propio documento en su apartado de "Consideraciones generales":

"Esta eficacia está condicionada por un hecho innegable: el mundo del fraude está en continuo cambio y los procedimientos son perfeccionados por los delincuentes constantemente, por lo que habrá que actualizar la información de forma permanente."

Examinado el documento, se observa que tienen un enfoque eminentemente empresarial o de "negocio". Su finalidad es tratar de evitar prácticas fraudulentas de las que se derive un perjuicio para la entidad. Con ello indirectamente se podrá evitar un perjuicio patrimonial para el usuario, pero no se protege su Derecho Fundamental a la Protección de Datos Personales, no se protegen sus derechos y libertades, que es la finalidad última que persigue el RGPD a través de la protección de datos desde el diseño. No se trata, por lo tanto, de un documento concebido para el cumplimiento del principio de responsabilidad proactiva (artículo 5.2 RGPD), ya que para ello debería haberse partido del mencionado análisis de riesgos que llevara a la adopción de medidas para la protección de los derechos y libertades, a partir siempre del diseño del tratamiento. Desde esta óptica, en la ya mencionada Guía de Privacidad desde el diseño de la AEPD se establecen diversas orientaciones, que no se cumplen en el supuesto que nos ocupa:

"Cualquier sistema, proceso o infraestructura que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños. Una política de PbD se caracteriza por la adopción de medidas proactivas que se anticipan a las amenazas, identificando las debilidades de los sistemas para neutralizar o minimizar los riesgos en lugar de aplicar medidas correctivas para resolver los incidentes de seguridad una vez sucedidos. Es decir, la PbD huye de la "política de subsanar" y se adelanta a la materialización del evento de riesgo".

La privacidad como configuración predeterminada:

"La PbD persigue proporcionar al usuario el máximo nivel de privacidad dado el estado del arte y, en particular, que los datos personales estén automáticamente protegidos en cualquier sistema, aplicación, producto o servicio. La configuración por defecto deberá quedar establecida desde el diseño a aquel nivel que resulte lo más respetuoso posible en términos de privacidad. En el caso de que el sujeto no tome ninguna acción de configuración, su privacidad debe estar garantizada y mantenerse intacta, pues está integrada en el sistema y configurada por defecto.

Privacidad incorporada en la fase de diseño:

"*La privacidad debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña. Para garantizar que la privacidad se tiene en cuenta desde las primeras etapas del diseño se debe:*
• Considerar como un requisito necesario en el ciclo de vida de sistemas y servicios, así como en el diseño de los procesos de la organización.
• Ejecutar un análisis de los riesgos para los derechos y libertades de las personas y, en su caso, evaluaciones de impacto relativas a la protección de datos, como parte

integral del diseño de cualquier nueva iniciativa de tratamiento.
• Documentar todas las decisiones que se adopten en el seno de la organización con un enfoque "privacy design thinking".

Respeto por la privacidad de los usuarios, manteniendo un enfoque centrado en el usuario:

"Sin obviar los intereses legítimos que persigue la organización con el tratamiento de datos que realiza, el fin último debe ser garantizar los derechos y libertades de los usuarios cuyos datos son objeto de tratamiento, por lo que cualquier medida adoptada debe ir encaminada a garantizar su privacidad. Ello supone diseñar procesos, aplicaciones, productos y servicios "con el usuario en mente", anticipándose a sus necesidades. El usuario debe tener un papel activo en la gestión de sus propios datos y en el control de la gestión que otros hagan con ellos. Su inacción no debe suponer un menoscabo a la privacidad, retomando uno de los principios ya mencionados y que propugna una configuración de privacidad por defecto que ofrezca el máximo nivel de protección".

Así, los procedimientos de contratación de productos bancarios de la parte reclamada requieren, en materia de protección de datos, de un correcto análisis de los riesgos en los derechos y libertades de los clientes, de una adecuada planificación, del establecimiento de medidas de seguridad evitativas de los riesgos, de un mantenimiento, actualización y control de aquellas desde la revisión continua de los riesgos, incluyendo la demostración del cumplimiento (observancia del principio de responsabilidad proactiva), especialmente, en el caso que nos atañe, en relación con las medidas de seguridad apropiadas. Y ello con el objeto de que se garantice el Derecho Fundamental a la Protección de Datos de los clientes, que incluye la efectiva disposición de los datos personales por los interesados, así como garantizar la seguridad de los datos personales de los clientes de manera efectiva y en particular, su custodia, para evitar la contratación no autorizada de productos y servicios de sus titulares. El cumplimiento de esta obligación impuesta por el RGPD al responsable del tratamiento se logra a través de la privacidad desde el diseño.

En este procedimiento se han llevado a cabo actuaciones previas de investigación para analizar la reclamación presentada ante la Agencia como consecuencia de un robo y como consecuencia de ello se ha analizado el procedimiento que BBVA tiene establecido para las contrataciones de productos financieros y las garantías que en esos procedimientos se establecen para evitar supuestos como el producido Así, examinado el procedimiento establecido por la entidad bancaria respecto a la gestión de incidentes en relación con el fraude, se observa que está totalmente desactualizado, no adaptado al RGPD y no enfocado en los riesgos para los derechos y libertades de los clientes, ni para su protección, lo que muestra que no se ha cumplido con la obligación dispuesta en el artículo 25 del RGPD en relación con el diseño y la integración de la protección de datos en el sistema de detección del fraude de la organización.

De la documentación aportada por BBVA en la instrucción de este procedimiento se constata la inobservancia de la obligación impuesta por el artículo 25 del RGPD, sin que las medidas adoptadas por esta entidad para el cumplimiento de otra normativa (RDL de servicios de pago y el Reglamento Delegado) puedan suplir lo dispuesto en

el artículo 25 del RGPD, que exhorta a la protección de los derechos y libertades de los ciudadanos en el tratamiento de sus datos, no a la mera gestión de la información o a la efectividad de medios de pago.

En efecto, analizada toda la documentación aportada, en las distintas fases de este procedimiento, por BBVA, se observa que esta entidad no cumplía con el principio de privacidad desde el diseño. En primer lugar, no existía un análisis de riesgos adecuado. Ni uno solo de los documentos aportados abordaba el riesgo de que cuando un cliente pierde, o le es sustraída, determinada documentación identificativa, (o los métodos o dispositivos para el acceso a su banca online) quedan al descubierto los datos personales que permiten la contratación a distancia de productos financieros.

Los documentos aportados no contienen ningún análisis de este riesgo y, con ello, no arbitraban medidas técnicas u organizativas que podrían evitar la lesión del derecho fundamental a la protección de datos, y junto a él, los bienes y derechos patrimoniales de que son titulares los clientes de la entidad bancaria. Por el contrario, estos documentos se centran en la evitación de riesgos esencialmente para la propia entidad. Abordan riesgos tecnológicos o de negocio que pueden concluir en un perjuicio patrimonial para el banco.

A este respecto, debe recordarse que conforme al artículo 25 del RGPD:

"Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados."

Es decir, la protección del derecho fundamental a la protección de datos no consiste en una mera espera "reactiva" a que pueda producirse un problema que lo lesione, sino que los responsables del tratamiento deben diseñar ("protección de datos desde el diseño") con carácter previo al inicio del tratamiento, las políticas adecuadas para la protección de dicho derecho fundamental. Y ello incluye todos los aspectos regulados en el RGPD, comenzando por las obligaciones de transparencia, el respeto al ejercicio de los derechos establecidos en el Reglamento, y el establecimiento de todas medidas técnicas y organizativas necesarias para garantizar el cumplimiento de dicha norma. Y todo ello debe estar planificado e implementado con carácter previo al inicio del tratamiento por el responsable.

Derivado de las actuaciones de inspección llevadas a cabo por esta Agencia, así como del resto de documentación y alegaciones presentadas por BBVA en este procedimiento, ha podido constatarse que dicho principio (y en consecuencia el artículo 25 del RGPD) no se cumplían por la entidad bancaria. No existía un análisis de riesgo que hubiera identificado el riesgo de contrataciones mediante suplantación cuando algún cliente extraviara y le fuera sustraída su documentación identificativa o su teléfono móvil.

A este respecto, el análisis de riesgo es una pieza clave del principio de privacidad desde el diseño, ya que es lo que permite el establecimiento de medidas técnicas y organizativas que los eviten o, en caso de producirse, los palíen. Como se ha señalado, el artículo 25 hace especial referencia a "los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas", como presupuesto para el establecimiento de dichas medidas.

Se ha comprobado que ni el riesgo estaba establecido ni con ello las medidas implantadas. Y todo ello queda corroborado a través de la documentación del procedimiento facilitada por la reclamada. En efecto, como ha quedado ampliamente narrado en los hechos probados de esta propuesta, desde el 14 de abril de 2020, y en reiteradas ocasiones, se había notificado a BBVA la sustracción del teléfono móvil número ***TELÉFONO.1** y la documentación identificativa de la parte reclamante. Sin embargo, BBVA mantuvo este dato personal de la parte reclamante como medio a través del cual se producía la autenticación de la identidad de la parte reclamante.

En este momento procedimental de propuesta de resolución de procedimiento sancionador, existen evidencias de que se ha vulnerado el principio de protección de datos desde el diseño (artículo 25 del RGPD) en relación con el sistema de gestión del fraude de la parte reclamada.

V

Tipificación y calificación de la posible infracción del artículo 25 RGPD

De confirmarse, la citada infracción del artículo 25 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"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; (…)"*

La LOPDGD, a efectos de la prescripción de la infracción, califica en su artículo 73.d) de infracción grave, siendo en este caso el plazo de prescripción de dos años, *"d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679."*

VI

Artículo 32 del RGPD
Falta de medidas de seguridad

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"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".

Examinadas las medidas de seguridad que con carácter general contaba la parte reclamada para supuestos de fraude y suplantación de identidad, existen evidencias de que BBVA no disponía de un procedimiento de las medidas de seguridad para la protección de los datos personales apropiadas en función de los posibles riesgos estimados.

Y ello se pone de manifiesto en la documentación remitida por la entidad financiera, ya que las medidas de seguridad contenidas en el documento denominado "PREVENCIÓN DEL FRAUDE Y DE LA ESTAFA" y en la demás documentación

aportada por BBVA, no se ajustan ni al RGPD ni a su enfoque de riesgos ni a la protección de los datos personales, estando claramente desactualizadas. El procedimiento establecido a tales efectos resulta ser manifiestamente insuficiente.

Además, aún examinando los procedimientos fijados por la entidad respecto del establecimiento y aplicación de medidas de seguridad, hemos de significar que en el supuesto concreto reclamado, que fue el origen de la investigación, ni tan siquiera se aplicaron correctamente las que constaban en el documento denominado "Prevención del fraude y de la estafa" del BBVA; como se ha detallado en fundamentos anteriores, con fechas posteriores a la comunicación del robo del teléfono móvil y tarjetas, así como de posibles documentos identificativos, el 14/04/2020, la parte reclamada tramitó la contratación de distintos productos financieros, detallados más arriba. Incluso la parte reclamada contestó a ese correo reconociendo haber detectado diversos cargos a través de banca online que suponía no había realizado la parte reclamante. Y adjuntaba un listado de cargos para su revisión por esta. Sin embargo, no existe constancia de que la entidad financiera tuviera implementadas medidas que evitaran los accesos reiterados.

Según reconoce la parte reclamada, todos esos productos fueron contratados electrónicamente a través del canal *"BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA*". Ello a pesar de que el reclamado era conocedor del robo de efectos personales (teléfono móvil, monedero, etc.) que podían hacer que los defraudadores estuvieran en condiciones de acceder a la banca online de la parte reclamante, como así hicieron.

En la explicación aportada por la parte reclamada se limita a detallar cómo habría sido realizada la contratación, indicando que se habría utilizado el sistema de banca a distancia. Esto probablemente vino propiciado por el hecho de que, con la sustracción de sus efectos personales, los defraudadores habrían tenido acceso a documentos identificativos de la parte reclamante, y posiblemente a la aplicación de banca on line en su móvil.

Pero lo cierto es que la parte reclamada recibió una alerta, el 14/04/2020, del robo del teléfono móvil y otros posibles documentos, con lo que debió disponer de medidas de seguridad que garantizaran, ya no solo que no se utilizaran productos ya contratados, como la tarjeta de crédito, sino que no se contrataran nuevos productos que permitieran a los defraudadores disponer de los activos dinerarios de la parte reclamante, e incluso solicitar créditos.

En su contestación en fase de actuaciones previas de investigación, la parte reclamada se limita a aportar documentación que no está directamente relacionada con las medidas de seguridad que tendría implementadas para la protección de los usuarios en caso de fraude. Afirma lo siguiente:

> *"En el caso de que el cliente comunique el hurto o extravío de su documento identificativo, es obligatorio añadir esa información en el teleproceso (sistema que emplean los trabajadores de caja) mediante bloqueo en cuenta (de texto libre) incluyendo el mensaje "USO DE DNI ROBADO. BAJO NINGUNA EXCUSA LEVANTAR BLOQUEO. AVISAR OFICINA XXXX Y RETENER DNI" y, a decisión del cliente, si también desea que interpongamos el bloqueo 007 para cargos: "transferencias", puesto que éstas también se pueden realizar por ventanilla con*

su DNI. De manera que sirvan de alerta para la Red.

Asimismo asegurarse de que el móvil e email son los validados y correctos del cliente, que no hayan sido modificados. Si no fuese así, por seguridad deberá cambiar sus claves de NET.

Se recomienda que el bloqueo permanezca, al menos, hasta que el documento robado/extraviado, deje de estar vigente. No obstante, siempre y cuando no afecte a la operativa del cliente se recomienda mantenerlo de forma indefinida. Es conveniente recoger la instrucción del cliente comunicando la pérdida de la documentación, así como la solicitud de bloqueo y/o desbloqueo de la cuenta.

NORMA INTERNA 94.30.005 se acompaña Documento nº 3."

Consultándose el mencionado documento 3, si bien contiene algunos apartados referidos a prácticas fraudulentas similares a las enjuiciadas en este expediente ("Cómo identificar" o "Suplantación de identidad"), no contiene ninguna previsión específica de las posibles alertas que deben saltar en la entidad cuando tiene noticia de determinados acontecimientos que ponen en riesgo los derechos y libertades de los ciudadanos. Particularmente, la pérdida o robo de documentación que posibilite la contratación de productos financieros. En ese caso, por muy adecuado que sea el proceso de autenticación de la identidad a distancia, está claro que el defraudador podrá superarlo por estar en posesión de la documentación o dispositivos electrónicos como el teléfono móvil, y para este caso la entidad financiera no dispone de ninguna medida que garantice la autenticidad del usuario.

En base a lo anteriormente expuesto, y tras la investigación llevada a cabo por esta Agencia, y el análisis de la documentación aportada por BBVA a este procedimiento sancionador, queda en entredicho el procedimiento establecido por BBVA para identificar a las personas que pueden solicitar la contratación de productos bancarios en supuestos en los que el cliente comunique el acceso ilegal por terceros a sus datos. Asimismo, la parte reclamada tampoco habría implementado medidas de seguridad adecuadas en relación con la sustracción de la documentación identificativa.

Con ello, ni de la documentación o información aportadas por el reclamado, ni mucho menos de los resultados producidos en este caso puede deducirse que BBVA dispusiera de un procedimiento adecuado referido a la implementación y aplicación de medidas de seguridad de datos personales apropiadas, técnicas u organizativas, para evitar que se realicen contrataciones online en nombre del titular de los datos,
De conformidad con las evidencias de las que se dispone en este momento de propuesta de resolución, se estima que la conducta de la parte reclamada podría vulnerar el artículo 32 del RGPD en relación con los procedimientos de seguridad de datos personales en los dos tratamientos referenciados, tanto en la contratación de productos financieros.

VII
Tipificación y calificación de la posible infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"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; (…)"*

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica"*.

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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:

(…)

> *f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.*

VIII
Criterios de graduación de la cuantía

- Por la infracción del artículo 25. (principio de protección de datos desde el diseño):

Confirme al artículo 83.4 del RGPD *"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.*

Se tienen en cuenta las siguientes circunstancias como agravantes:

- La naturaleza, gravedad o 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.

A este respecto debe señalarse que la carencia de un diseño adecuado de los tratamientos de datos personales afecta a tratamientos de datos personales relativos a la contratación de productos financieros, que pueden verse afectados por diversos riesgos de importante gravedad, como por ejemplo el fraude y la suplantación de identidad, lo que conlleva, no sólo la pérdida de disposición de los datos personales por el interesado, sino también riesgo de sufrir eventuales daños de carácter patrimonial.

La infracción se prolonga en el tiempo, porque al menos desde la entrada en vigor del RGPD no se ha aplicado al tratamiento referenciado el principio de protección de datos desde el diseño.

Asimismo, se ha de considerar para la determinación de la sanción el número de interesados potencialmente afectados, mucho más cuando lo examinado en este caso es el procedimiento de gestión del fraude implantado por la entidad bancaria que afecta a todos los clientes del BBVA y la falta de cumplimiento del principio de protección de datos desde el diseño.

En este sentido las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en su versión de 12 de mayo de 2022, sometidas a consulta pública, señalan *"como una de las circunstancias a valorar en la graduación de la sanción: "El número de interesados concretamente, pero también potencialmente afectados", y, aclara con relación a ese criterio: "Cuanto más alto es el número de interesados implicados, mayor ponderación podrá tener la autoridad de control atributo a este factor. En muchos casos también puede considerarse que la infracción asume connotaciones «sistemáticas» y, por lo tanto, puede afectar, incluso en diferentes momentos, sujetos de datos adicionales que no han presentado quejas o informes a la autoridad supervisora. La autoridad de control podrá, en función de las circunstancias del caso, considere la relación entre el número de interesados afectados y el número total de interesados en ese contexto (por ejemplo, el número de ciudadanos, clientes o empleados) con el fin de evaluar si la infracción es de carácter sistémico".* (artículo 83.2.a) RGPD)

- La negligencia grave en la infracción. Debe tenerse en cuenta que el cumplimiento del principio de protección de datos desde el diseño es especialmente importante en una entidad financiera, cuyos tratamientos de datos personales derivados del continuo tráfico jurídico mercantil, entraña múltiples riesgos en los derechos y libertades de las personas físicas, como pueden ser el de suplantación de identidad o el riesgo evidente de una pérdida patrimonial para el cliente que sufre las consecuencias.

  En este mismo sentido, 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 BBVA 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. [Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006). Artículo 83.2.d) RGPD)

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (art. 76.2.b) LOPDGDD) al tratarse de una entidad financiera que basa su negocio en la utilización de los datos personales de sus clientes.

- Por la infracción del artículo 32 RGPD

Conforme al artículo 83.4 RGPD: *"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:"*

Se tienen en cuenta las siguientes circunstancias como agravantes para cada una de dos infracciones del artículo 32 del RGPD:

- La naturaleza, gravedad o 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.

  A este respecto debe señalarse que la falta de un procedimiento implantado que garantice la seguridad de los datos personales adecuado al riesgo afecta a tratamientos de datos personales relativos a la contratación de productos financieros, que pueden verse afectados por diversos riesgos de importante gravedad, como por ejemplo el fraude y la suplantación de identidad, lo que conlleva, no sólo la pérdida de disposición de los datos personales por el interesado, sino también riesgo de sufrir eventuales daños de carácter patrimonial. De igual forma la infracción afecta a la falta de medidas de seguridad apropiadas en relación con la comunicación indebida de una deuda controvertida a los sistemas de información crediticia, con la aparición de diversos riesgos tales como eventuales daños de carácter patrimonial o reputacionales.

  Asimismo, se ha de considerar para la determinación de la sanción el número de interesados potencialmente afectados, mucho más cuando lo examinado en este caso es el procedimiento de gestión del fraude implantado por la entidad bancaria o el procedimiento de comunicación de deudas a sistemas de información crediticia en relación con las medidas de seguridad apropiadas y que afecta a todos los clientes del BBVA.

  En este sentido las Directrices 04/2022 del Comité Europeo de Protección de Datos sobre el cálculo de las multas administrativas con arreglo al RGPD, en

su versión de 12 de mayo de 2022, sometidas a consulta pública, señalan *"como una de las circunstancias a valorar en la graduación de la sanción: "El número de interesados concretamente, pero también potencialmente afectados", y, aclara con relación a ese criterio: "Cuanto más alto es el número de interesados implicados, mayor ponderación podrá tener la autoridad de control atributo a este factor. En muchos casos también puede considerarse que la infracción asume connotaciones «sistemáticas» y, por lo tanto, puede afectar, incluso en diferentes momentos, sujetos de datos adicionales que no han presentado quejas o informes a la autoridad supervisora. La autoridad de control podrá, en función de las circunstancias del caso, considere la relación entre el número de interesados afectados y el número total de interesados en ese contexto (por ejemplo, el número de ciudadanos, clientes o empleados) con el fin de evaluar si la infracción es de carácter sistémico".* (artículo 83.2.a) RGPD)

- La negligencia grave en la infracción. Debe tenerse en cuenta que en el respeto al principio de responsabilidad proactiva y el establecimiento de medidas de seguridad apropiadas en atención a los riesgos en los derechos y libertades de las personas físicas detectados, es especialmente importante en una entidad financiera. Los tratamientos de datos personales derivados del continuo tráfico jurídico mercantil de una entidad financiera, entraña múltiples riesgos en los derechos y libertades de las personas físicas, como pueden ser el de suplantación de identidad o el riesgo evidente de una pérdida patrimonial para el cliente que sufre las consecuencias o la comunicación indebida de una deuda controvertida a los sistemas de información crediticia.

  En este mismo sentido, 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 BBVA 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. [Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006)]. Artículo 83.2.b) RGPD)

- Toda infracción anterior cometida por el responsable del tratamiento. Constan en esta Agencia dos expedientes sancionadores contra la parte reclamada por insuficiencia de medidas de seguridad apropiadas para garantizar los derechos y libertades de las personas físicas: PS/00419/2022 y PS/00429/2022. (Artículo 83.2.e) RGPD)

- La vinculación de la actividad del infractor con la realización de tratamientos de datos personales (art. 76.2.b) LOPDGDD)

IX
Propuestas de sanción

En función de los factores a tener en cuenta en la graduación de la cuantía de la sanción, conforme a lo detallado en los apartados anteriores, la posible sanción a imponer, sin perjuicio de lo que resulte de la instrucción de este expediente, serían las siguientes:

a) Por la infracción del artículo 25 del RGPD en relación con el principio de protección de datos desde el diseño y por defecto: QUINIENTOS MIL EUROS (500.000 €)

b) Por la infracción del artículo 32 del RGPD por falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros: QUINIENTOS MIL EUROS (500.000 €)

Lo que hace un total de UN MILLÓN de euros (1.000.000 €)

X
Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, cumpliendo con la protección de datos desde el diseño y por defecto en el sistema de detección del fraude de la organización, y la adopción de procedimientos de seguridad de datos personales tanto en la contratación de productos financieros, como en la inclusión y mantenimiento de los datos de los clientes en los sistemas de información crediticia, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

A este respecto, el reclamado deberá analizar los riesgos, así como establecer las medidas técnicas, organizativas y de seguridad necesarias para evitar que, en casos de sustracción o extravío de documentación identificativa o dispositivos de acceso a banca on line, puedan realizarse contratación de servicios bancarios y financieros sin consentimiento del titular de la documentación y dispositivos

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

A la vista de lo expuesto se procede a emitir la siguiente

PROPUESTA DE RESOLUCIÓN

Que por la Directora de la Agencia Española de Protección de Datos se sancione a BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF A48265169:

- Por una infracción del Artículo 25 del RGPD, tipificada en el Artículo 83.4 del RGPD, con una multa de 500.000 € (quinientos mil euros).

- Por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, con una multa de 500.000 € (quinientos mil euros).

Que por la Directora de la Agencia Española de Protección de Datos se declare la terminación del procedimiento por reconocimiento de responsabilidad y pago voluntario de BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF A48265169, respecto a las siguientes infracciones:

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del RGPD, con relación a la contratación no autorizada de productos.

- La infracción del artículo 32 del RGPD tipificada en el artículo 83.4 del mismo Reglamento, por la falta de medidas de seguridad con relación a los procedimientos de comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales,

- La infracción del artículo 6.1 del RGPD tipificada en el artículo 83.5 del mismo Reglamento, con relación a la incorporación de datos personales en los sistemas de información crediticia.

Asimismo, de conformidad con lo establecido en el artículo 85.2 de la LPACAP, se le informa de que podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá una reducción de un 20% del importe de la misma. Con la aplicación de esta reducción, la sanción quedaría establecida en ochocientos mil euros y su pago implicará la terminación del procedimiento. La efectividad de esta reducción estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de la cantidad especificada anteriormente, de acuerdo con lo previsto en el artículo 85.2 citado, deberá hacerla efectiva mediante su ingreso en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa, por pago voluntario, de reducción del importe de la sanción. Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para proceder a cerrar el expediente.

En su virtud se le notifica cuanto antecede, y se le pone de manifiesto el procedimiento a fin de que en el plazo de DIEZ DÍAS pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP.

926-170223

H.H.H.
INSTRUCTOR

Anexo

Índice del Expediente PS/00677/2022

SEXTO**:** Con fecha 27 de septiembre de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de BBVA en el que aduce alegaciones a la propuesta de resolución.

SÉPTIMO: En fecha 3 de octubre de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **800.000 euros,** haciendo uso de la reducción prevista en la propuesta de resolución parcialmente transcrita anteriormente.

OCTAVO: El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere la propuesta de resolución.

NOVENO: En la propuesta de resolución transcrita anteriormente se constataron los hechos constitutivos de infracción, y se propuso que, por la Directora, se impusiera al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".*

FUNDAMENTOS DE DERECHO

I
Competencia

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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:
"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, elórgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

III

Contestación a las alegaciones aducidas a la propuesta de resolución

Con relación a las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por BBVA:

"PRELIMINAR.- RATIFICACIÓN Y REITERACIÓN DEL CONTENIDO DEL ESCRITO DE ALEGACIONES AL ACUERDO DE INICIO"

Con carácter previo, desde BBVA se reitera en lo señalado en sus alegaciones al acuerdo de inicio, y considera que la contestación a sus alegaciones efectuada en el Fundamento de derecho III de la propuesta de resolución no da respuesta a lo alegado por BBVA, sino que supone una reiteración de lo argumentado por esta Agencia en el acuerdo de inicio.

En respuesta a estos argumentos cabe señalar que la propuesta de resolución no supone una reiteración del acuerdo de inicio, sino que en su Fundamento de Derecho

III se dio debida contestación a las alegaciones esgrimidas por BBVA en su escrito de alegaciones. En el Fundamento de Derecho III se sigue la estructura argumental del escrito presentado por BBVA. Además, con objeto de dar una respuesta pertinente a los razonamientos del escrito de alegaciones, se transcriben algunas partes de este, y, por último se lleva a cabo un análisis pormenorizado de los documentos aportados por BBVA junto al escrito de alegaciones.

En consecuencia, puede comprobarse fácilmente que la propuesta de resolución del presente procedimiento sí da debida respuesta a los argumentos aducidos por BBVA al acuerdo de inicio.

Por todo lo expuesto, se desestima la presente alegación.

"PRIMERA.- SOBRE EL ALCANCE DE LAS CUESTIONES DILUCIDADAS EN EL PRESENTE PROCEDIMIENTO SANCIONADOR

En esta alegación BBVA vuelve a atribuir a "*una serie de desafortunadas vicisitudes*" (un "*desafortunado incidente*" se dice el escrito de alegaciones al acuerdo de inicio), los hechos que motivaron la incoación del presente procedimiento. BBVA considera que, de una situación particular completamente desafortunada, y respecto de la que BBVA no ha tenido inconveniente alguno en asumir su responsabilidad, se extrae la consecuencia de que existe una vulneración "sistemática", convirtiendo así la resolución de un caso concreto en una suerte de "causa general" contra BBVA. Según la reclamada, había desarrollado actuaciones encaminadas al cumplimiento de la Protección de Datos desde el Diseño y por Defecto (en adelante, PDDD) y precisamente como consecuencia del análisis derivado del cumplimiento de ese principio, había implementado medidas adecuadas desde el punto de vista de la seguridad para impedir el riesgo, aun cuando, desafortunadamente, dichas medidas fallaron en el presente caso.

Dos son las cuestiones que se plantean en esta alegación formulada por la parte reclamada:

1. La AEPD está convirtiendo la resolución de un caso concreto en una suerte de "causa general" contra BBVA.

2. BBVA considera que ha desarrollado actuaciones encaminadas al cumplimiento de la protección de datos desde el diseño y por defecto, y precisamente como consecuencia del análisis derivado del cumplimiento de ese principio, había implementado medidas adecuadas desde el punto de vista de la seguridad para impedir el riesgo.

Vamos a examinarlas de manera diferencia.

<u>1. La AEPD no está convirtiendo la resolución de un caso concreto en una suerte de "causa general" contra BBVA.</u>

El artículo 57.1 del RGPD le confiere a la AEPD, entre otras funciones, las de controlar la aplicación del RGPD y hacerlo aplicar, así como tratar las reclamaciones

presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control y llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública.

El TJUE ya ha tenido oportunidad de establecer que el ámbito de los poderes de las autoridades de control ha de entenderse en un sentido amplio y que se extiende a cualesquiera circunstancias que se revelen tras la investigación a que se refiere el art. 57.1.f) RGPD tras la reclamación presentada por un interesado, si dicha investigación determina una insuficiencia de la protección del derecho del interesado a la protección de datos personales, "*con independencia del origen o la naturaleza de dicha insuficiencia"*, sin limitarse al motivo originario de la reclamación a los efectos de no dejar desprotegidos a los interesados. Por todas, STJUE de 16 de julio de 2020, C-311/18, Data Protection Commissioner Schrems 2.

Las investigaciones de la AEPD en relación con las reclamaciones presentadas pretenden siempre determinar de forma adecuada lo sucedido. Y ello porque no pueden quedarse en el sustrato superior de una eventual reclamación, sino que tiene que ahondar en el porqué de los hechos acontecidos y cuál es la causa última del incumplimiento, controlando así la aplicación del RGPD y haciéndolo aplicar. La causa última puede ser desde un error humano puntual hasta un inadecuado diseño de determinados tratamientos de datos personales.

Ni el RGPD ni la LOPDGDD determinan que la actuación de la autoridad de control quede restringida a la específica y concreta queja de los afectados. Y donde la Ley no distingue, no se puede distinguir.

Se desnaturalizaría, de contrario, el papel que en la defensa del derecho fundamental a la protección de los datos personales le confiere el RGPD a la AEPD si la información y los indicios que pudiera obtener a través de sus investigaciones, consecuencia de una reclamación -indicios que pudieran ser más que evidentes de la comisión de una infracción que afectara a más interesados que a los que efectivamente han reclamado (como podrían ser potencialmente los clientes de una entidad)- se obviaran so pretexto de que no responden estrictamente a los hechos referidos por el interesado. Es como si le obligaran a la AEPD a mirar para otro lado al detectar un eventual incumplimiento del RGPD porque el interesado no se ha quejado al respecto en su reclamación.

Esta interpretación impediría a cualquier autoridad de control europea, y por ende a la AEPD, que pudiera investigar o iniciar un procedimiento a los efectos, no sólo de imponer en su caso la multa que correspondiera, sino también o alternativamente a aquella de imponer medidas correctivas que restablecieran la legalidad vigente. De esta forma se podrían estar dejando desprotegidos a otros interesados que no fuera la parte reclamante, imposibilitando efectivamente a la AEPD ejercer las funciones conferidas por el RGPD.

A lo anterior hemos de añadir que, ninguna norma impide que el órgano que ejerce la

potestad sancionadora, cuando determina la apertura de un procedimiento sancionador, siempre de oficio, determine su alcance conforme a las circunstancias puestas de manifiesto en las reclamaciones y en la información suministrada por el reclamado o antes de la admisión a trámite de las reclamaciones, aunque las mismas no se ajusten estrictamente a las pretensiones del denunciante/reclamante. Y todo ello sin perjuicio de que el acuerdo de inicio del procedimiento sancionador no está constreñido por la denuncia (la "reclamación") presentada por el particular, sino que, pueden surgir de actuaciones de solicitud de información, de las actuaciones previas de investigación y de la posterior tramitación del procedimiento sancionador otros hechos que habrán de ser, en su caso, indicados en la propuesta de resolución, y en la propia resolución. Lo contrario sería establecer que es el reclamante/denunciante quien puede determinar el objeto del procedimiento sancionador, lo cual no sólo no es lo querido por la ley, en cuanto que los procedimientos sancionadores siempre se inician de oficio, sino que podría dar lugar a todo tipo de fraudes.

Dicho todo lo anterior, y centrándonos en el objeto del presente procedimiento, se ha de indicar que derivado del examen e investigación de una reclamación presentada ante la AEPD, la propia parte reclamada presentó en el marco de las actuaciones previas de investigación un protocolo "Normativa 94.30.005 PREVENCION DEL FRAUDE Y LA ESTAFA" (versión 8 de 1 de junio de 2015) que recoge las instrucciones para la prevención de fraude que tiene establecidas para las sucursales, el cual se encuentra recogido en el Hecho Probado Cuadragésimo tercero (documento 3) y examinado profusamente en el Fundamento de Derecho VI de la propuesta de resolución. Dicho documento se presentó por la parte reclamada para justificar la corrección de sus actuaciones en materia de detección del fraude en relación con la reclamación investigada.

Del resultado de las actuaciones previas de investigación se infirieron evidencias claras de la posible comisión de una serie de infracciones del RGPD, todas relacionadas con la reclamación concreta presentada: unas en relación con los hechos sufridos por la parte reclamante y otras conexas directamente a las anteriores y relativas a los procedimientos implantados por la entidad para la prevención del fraude (que afectaban, obviamente, a la parte reclamante y a cualquier cliente de la entidad bancaria).

Así, estas últimas responden a un incumplimiento de los artículos 25 y 32 del RGPD respectivamente, que afectan a la parte reclamante y a cualquier cliente de la entidad bancaria, constituye infracciones del RGPD aunque no se hubiera recibido la reclamación.

Asimismo, la solicitud de la prueba practicada y su valoración está conectada con la reclamación de dio lugar a la incoación del presente procedimiento.

El instructor del procedimiento acordó la apertura de un período de prueba sin que BBVA, sorprendentemente, presentara escrito de respuesta a la práctica de pruebas ni documento alguno de los solicitados (Hecho Probado Cuadragésimo sexto), ni en el momento procedimental oportuno, ni antes de formularse la propuesta de resolución, ni en las alegaciones a la propuesta de resolución, de tal forma que no ha acreditado que dicha documentación exista.

Recordemos que en esta práctica se solicitaba a BBVA que aportara "*evaluación de impacto de protección de datos (en adelante EIPD), fechada y firmada, en materia del tratamiento de los datos personales de los clientes del BBVA en materia de "BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA", "medidas técnicas y organizativas que tenía previstas el BBVA en fecha 14/04/2020 para evitar el fraude por suplantación de identidad, concretamente, en las operaciones a través de "BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA",* y, en tercer lugar, "*las medidas técnicas y organizativas que el BBVA tenía implantadas con fecha 14/04/2020, para que las comunicaciones realizadas a la entidad por sus clientes por la pérdida, extravío o sustracción del documento de identidad, teléfono móvil (donde BBVA envía el factor de autenticación) o las tarjetas de crédito, produzcan efecto en sus diversos canales de relación con el cliente relativos la operativa que este pueda realizar".*

De la mera lectura de los Antecedentes del presente documento puede comprobarse la relación de las pruebas acordadas con los hechos objeto de la reclamación.

Por otra parte, la documentación aportada por BBVA en las actuaciones previas de investigación y en este procedimiento ha sido analizada pormenorizadamente a efectos de determinar si da cumplimiento con la PDDD del artículo 25 del RGPD con relación a los procesos de contratación de productos bancarios, y con la existencia de medidas de seguridad del artículo 32 del RGPD, habiéndose justificado en el presente procedimiento como el incumplimiento de estos dos preceptos por BBVA está íntimamente conectado con los hechos objeto de la reclamación y de la documentación aportada por BBVA.

Sin embargo, por el contrario de lo realizado por la AEPD, BBVA ni en las alegaciones al acuerdo de inicio ni en las aportadas a la propuesta de resolución ha analizado cómo las medidas de los documentos aportados están relacionados con los hechos objeto de reclamación, y como pudieron evitar las tratamientos ilegales de datos, tan sólo se dice que "*debe hacerse referencia a los Documentos 1 a 8 aportados junto al presente escrito, de los que se desprende que mi representada ha proveído las directrices a seguir por las distintas áreas de negocio para la implementación de medidas de seguridad sobre los Sistemas de Información propiedad de BBVA*".

Las conductas concretas objeto de reclamación y constitutivas de las diversas infracciones atribuidas a BBVA han sido examinadas en las actuaciones realizadas en el presente procedimiento, como se constata de los hechos probados y de los fundamentos de derechos de la propuesta de resolución, partiendo de los hechos objeto de la reclamación, así como de los actos de instrucción.

Por último, en contestación a esta alegación, cabe también señalar que los hechos constitutivos de la infracción del artículo 25 del RGPD y la comisión de la infracción del artículo 32 del RGPD no pueden considerarse "*una situación particular*", sino que, del análisis de la documentación aportada por BBVA a lo largo de este procedimiento y en virtud de los hechos que concurren en el presente procedimiento y las consecuencias que han tenido para la parte reclamante, ha quedado acreditado la comisión de dos infracciones:

A) La infracción del artículo 25 del RGPD, atribuible a BBVA debido a que sus procedimientos de contratación de productos bancarios carecen, en materia de

protección de datos, de una correcta identificación y análisis de los riesgos en los derechos y libertades de los clientes (ausencia del enfoque en los riesgos en los derechos y libertades de los interesados), de una adecuada planificación, del establecimiento de medidas técnicas y organizativas apropiad, de todo tipo, tendentes a evitar la materialización de los riesgos, de un mantenimiento, actualización y control de aquellas desde la revisión continua de los riesgos, incluyendo la demostración del cumplimiento (observancia del principio de responsabilidad proactiva), como exige el artículo 5.2 del RGPD.

B) La infracción del artículo 32 del RGPD, atribuible a BBVA, ante la inexistencia de medidas de seguridad de datos personales apropiadas, técnicas u organizativas, con relación a los procedimientos de seguridad de datos personales en la contratación de productos financieros.

Por lo tanto, en ambas infracciones se produce un incumplimiento de las obligaciones del RGPD cuyas consecuencias se han puesto de manifiesto, concretamente, en el carácter continuado de los tratamientos ilegales de datos personales de la parte reclamante, a modo de ejemplo, las diversas operaciones bancarias fraudulentas realizadas por terceros con los datos personales de la parte reclamante, siendo atribuible a BBVA la responsabilidad de la falta de observancia de lo dispuesto en los artículos 25 y 32 del RGPD.

Se ha de reiterar que ambas infracciones del RGPD lo son, y se ha puesto de manifiesto durante la tramitación del procedimiento, con independencia de lo indicado en la reclamación.

No estamos ante una infracción potencial del RGPD, sino ante dos infracciones existentes que se materializan en un perjuicio de los derechos y libertades de un ciudadano. Como ejemplo de ello, lo ocurrido con la parte reclamante en el presente caso es suficientemente indicativo, ante unos hechos en los que se han producido reiteradas vulneraciones del RGPD, y como consecuencia de los cuales se ha puesto de manifiesto la ineficacia o la inexistencia del cumplimiento efectivo del RGPD. A este respecto debe tenerse en cuenta que el artículo 5.2 de dicha norma impone la obligación de ser capaz de demostrar que ha actuado conforme al principio de responsabilidad proactiva.

Estas infracciones, al estar basadas en las instrucciones que determinan el régimen de la organización y de la operativa del BBVA, tienen carácter sistémico, y no evitan tratamientos por terceros ajenos al titular legítimo de los datos, porque no está contemplado en la documentación aportada como ya se ha indicado en los hechos probados.

En conclusión, la AEPD no está convirtiendo el examen de una reclamación en una suerte de “causa general” contra la entidad bancaria, dado que, a lo largo del procedimiento, y con independencia de la documentación aportada por la parte reclamante, ha sido la propia entidad la que ha facilitado la información de la que se deducía las infracciones identificadas como ha quedado reflejado en los hechos probados.

2. BBVA considera que ha desarrollado actuaciones encaminadas al cumplimiento del

principio de la PDDD y precisamente como consecuencia del análisis derivado del cumplimiento de ese principio, había implementado medidas adecuadas desde el punto de vista de la seguridad para impedir el riesgo.

En primer término, se debe aclarar una cuestión de concepto. El responsable del tratamiento está obligado a cumplir con el PDDD, no sólo a desarrollar actuaciones *encaminadas* a su cumplimiento. Y las medidas técnicas y organizativas apropiadas a implementar no son sólo de seguridad, sino de cualquier tipo para aplicar de forma efectiva los principios de protección de datos a fin de cumplir los requisitos del RGPD y proteger los derechos de los afectados.

La parte reclamada pretende de forma interesada y constante ligar las medidas de seguridad, y sólo las de seguridad, referidas a la infracción del art. 32 del RGPD con las medidas previstas en el artículo 25 del RGPD, como si de un totum revolutum se tratara, a los efectos de generar una asociación de ideas para que prevalezca su interpretación sobre la existencia del concurso medial.

Sin embargo, a lo largo del procedimiento se ha explicado de forma pormenorizada la diferente tipificación del art. 25 y 32 del RGPD. Adicionalmente, cabe indicarse que si ambas infracciones estuviesen íntimamente relacionadas, lo normal sería que se imputaran habitualmente de forma simultánea, cuando esto no es así.

Segundo que, frente a lo alegado por la parte reclamada de que ha cumplido, los hechos probados, que no han sido impugnados ni rebatidos por esta, muestran claramente lo 8contrario tal y como se pone de manifiesto en los fundamentos de derecho de la propuesta de resolución.

Por todo lo expuesto, se desestima la presente alegación.

"SEGUNDA.- ACERCA DE LA CONCURRENCIA DE CONCURSO MEDIAL ENTRE LAS DOS INFRACCIONES IMPUTADAS A BBVA"

Según BBVA, esta Agencia había realizado una interpretación errónea de sus alegaciones en cuanto a la inexistencia de concurso medial, cuando lo que BBVA planteaba era lo siguiente: "*la falta de aplicación de las medidas a las que se refiere el artículo 32.1 traería necesaria e inseparablemente causa de la falta de concepción o diseño de las mismas en el momento de determinar los medios y fines del tratamiento. De este modo, la AEPD consideraría sancionables la falta de diseño de una determinada medida de seguridad y su falta de aplicación, lo que obviamente sólo podría traer causa de esa falta de diseño previo, concurriendo así los requisitos exigidos para la apreciación del concurso medial en el presente caso*". Además, reclama la aplicación del concurso medial tal y como se recoge en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, "LRJSP").

Dos son las cuestiones que tratar en relación con esta alegación:

1. Interpretación errónea de las alegaciones del BBVA respecto del concurso medial.

2. La aplicación del concurso medial en los términos del artículo 29 de la LRJSP.

Vamos a examinarlas de manera diferenciada.

1. Interpretación errónea de las alegaciones del BBVA respecto del concurso medial.

En contestación a la primera de las alegaciones, aclarar en primer término que se vuelven a confundir conceptos y tipificaciones en aras de abonar la idea de la existencia del concurso medial.

Esta alegación denota una confusión de concepto al considerar que dos infracciones que, primero, están perfectamente definidas en el RGPD, y que como se ha explicado a lo largo del procedimiento, son diferentes y, segundo, están tipificadas de manera independiente en el RGPD y calificadas también de forma diferente en la LOPDGDD a efectos de prescripción, son consecuencia una de la otra.

De hecho, los silogismos que se utilizan de contrario no son ciertos en una comprensión e interpretación correcta de lo que resulta ser el cumplimiento del RGPD. Por ejemplo:

- La falta de medidas de seguridad no es lo mismo que la falta de aplicación de medidas de seguridad, ni una viene ligada indisolublemente a la otra.
- Pueden estar implantadas medidas de seguridad y no aplicarse las mismas o aplicarse incorrectamente.
- La falta de aplicación de las medidas de seguridad puede que no derive de un problema de diseño previo. Puede ser el responsable del tratamiento no haya dado instrucciones respecto de su aplicación.
- En ocasiones, algunas organizaciones no tienen implantadas específicamente medidas de seguridad conforme al RGPD, ni trasmiten a sus empleados siquiera si tienen que aplicar medidas de seguridad, más estos empleados realizan o dejan de realizar alguna acción que evita la materialización del riesgo.
- Puede que no haya implantadas medidas de seguridad, pero sí otras medidas técnicas u organizativas apropiadas, de otro tipo, que impidan la materialización del riesgo. Por ejemplo, una medida consistente en la concienciación de los empleados no es una medida de seguridad de las del artículo 32 del RGPD sino una de las medidas del artículo 25 del RGPD, pero que puede evitar que se materialice un riesgo de suplantación de identidad.
- Puede que existan algunas pocas medidas de seguridad que se apliquen correctamente y eviten la materialización del riesgo, sin perjuicio de que exista, en atención a todos los riesgos identificados, una flagrante falta de todas las medidas de seguridad que deberían estar implantadas.
- Puede que hayan sido diseñadas e implantadas correctamente las medidas de seguridad y que se apliquen incorrectamente o que simplemente no se apliquen.

Se podría continuar ad infinitum con ejemplos en los que la falta de medidas de seguridad o su falta de aplicación traiga causa, como dice la parte reclamada, “obviamente” de ese diseño previo, lo que, por cierto, tampoco acontece en el supuesto examinado.

En segundo lugar, que, de nuevo, BBVA interpreta de forma incorrecta las conductas que suponen las infracciones de los artículos 25 y 32 del RGPD, ya que considera que el incumplimiento del artículo 32 del RGPD se refiere a la existencia y aplicación de "medidas" (sin especificar qué tipo de medidas), y la infracción del artículo 25 se determina por la ausencia de concepción o diseño de tales medidas.

En efecto, la PDDD no sólo abarca el diseño sino también la determinación de medidas técnicas y organizativas apropiadas de todo tipo. En primer lugar, debe realizarse una identificación y evaluación de los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, identificación y evaluación de riesgos que hasta el momento no ha sido aportada por BBVA, so pena ha sido solicitada dicha documentación en la prueba practicada en el procedimiento; y, posteriormente, "*aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento*, *medidas técnicas y organizativas apropiadas".* (artículo 25 del RGPD).

A modo de ejemplo, constituyen medidas técnicas y organizativas que no son de seguridad las medidas relativas a la gestión de información a los clientes, el establecimiento de un canal o un procedimiento que articule la tramitación de escritos presentados por los de clientes de BBVA que afectan a la protección de datos de carácter personal, cursos de formación generales al personal del BBVA o la realización de auditorías, lo cual sería especialmente oportuno en este caso, teniendo en cuenta las carencias de las medidas que se han puesto de manifiesto en este caso.

Aunque las infracciones del artículo 25 y del artículo 32 del RGPD se refieren a los procedimientos establecidos por BBVA, lo cierto es que la falta de tales procedimientos adecuados al RGPD afecta a los clientes de BBV. Esto ocurrió, por ejemplo, en el caso de la parte reclamante que comunicó por diversos medios la sustracción de su documentación y del teléfono móvil, hechos que, pueden afectar a sus datos personales, a sus derechos y libertades, que debieron producir efecto, una reacción resolutiva respecto de la situación denunciada, en los diversos canales de relación de BBVA con sus clientes relativos la operativa que estos puedan realizar; no tiene sentido que siguiera constando en los ficheros de BBVA el mismo número de teléfono de la parte reclamante (******TELÉFONO.1***) una vez comunicado su sustracción, y que este siguiera siendo usado como factor de autenticación de la parte reclamante y esto se debió a la falta de un procedimiento adecuado desde la perspectiva del RGPD como ha quedado constatado en el hechos probados.

2. La aplicación del concurso medial en los términos del artículo 29 de la LRJSP.

Por el contrario de lo afirmado por la parte reclamante, la AEPD no ha indicado en ningún momento:

- Que la aplicación del RGPD y de la LOPDGDD excluya la aplicación del resto del ordenamiento jurídico.
- Que la aplicación del RGPD y de la LOPDGDD excluya en los procedimientos sancionadores tramitados por la AEPD la consideración de la Jurisprudencia existente.

- Que la aplicación del RGPD y de la LOPDGDD excluya la aplicación en los procedimientos sancionadores tramitados por la AEPD de los principios del procedimiento sancionador.
- Que la aplicación del RGPD y de la LOPDGDD excluya la aplicación en los procedimientos sancionadores tramitados por la AEPD del principio de proporcionalidad.
- Que no pueda existir en alguna ocasión, atendiendo siempre a las circunstancias del caso concreto, concurso medial (aunque no sea el caso del procedimiento ahora examinado).
- Que a la AEPD no le resulte de aplicación la LRJSP.

La AEPD, cumpliendo estrictamente toda la normativa que le resulta de aplicación, que incluye, como no podía ser de otra forma la Constitución Española y la Carta de Derechos Fundamentales de la Unión Europea, y los principios del procedimiento sancionador, lo que afirma es que:

- El principio de proporcionalidad es aplicable al procedimiento sancionador.
- El legislador europeo ha reglamentado lo relativo al principio de proporcionalidad en el artículo 83 del RGPD.
- Dado que el RGPD tiene una regulación completa y propia del principio de proporcionalidad, resultando que no existe laguna legal alguna, no resulta de aplicación específicamente y en concreto el artículo 29 de la LRJSP.

En relación con la supuesta confusión entre supletoriedad y subsidiaridad comenzaremos por repetir literalmente lo que se indicó en la propuesta de resolución:

> "2. Al no haber laguna legal, no hay aplicación supletoria del art. 29 de la LRJSP.
>
> Amén de lo expuesto, 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 art. 29 de la LRJSP, dado que el RGPD es un sistema cerrado y completo como ya se aclaró en las alegaciones al acuerdo de inicio
>
> 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 art. 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".

Como ya indicábamos además, 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-, 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, 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.

Aclarar, con carácter previo que, la supletoriedad se refiere a supuestos en los que en una determinada norma no se regula un específico supuesto, laguna legal, dando lugar a la aplicación de otra norma jurídica que regule tal situación, siempre que no resulte disconforme con el ordenamiento jurídico.

Mientras que la subsidiaridad hace referencia a un concurso de normas, lo que supone que para un determinado supuesto pueden ser aplicables dos o más normas, de manera que la norma subsidiara cede en beneficio de la principal.

Pues bien, vista la literalidad de lo señalado por la AEPD se examinaba tanto la supletoriedad como la subsidiariedad para concluir la no aplicación del artículo 29 de la LRJSP sino del artículo 83 del RGPD en relación con el principio de proporcionalidad.
Se indicaba:

- Que el principio de proporcionalidad se aplica al procedimiento sancionador.
- Que el principio de proporcionalidad se regula de forma completa en el artículo 83 del RGPD.
- Que no hay laguna legal.
- Que ni el RGPD ni la LOPDGDD remiten a la aplicación, por existencia de laguna legal, del artículo 29 de la LRJSP.
- Que en los procedimientos tramitados por la AEPD, recalcamos, para los procedimientos administrativos tramitados, se prevé la aplicación subsidiaria de las normas generales sobre los procedimientos administrativos.
- Que en los procedimientos tramitados por la AEPD recalcamos, para los procedimientos administrativos tramitados y no en relación con los principios del procedimiento sancionador, no se establece en la LOPDGDD una aplicación subsidiaria de la LRJSP.
- Se concluía que no había ni supletoriedad ni subsidiaridad que hicieran que se aplicase el artículo 29 de la LRJSP.

En relación con la cita de las Directrices 04/2022 del CEPD sobre el cálculo de multas administrativas conforme al RGPD, en su versión 2.1, adoptadas el 24 de mayo de

2023, en su apartado 22 se hace referencia a tres tipos de concurrencias, a saber, de infracción, unidad de acción y pluralidad de acciones: "*Al examinar el análisis de las tradiciones de los Estados miembros en materia de normas de concurrencia, tal como se indica en la jurisprudencia del TJUE5 , y teniendo en cuenta los diferentes ámbitos de aplicación y las consecuencias jurídicas, estos principios pueden agruparse aproximadamente en las tres categorías siguientes: - Concurrencia de infracciones (capítulo 3.1.1), - Unidad de acción (capítulo 3.1.2), - Pluralidad de acciones (capítulo 3.2).*

En los supuestos de concurrencia de infracciones la previsión establecida al respecto es la contenida en el artículo 83.3 del RGPD que establece un límite cuantitativo en estos supuestos de concurrencia: "*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."* (el subrayado es nuestro).

Si admitiéramos el argumento esgrimido por BBVA, podría extraerse que la "plena aplicabilidad del concurso medial" referido a la aplicación preferente del artículo 29 de la LRJSP, en su única pretensión de pagar una única multa en lugar de las dos impuestas, desplazan o anulan la vigencia del art 83.3 RGPD, lo que resulta a todo punto contrario por el ordenamiento jurídico.

Asimismo, en este momento hemos de recordar que la gravedad de las infracciones del RGPD se determina en atención a las reglas establecidas en este y no en la LOPDGDD. La tipificación de las infracciones se encuentra regulada en el artículo 83, apartados 4, 5 y 6 del RGPD, mientras que la calificación de las infracciones como muy graves, graves o leves a los solos efectos de la prescripción se dispone en los artículos 72, 73 y 74 de la LOPDGDD. Mas, en contra de lo que indica la parte reclamante, la gravedad de las infracciones no se regula en estos preceptos de la LOPDGDD.

Por último y no menos importante, la AEPD no sanciona por una misma ofensa, como aduce la parte reclamada, sino que se han constatado a través de hechos probados no rebatidos por el BBVA, la comisión de dos infracciones diferenciadas, tipificadas de forma diferenciada, no existiendo, además, en el caso concreto, concurso medial.

Por todo lo expuesto, se desestima la presente alegación.

"*TERCERA.- SOBRE LA INEXISTENTE VULNERACIÓN DEL ARTÍCULO 25 DEL RGPD"*

En primer lugar, y antes de examinar las alegaciones formuladas en relación con la vulneración el artículo 25 del RGPD,

1. El artículo 25 del RGPD parte de la necesidad de tener en cuenta una serie de elementos:

- Estado de la técnica
- Coste de la aplicación

- Naturaleza, ámbito, contexto y fines del tratamiento
- Riesgos que entraña el tratamiento para los derechos y libertades de las personas físicas.

2. Impone una obligación al responsable, que determina los fines y los medios del tratamiento, dando, en este caso, especial relevancia a los medios.

3. El mismo debe aplicar, tanto al determinar los medios del tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas (por ejemplo, la seudonimización), concebidas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías que sean necesarias en el tratamiento.

4. Con ello, se persigue un doble fin:
- Cumplir los requisitos del RGPD
- Proteger los derechos de los afectados.

El RGPD pretende lograr con la aplicación de sus disposiciones la protección de los derechos de los afectados. Por tanto, el foco debe dirigirse siempre a la identificación y evaluación de los riesgos en los derechos y libertades de los afectados, con la posterior adopción de medidas técnicas y organizativas de todo tipo destinadas a evitar su materialización.

Así, el artículo 25 del RGPD hace referencia a los “Riesgos que entraña el tratamiento para los derechos y libertades de las personas físicas”.

Si el enfoque que adopta la empresa u organización no está orientado a los riesgos para los derechos y libertades de los interesados sino, a los riesgos para la propia empresa u organización, no sólo no se va a procurar una protección eficaz a los interesados (pues hacia donde no miras, no ves), sino que se incumple el art. 25 del RGPD.

Puede coincidir que las medidas adoptadas por el responsable del tratamiento para la cubrir los riesgos de su organización, puedan eventualmente evitar la materialización de los riesgos en los derechos y libertades de sus clientes, pero no puede darse por cumplido la PDDD, en el marco de la responsabilidad proactiva, cuando no se ha aplicado el enfoque prescrito en el artículo 25 del RGPD que se centra en identificar los riesgos de diversa probabilidad y gravedad que entraña un tratamiento para los derechos y libertades de las personas físicas, con el fin último de proteger los derechos de los interesados.

Si bien es cierto que no es nuevo el concepto de la PDDD, tal y como alega BBVA, también lo es que, en materia de protección de datos, la configuración de la PDDD como una obligación para el responsable del tratamiento con las características y elementos antes descritos sí es una cuestión a todo punto novedosa. Y que no puede considerarse cumplida la obligación impuesta por el legislador comunitario si el principio de la PDDD no se aplica en los términos dispuestos en el RGPD.

Ello no puede ser así si la documentación, por ejemplo, es anterior al RGPD (resultando que simplemente la PDDD en materia de protección de datos no se encontraba configurada legalmente), si no identifica y evalúa los riesgos en los

derechos y libertades de los interesados o si el enfoque no está centrado en los interesados sino en los riesgos en la organización. Agravado por encontrarnos en una sociedad cambiante donde el fraude en continua evolución está más que presente y en la que la tecnología ha incrementado de forma exponencial las formas de engaño.

Además, tanto la evaluación de riesgos como las medidas adoptadas deben estar actualizadas, frente a un entorno de continua sofisticación de los mecanismos de fraude, como reconoce el propio documento "PREVENCION DEL FRAUDE Y LA ESTAFA", en su apartado de "Consideraciones generales":

"Esta eficacia está condicionada por un hecho innegable: el mundo del fraude está en continuo cambio y los procedimientos son perfeccionados por los delincuentes constantemente, por lo que habrá que actualizar la información de forma permanente."

Resulta inconcebible que un documento de prevención del fraude y la estafa de 2015, no sólo prevea todos los riesgos actuales, ocho años después, sino que tenga en sí mismo plena vigencia.

Sobre este particular nos remitimos a los hechos probados, en relación con los documentos aportados por la parte reclamada y su contenido y a su valoración dispuesta en los fundamentos de derecho

Un ejemplo de que la parte reclamada no ha aplicado correctamente la PDDD lo podemos observar en la falta de identificación del riesgo.
Nos referimos, en concreto, a la constante referencia que realiza la parte reclamada de que sus clientes son los responsables de custodiar con una mínima diligencia las claves o credenciales que les fueron suministradas, tal y como dicen que les advierten a estos de manera reiterada.
La pérdida accidental, el olvido o el robo de las claves o credenciales de un cliente es algo más que habitual.
Que otra persona pueda, de manera fortuita o no, tener acceso a las claves o credenciales de otra distinta tampoco es nada extraño.
Que la probabilidad de que esto suceda aumenta notablemente si tenemos en consideración el número de clientes de esta entidad bancaria.
Amén del nivel de fraude actual.
Que una persona pueda acceder a la banca digital de un cliente por la causa descrita no es imprevisible.
Si además un cliente denuncia el acceso por un tercero con sus claves y credenciales, la posibilidad de materialización del riesgo se ve incrementada.
Y todo ello sin perjuicio de ese deber de custodia del cliente. Simplemente es algo que sucede.

Nos encontramos de esta forma con un riesgo palpable presente en el tratamiento, que aún en este momento la entidad bancaria sigue sin identificar, sin evaluar y sobre el que no ha establecido ni se previeron medidas técnicas u organizativas de ningún tipo.
Desplazar su responsabilidad como responsable del tratamiento a sus clientes no sólo supone una falta de lealtad, sino un incumplimiento flagrante de sus obligaciones.

Respecto a la custodia de la contraseña de acceso, se reproduce aquí lo que ya se

respondió a BBVA en sus alegaciones al acuerdo de inicio:

"*BBVA considera que "el acceso por el cliente a la banca on-line de BBVA exige la utilización de un primer factor de autenticación cuya custodia y control no le corresponde, recayendo sobre el cliente". Cabe plantear entonces qué tipo de solución aporta BBVA al cliente en caso de que un tercero tenga acceso al primer factor de autenticación, cuando es evidente que esto se ha producido, y el cliente avisa a BBVA con carácter previo que ha perdido el control sobre sus datos personales. En este procedimiento ha quedado acreditado que BBVA no dispone de ninguna medida de seguridad de gestión de contraseñas, de autenticación o de otro tipo en supuestos de alto riesgo de fraude, para la protección de los usuarios y evitar, entre otros, el uso recurrente del primer factor de autenticación por parte de persona distinta del titular.*

No se trata, como dice BBVA de la "imposición a mi mandante de una responsabilidad de la que carece, pues en modo alguno puede estar bajo su control la evitación de que las credenciales de todos sus usuarios de banca on-line puedan serles sustraídas a sus clientes por terceros". Como se ha dicho, la responsabilidad recae desde el momento en que BBVA carece de medida de seguridad alguna de gestión de contraseñas, autenticación de los usuarios, de bloqueo o de algún otro tipo, para evitar accesos no autorizados en supuestos de pérdida o robo de datos que pueden ser utilizados para cometer un fraude, ni siquiera para evitar que el fraude continúe cometiéndose, una vez que la pérdida o robo les ha sido comunicada."

Y todo ello porque este riesgo notorio sigue sin ser detectado por la entidad. Ni lo previó inicialmente cuando empezó a diseñar el procedimiento ni tampoco después, a pesar del nivel elevado de fraude está aumentando considerablemente con técnicas cada vez más sofisticadas.

Por otro lado, la mera alegación realizada por la parte reclamada de que se ha cumplido con la PDDD no es suficiente si no se acredita oportunamente su cumplimiento, tal y como acontece en el presente procedimiento, al no haber aportado la documentación específica que, entre otras cuestiones, pusiera de manifiesto que se había efectuado una identificación y evaluación de los riesgos respecto de los derechos y libertades de los interesados en relación con el fraude.

Máxime cuando se le dio la oportunidad de acreditarlo a través de la documentación específicamente solicitada como prueba en el procedimiento sancionador, relativa a la identificación y valoración de los riesgos (evaluación de impacto de protección de datos y, en su defecto, análisis de riesgos).

Documentación que, recordemos, no se ha aportado por el BBVA.

Continúa BBVA en sus alegaciones manteniendo que "*mi representada elaboró diversos documentos encaminados a evitar la suplantación de la identidad de los clientes en su operativa con el Banco".*

En respuesta a este argumento, cabe señalar que BBVA no menciona tampoco a qué documentos en concreto se refiere. Del análisis realizado tanto en el acuerdo de inicio como en la propuesta de resolución de la documentación aportada por BBVA, se determina que ninguno los documentos aportados (tampoco el documento

denominado “Prevención del fraude y de la estafa”) abordaban el riesgo relativo a que cuando un cliente pierde, o le es sustraída, determinada documentación identificativa, o los métodos o dispositivos para el acceso a su banca online, quedan al descubierto los datos personales que permiten la contratación a distancia de productos financieros.

Según BBVA *“el riesgo materializado en el presente expediente y que mi representada reconoció a limine mediante el pago de las sanciones directamente relacionadas con el mismo no deriva del hecho de que se sustrajeran a la interesada su documento nacional de identidad, tarjetas y teléfono móvil, sino de que quien llevó a cabo esa sustracción pudo acceder a un elemento de autenticación y verificación de la interesada, las claves de acceso a su banca privada”.*

BBVA quiere atribuir a la parte reclamante, y no a los terceros que le sustrajeron los documentos y el móvil, la responsabilidad de las operaciones bancarias fraudulentas, debido a la falta de cuidado en la custodia de la clave de acceso a su banca privada.

A este respecto, debe recordarse que la conducta que constituye la infracción en este caso son unas medidas de gestión de incidentes de fraude cuando, una vez que un cliente de BBVA comunica la sustracción de sus documentos, de su teléfono móvil o de su clave de autenticación, esta comunicación no evita que se produzcan tratamientos ilegales de sus datos.

Una vez contestados estos primeros argumentos a los que se refiere BBVA en esta alegación, los razonamientos posteriores no se justifican en modo alguno.

Esta Agencia no confunde los riesgos con las causas generadoras de los riesgos, y no se exige “*la necesidad de poder detectar cualesquiera causas que pudieran motivar el mismo*”, pero, del mismo modo que en el documento "PREVENCION DEL FRAUDE Y LA ESTAFA", cuya transcripción parcial consta en el Hecho Probado Cuadragésimo Tercero (documento nº 3), se contempla cómo debe actuarse en caso de Hurto o Extravío del Documento de Identidad, debe contemplarse las medidas apropiadas de todo tipo que eviten la suplantación cuando se ha comunicado a BBVA la sustracción o pérdida de la contraseña de acceso a la “*BANCA A DISTANCIA TELEFONÍA MÓVIL/ TARJETA”*, o del dispositivo a través del cual se establece el segundo factor de autenticación.

BBVA considera que “*En el presente supuesto se ha producido un fallo en una medida concreta de seguridad, no una vulneración del principio de privacidad desde el diseño.”*

En efecto, la PDDD no sólo abarca la adopción de medidas técnicas y organizativas apropiadas de seguridad, sino de todo tipo. Nos remitimos a lo ya explicitado sobre el contenido y elementos de la PDDD.

A modo de ejemplo, constituyen medidas técnicas y organizativas que no son de seguridad las relativas al establecimiento de un procedimiento de comunicación con los clientes, cursos de concienciación al personal del BBVA o la realización de auditorías, lo cual sería especialmente oportuno en este caso, teniendo en cuenta las

carencias que se han puesto de manifiesto en este caso. Además, medidas que eviten el uso de datos que se han visto comprometidos (por ejemplo, en caso de pérdida o sustracción) para la contratación de productos bancarios.

De los reiterados incumplimientos que se han producido por parte de BBVA se determina que la vulneración del artículo 25 del RGPD tiene carácter sistémico. Como ha quedado constatado en los Hechos Probados a partir de la documentación aportada por BBVA no existe unas pautas que permitan actuar ante este determinado riesgo, que como se ha indicado cada vez es más frecuente y sofisticado. Además, y como también consta en los Hechos Probados, las diversas comunicaciones realizadas por la parte reclamante a BBVA no han evitado los múltiples y repetidos tratamientos ilegales de sus datos personales, por lo que no estamos hablando de un fallo ocasional o puntual. Si todo el sistema falla y de forma continua, es que no hay establecido un procedimiento adecuado desde la PDDD.

Por último, el RGPD establece una la protección de los derechos y libertades de las personas físicas, la cual no es equiparable a los intereses propios de la entidad que tiene que velar por sus propios intereses. En el presente caso se comprueba cómo una indebida protección de los derechos y libertades de los clientes les produce un perjuicio, que como se puede observar no tiene repercusión en la propia entidad financiera.

No considera BBVA que la entrada en vigor del RGPD suponga un cambio en las obligaciones que entraña en materia de protección de datos: "…*si los documentos aportados por mi representada configuran las directrices a seguir para la garantía del principio y las medidas a adoptar ante determinadas situaciones de riesgo, como las consistentes en la posible suplantación de sus clientes en la interrelación de aquéllos con BBVA, tal y como ha acreditado mi representada, el hecho de que dichos documentos sean anteriores o posteriores al RGPD resulta irrelevante, siempre y cuando respondan a un principio que existe en materia de protección de datos desde más de veinte años antes de que el RGPD fuera plenamente aplicable o, incluso, hubiera entrado en vigor*."

Sin embargo, el RGPD, tal y como hemos explicitado, consagra la responsabilidad proactiva, la cual implica la implantación de un modelo de cumplimiento y de gestión del RGPD que determina la observancia generalizada de las obligaciones en materia de protección de datos. Comprende el establecimiento, mantenimiento, actualización y control de las políticas de protección de datos en una organización, especialmente si es una gran empresa, -entendidas como el conjunto de directrices que rigen la actuación de una organización, prácticas, procedimientos y herramientas-, desde la PDDD y por defecto, que garanticen el cumplimiento del RGPD, que eviten la materialización de los riesgos y que le permita demostrar su cumplimiento.

Por todo lo expuesto, se desestima la presente alegación.

"CUARTA.- SOBRE LA INEXISTENTE VULNERACIÓN DEL ARTÍCULO 32 DEL RGPD"

BBVA comienza esta alegación repitiendo sus argumentos respecto a la existencia de

bis in idem o, en su defecto, de concurso medial entre las dos infracciones que pretenden imponerse a BBVA cuestión a las cuales se le ha dado respuesta en los apartados SEGUNDO y TERCERO de esta contestación a las alegaciones a la propuesta de resolución.

Continúa diciendo que "*BBVA ya se ha referido con anterioridad a cómo los documentos aportados junto con su escrito de alegaciones al Acuerdo de Inicio evidencian la existencia de tales medidas*", estos documentos ya han sido analizados tanto en el acuerdo de inicio como en el Fundamento de Derecho III de la propuesta de resolución.

Se transcribe en el escrito de alegaciones una serie de enlaces informativos sobre la seguridad, pero no pueden considerarse estrictamente medidas de seguridad.

En el documento se aporta "*información relevante acerca de las credenciales del usuario y su debida protección, siendo preciso recordar que dichas credenciales, que han de encontrarse bajo el exclusivo control del cliente, constituyen, conforme a la normativa reguladora de medios de pago, y tal como se analizó detalladamente en las alegaciones al Acuerdo de Inicio, el primer factor de verificación de la identidad".*

De nuevo BBVA quiere atribuir a cualquier cliente, la responsabilidad de las operaciones bancarias fraudulentas, debido a la falta de cuidado en la custodia de la clave de acceso a su banca privada, sin asumir su responsabilidad por no adoptar medidas técnicas y organizativas apropiadas de seguridad:

" […] *Y en modo alguno cabe imputar a mi representada la posible quiebra que en la seguridad del acceso a la banca on-line pudo derivarse de la insuficiente o inadecuada custodia de ese primer factor de autenticación."*

Esta cuestión ya se respondió anteriormente, "*Como se ha dicho, la responsabilidad recae desde el momento en que BBVA carece de medida de seguridad alguna de gestión de contraseñas, autenticación de los usuarios, de bloqueo o de algún otro tipo, para evitar accesos no autorizados en supuestos de pérdida o robo de datos que pueden ser utilizados para cometer un fraude, ni siquiera para evitar que el fraude continúe cometiéndose, una vez que la pérdida o robo les ha sido comunicada.""*

Por todo lo expuesto, se desestima la presente alegación.

"QUINTA: SOBRE LA VULNERACIÓN DEL PRINCIPIO DE PROPORCIONALIDAD EN LA IMPOSICIÓN DE LA SANCIÓN"

En este apartado BBVA estima que "*resulta necesario que por el Órgano Sancionador se proceda a evaluar meticulosamente las circunstancias concurrentes en el presente supuesto en el que solamente se han visto afectada dos personas, con la finalidad de determinar la cuantía de la medida punitiva que en su caso proceda adoptar contra mi mandante en el negado supuesto en que así procediese hacerlo, algo que, a juicio de esta parte, no ha realizado la AEPD, tal y como se razonará.".*

Frente al análisis detallado que exige BBVA en su escrito de alegaciones a la

propuesta de resolución, cabe señalar que ya el acuerdo de inicio, en su Fundamento de Derecho X, recoge desde la página 34 a la 39 los criterios de graduación de la cuantía de cada una de las sanciones con una amplia fundamentación, por lo que las circunstancias previstas en el artículo 83.2 del RGPD aplicables al caso han sido suficientemente motivadas.

Partiendo de esa base, en respuesta a la evaluación meticulosa a que se refiere BBVA en sus alegaciones a la propuesta de resolución, el Tribunal Constitucional señaló en STC 16 de junio de 1982 (RTC 1982, 36) "*que la motivación escueta o sucinta, si es suficientemente indicativa no equivale a ausencia de motivación ni acarrea su nulidad* ". En la misma línea, el Tribunal Supremo estableció (STS 30 enero de 2001 [RJ 2001, 1147]) que "*La motivación ha de ser suficientemente indicativa, lo que significa que su extensión estará en función de la mayor o menor complejidad de lo que se cuestione o de la mayor o menor dificultad del razonamiento que se requiera, lo que implica que pueda ser sucinta o escueta, sin necesidad de amplias consideraciones, cuando no son precisas ante la simplicidad de la cuestión que se plantea y que se resuelve*".

La Jurisprudencia utiliza un criterio muy flexible, y admite que esta motivación se haga, bien directamente, bien por referencia a informes o dictámenes obrantes en las actuaciones (STS de 21 de enero de 2003 [RJ 2003, 893]), mediante la incorporación de la propuesta de resolución (STS de 10 de noviembre de 1993 [RJ 1993, 8201]), o resulta del mismo expediente administrativo (STS 29 de julio de 2002 [RJ 2002, 7385). Es lo que se conoce como motivación "in alliunde".

Dando una respuesta más extensa según las consideraciones realizadas por BBVA, la falta de aplicación de la Protección de Datos desde el Diseño y por Defecto en el procedimiento establecido por la entidad bancaria respecto a la gestión de incidentes en relación con el fraude ha quedado acreditado en este procedimiento, por un lado, así como inexistencia de las medidas técnicas y organizativas de seguridad adecuadas en la gestión del fraude, de estas últimas, en particular, la relativa a la gestión del primer factor de autenticación cuando de forma reiterada se ha comunicado por el afectado (y así ha sido comprobado por el BBVA) que terceros han tenido acceso a aquel, por otro lado.

Pues bien, estas dos infracciones no afectan tan sólo a la parte reclamante, sino a todos aquellos clientes de BBVA afectados por el mismo riesgo, que hayan sufrido o puedan sufrir las consecuencias de la falta de un procedimiento adecuado de gestión del fraude con medidas que aseguren la PDDD (artículo 25 del RGPD), o la carencia de medidas de seguridad (artículo 32 del RGPD), ante una situación de suplantación o de uso ilegal de los datos personales que les conciernen.

Por lo tanto, a diferencia de lo alegado por BBVA, estas infracciones sí tendrían carácter sistémico, al no tratarse de conductas que afecten a un caso en particular.

Teniendo en cuenta, además, que según el documento "*Presentación Prensa 4T2022*" de consulta pública en la web https://www.bbva.com/es/resultados-4t22/, el volumen total de clientes activos del Grupo BBVA superó la cifra de 67 millones a finales de 2022, siendo el 55% de los nuevos clientes captados por canales digitales, lo que refuerza la necesidad de un procedimiento de gestión de incidentes que asegure los derechos y libertades de las personas físicas con medidas técnicas y organizativas

apropiadas de todo tipo, que aplique de forma efectiva los principios de protección de datos, y, por otra parte, que se adopten medidas de seguridad para evitar tratamientos ilegales de datos como los ocurridos en este caso.

El carácter de entidad financiera determina que los tratamientos de datos de sus clientes tengan riesgos de mayor probabilidad y gravedad que las actividades de tratamiento de empresas con otro tipo de actividad, lo que determina una circunstancia a tener en cuenta al efecto de graduar la sanción, al igual que ocurre que con los datos financieros de los clientes, así se establece en las Directrices 04/2022 del Comité Europeo de Protección de Datos, sobre el cálculo de las multas bajo el RGPD, adoptado el 23 de mayo de 2023, en cuyo apartado 57 establece:

"En cuanto al requisito de tener en cuenta las categorías de datos personales afectadas (artículo 83, apartado 2, letra g) del RGPD), el RGPD destaca claramente los tipos de datos que merecen una protección especial y, por lo tanto, una respuesta más estricta en términos de multas. Esto se refiere, como mínimo, a los tipos de datos cubiertos por los artículos 9 y 10 del RGPD, y a los datos fuera del ámbito de aplicación de estos artículos cuya difusión causa daños o dificultades inmediatas al interesado (por ejemplo, datos de localización, datos sobre comunicación privada, números de identificación nacionales o datos financieros, como resúmenes de transacciones o números de tarjetas de crédito). En general, cuanto más se trate de tales categorías de datos o más sensibles sean los datos, más peso podrá atribuir la autoridad de control a este factor." (el subrayado es nuestro).

Por último, respecto a la cuantía de la sanción, en la propia web del BBVA (https://www.bbva.com/es/resultados-4t22/), se encuentra disponible el documento "Informe 4T2022", en el cual puede consultarse la cuantía del margen bruto de la cuenta de resultados, que alcanza los 24.890 millones de euros, si bien no es exactamente "*del volumen de negocio total anual global del ejercicio financiero anterior*" (artículo 83.4 del RGPD), es una cifra menor al volumen de negocio y además del año 2022, pero otorga una imagen fiel del gran tamaño del Grupo BBVA, y de la proporcionalidad en el cálculo de la cuantía de ambas sanciones conforme a lo dispuesto en el artículo 83.4 del RGPD. Volviendo a las Directrices 04/2022, del Comité Europeo de Protección de Datos, en su interpretación del RGPD, señala que:

"120. Por consiguiente, en los casos en que el responsable o encargado del tratamiento sea (parte de) una empresa en el sentido de los artículos 101 y 102 del TFUE, el volumen de negocios combinado de dicha empresa en su conjunto puede utilizarse para determinar el límite máximo dinámico de la multa (véase el capítulo 6.2.2) y para garantizar que la multa resultante se ajuste a los principios de efectividad, proporcionalidad y disuasión (artículo 83, apartado 1, del RGPD)[51].

.

121. El TJUE ha desarrollado una amplia jurisprudencia sobre el concepto de empresa. El término «empresa», «incluye a todas las entidades que ejercen una actividad económica, independientemente de la condición jurídica de la entidad y de la forma en que se financia»[52.] A efectos del derecho de la competencia, las «empresas» se identifican por tanto con unidades económicas y no con unidades jurídicas. Diferentes sociedades pertenecientes al mismo grupo pueden constituir una unidad económica y, por tanto, una empresa en el sentido de los artículos 101 TFUE y 102 TFUE [53].

[…]
51 Véase la Decisión vinculante 1/2021 del CEPD, apartados 412 y 423, y también los asuntos C-286/13 P, Dole food y Dole Fresh Fruit Europe/Comisión Europea, apartados 149 y C-189/02 P, Dansk Rørindustri y otros/Comisión, apartado 258.
52 Asunto C-41/90, Klaus Höfner y Fritz Elser c. Macrotron GmbH, apartado 21. Véase también, por ejemplo, los asuntos acumulados C-159 y 160/91, Poucet y Pistre c. Assurances Générales de France, apartado 17; asunto C-364/92, SAT Fluggesellschaft mbH contra Eurocontrol, apartado 18; asuntos acumulados C-180 a 184/98, Pavlov y otros, apartado 74; y asunto C-138/11, Compass-Datenbank GmbH c. Republik Österreich, apartado 35.
53 Asunto C-516/15 P, Akzo Nobel y otros/Comisión, apartado 48." (el subrayado es nuestro)

Por todo lo expuesto, se desestima la presente alegación.

IV
Imposición de medidas

De acuerdo con lo previsto en el acuerdo de inicio y en la propuesta de resolución, se ordena a BBVA que en el plazo de 9 meses proceda a adecuar sus procedimientos a la normativa de protección de datos, cumpliendo con el principio de protección de datos desde el diseño en el sistema de detección del fraude de la organización, y la adopción de procedimientos de seguridad de datos personales tanto en la contratación de productos financieros, como en la inclusión y mantenimiento de los datos de los clientes en los sistemas de información crediticia, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…". La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Respecto a la infracción del artículo 25 del RGPD, el reclamado deberá analizar los riesgos, así como establecer las medidas técnicas y organizativas apropiadas de todo tipo necesarias para evitar que, en casos de sustracción o extravío de documentación identificativa o dispositivos de acceso a banca online, puedan realizarse contratación de servicios bancarios y financieros sin el consentimiento del titular de la documentación y dispositivos sustraídos, incluyendo las medidas necesarias para que las comunicaciones realizadas a la entidad por sus clientes por la pérdida, extravío o sustracción del documento de identidad, teléfono o las tarjetas de crédito, produzcan efecto en sus diversos canales de relación con el cliente relativos la operativa que este pueda realizar.

Respecto a la infracción del artículo 32 del RGPD, el reclamado deberá analizar los riesgos, así como establecer las medidas de seguridad necesarias para que no se realicen contrataciones online en nombre del titular de los datos y, por otra parte, que los datos de los clientes sean incluidos en sistemas de información crediticia cuando la deuda es controvertida.

No obstante lo anterior, en el texto de la resolución se establecen cuáles han sido los hechos que determinan la necesidad de adecuación a la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce penamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

De acuerdo con lo señalado, la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **PS/00677/2022**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a **BANCO BILBAO VIZCAYA ARGENTARIA, S.A.** para que en el plazo de nueve meses notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho de la propuesta de resolución transcrita en la presente resolución.

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

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1331-121222

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