- **Expediente N.º: EXP202206311**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: RECLAMACIÓN

Con fecha 10 de mayo de 2022 tuvo entrada en el Registro General de la Agencia Española de Protección de Datos la reclamación de ***A.A.A.*** (en adelante, la parte reclamante), trasladada por el Departamento de Conducta de Entidades del Banco de España, ante el que fue presentada el 10 de febrero de 2022.

La reclamación se dirige contra CAIXABANK, S.A. con NIF A08663619 (en adelante, la parte reclamada, la entidad bancaria o CaixaBank). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante, cliente de CaixaBank, considera que dicha entidad bancaria no respeta las normas relativas a la confidencialidad de los datos de carácter personal. Indica que, en su área personal, en concreto, *en el apartado correspondiente a* ***"(...)"*** figura un documento (de fecha 1 de febrero de 2021) relativo a una transferencia realizada por un tercero a otra persona desconocida (en el que figuran numerosos datos personales, tales como DNI, domicilio postal, número de cuenta bancaria, etc.). A raíz de lo ocurrido, ha presentado una reclamación ante la mencionada entidad bancaria. La parte reclamante manifiesta que CaixaBank no ha respondido en relación con los hechos objeto de la reclamación.

Junto a la reclamación, aporta varias capturas de pantalla en las que figuran justificantes de órdenes de traspaso de marzo de 2021, así como un documento denominado Actualización de datos de fecha 1 de febrero de 2021, copia del documento relativo a la solicitud de emisión de la transferencia controvertida (de fecha 1 de febrero de 2021), e-mail confirmando la recepción de la reclamación efectuada y respuesta de la parte reclamada, de fecha 10 de noviembre de 2021, en la que se indica lo siguiente:

"Nos dirigimos a usted en respuesta a su reclamación, la cual muestra su disconformidad con unos recibos cargados en su cuenta y no autorizados (...). En este sentido, una vez realizadas las comprobaciones oportunas, debemos comunicarle que CaixaBank se limita a cargar los recibos conforme a lo que indica el emisor de la orden de pago. Por lo que deberá dirigirse a la compañía emisora del recibo para solicitarle la orden de domiciliación correspondiente.

Por lo que entendemos que su pretensión ha quedado satisfecha y damos por concluida nuestra actuación en este asunto, (…)".

SEGUNDO: TRASLADO DE LA RECLAMACIÓN

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 08/06/2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 26/07/2022 se recibe en esta Agencia escrito, al que acompaña copia del escrito de 22 de julio de 2022 enviado al reclamante en respuesta a su reclamación, en el que se indica los siguiente:

"Nos ponemos en contacto con usted con la finalidad de atender una reclamación que nos trasladó la Agencia Española de Protección de Datos (…)

En relación a su reclamación en la que manifiesta que ***(…)*** *figura un documento, de fecha 1 de febrero de 2021, que no se corresponde a ninguna operativa por Usted realizada, cúmplenos informarles lo siguiente:*

(i) En la fecha indicada (1 de febrero de 2021), consta que Usted realizó la siguiente operativa (Documento nº1):

(…)

(…).

(…).

(…).

TERCERO: ADMISIÓN A TRÁMITE DE LA RECLAMACIÓN

Con fecha 10 de agosto de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: ACTUACIONES PREVIAS DE INVESTIGACIÓN

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

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

CAIXABANK, S.A. con NIF A08663619 con domicilio en ***DIRECCIÓN.1*** VALENCIA (VALENCIA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Los representantes de la entidad reclamada manifiestan que, de acuerdo con lo indicado por el Reclamante, el ***(…)*** no se correspondía con la operativa realizada. También indican lo siguiente:

(…)

Se ha informado al reclamante por carta enviada por correo certificado con acuse de recibo.(…)"

En relación al resultado del análisis realizado sobre este incidente y si del mismo se ha detectado que pudiera haber una brecha de datos personales que afecte a otros clientes, los representantes de la entidad informan que:

"a) (…):

(…).

b) (…)".

En relación con la brecha de datos personales, los representantes de la entidad aportan la siguiente información:
(…).

(…)

(i) ***(…)***

(ii) ***(…)***

(iii) ***(…)***

(iv) ***(…)***

(…).

Por lo que se refiere a las acciones llevadas a cabo como consecuencia de este suceso concreto fue la ***(…)***

a) ***(…).***
b) ***(…).***
c) ***(…).***
d) ***(…).***
e) ***(…).***

*(…)****.***

(…).

CONCLUSIONES

El hecho de que el reclamante tuviera acceso ***(…)*** a un documento relativo a una transferencia de un tercero (en la que figuran numerosos datos personales de dicho tercero, ordenante de la transferencia, así como del destinatario de la misma, tales como DNI, domicilio postal, número de cuenta bancaria, etc) se debe a una brecha de datos personales ***(…).***

La parte reclamada nos indica que la causa de la brecha está motivada porque dos operaciones (la realizada por el reclamante y por un tercero) ***(…).***

Por este motivo el reclamante podía acceder a un justificante de transferencia realizada por un tercero.

Según consideran ***(…)*** no obstante como solución ***(…).***

Esta brecha de datos personales afectó a la operación que llevó a cabo el Reclamante, que tuvo acceso a datos de terceros (el ordenante y el destinatario de la transferencia). CaixaBank ha realizado un análisis en que indica que esta operación no ha afectado a más clientes.

Del análisis de la información facilitada se desprende que el origen del incidente fue debido a ***(…).***

A cada una de las escasas operaciones que puedan ***(…).***

La forma de solucionar la incidencia, ***(…).***

QUINTO: ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

Con fecha 27 de enero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP):

-Por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD.

- Por la presunta infracción del Artículo 25 del RGPD, tipificada en el Artículo 83.4 del RGPD.

- Por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

SEXTO: COPIA DEL EXPEDIENTE Y AMPLIACIÓN DE PLAZO

Notificado el citado acuerdo de inicio 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), el día 6 de febrero de 2023 la parte reclamada solicitó copia del expediente, así como ampliación de plazo para presentar alegaciones.

El 8 de febrero de 2023, se remitió a la parte reclamada el expediente, concediendo al mismo tiempo un nuevo plazo para presentar alegaciones.

SÉPTIMO: ALEGACIONES AL ACUERDO DE INICIO

La parte reclamada presentó escrito de alegaciones al acuerdo de inicio en un escrito de 20 de febrero de 2023 en el que, en síntesis, manifestaba lo siguiente:

CaixaBank considera que acuerdo de inicio está basado en meras conjeturas, parte de una supuesta infracción del artículo 25 del RGPD (falta de privacidad desde el diseño), de la que derivarían la presunta infracción de otros dos artículos del RGPD (5.1 f) y 32)

CaixaBank afirma a lo largo de su escrito de alegaciones que no se ha infringido la normativa de protección de datos personales.

Comienza sus alegaciones interpretando el contenido del acuerdo de inicio, que considera que la entidad ha infringido los artículos 5.1 f), 25 y 32 del RGPD.

De acuerdo con la interpretación de dicha entidad, el acuerdo entiende que la entidad no ha cumplido las obligaciones del principio de protección de datos desde el diseño (artículo 25.1 del RGDP), lo que a su vez habría supuesto una quiebra del principio de confidencialidad y seguridad y habría llevado a una presunta ausencia de medidas de seguridad, técnicas y organizativas que garantizasen la protección del derecho fundamental a la protección de datos personales.

La parte reclamada resalta que todo parte de una concreta reclamación, derivada del hecho de que el ***(…)*** un documento que correspondía a otro cliente de la mencionada entidad bancaria.

Esta circunstancia denunciada trae causa de un error cuya probabilidad, según afirma la entidad financiera, es ***(…)***.

El acuerdo de inicio, parte de las conclusiones del informe de actuaciones previas de investigación, valorando que la entidad financiera no ha llevado a cabo ninguna actuación de privacidad desde el diseño, produciéndose una vulneración del principio de seguridad como consecuencia de la ausencia de medidas de seguridad adecuadas.

En opinión de CaixaBank, la AEPD se basa en meras conjeturas contenidas en el informe de actuaciones previas de investigación, que son traducidas en la supuesta comisión de tres infracciones, sancionadas con un importe total de cinco millones de euros.

1. En opinión de CaixaBank, las imputaciones dirigidas contra la misma son inexactas:

Según afirma la entidad financiera, la AEPD se funda para imputar a dicha entidad la comisión de tres infracciones que serían sancionadas con un total de cinco millones de euros en:

- (…).

- (…).

- (…).

(…).

a. En relación con la probabilidad de reiteración del incidente:

Las conclusiones del informe de actuaciones previas de investigación consideran ***(…).***

Según indica CaixaBank:

"Como indicó mi representada en respuesta al requerimiento efectuado por esa AEPD ***(…).***

A continuación, la entidad financiera destaca que en el supuesto objeto de la reclamación no solo se produjo la ***(…).***

La entidad financiera resalta que la AEPD considera que la probabilidad de que este hecho se reitere en el tiempo (destaca que no se ha indicado con qué periodicidad ni el grado de concurrencia) es *"razonable"*, ***(…).***

A continuación, realiza una serie de cálculos que llevan a concluir que, según dicha entidad financiera, la probabilidad de reiteración del incidente sería ***de (…).*** Asimismo, afirma que ***(…).***

CaixaBank aporta su corpus normativo en materia de seguridad. Circunstancia que, en opinión de dicha entidad bancaria, acredita el cumplimiento del principio de privacidad desde el diseño.

b. En relación con la ***(…)***:

El Inspector concluye en su informe de actuaciones previas de investigación que ***(…).***

La entidad financiera indica:

"La conclusión, siempre en condicional, alcanzada por el Inspector, parece ser la de que si en un caso concreto ***(…)****, lo que permite al Acuerdo de Inicio extraer la consecuencia de que las medidas adoptadas por CAIXABANK no resultan ajustadas a la normativa de protección de datos personales."*

(…).

(…).

CaixaBank entiende que la documentación aportada acredita ***(…).***

c. En relación con la medida adoptada para solucionar el incidente:

CaixaBank critica que la AEPD califique la solución adoptada una vez detectada la incidencia como un *"mero parche".*

Destaca que el acuerdo de inicio pasa de la posibilidad (reflejada en las conclusiones del informe de actuaciones previas de investigación) de que la solución adoptada no fuera suficiente a considerarla de forma taxativa *"poco satisfactoria"* e incapaz de resolver el problema indicado.

Según la entidad bancaria, dicha conclusión resulta gratuita, dado que la solución adoptada ***(…).***

A continuación, CaixaBank concluye que no será posible que vuelva a producirse la incidencia.

Según la entidad financiera ***(…)*** fue la solución y no un "mero parche". Afirmando a continuación:

"(…) (…)".

Aporta el documento ***(…).***

Concluyendo que, en su opinión, la solución adoptada resuelve de forma definitiva el problema.

Asimismo, destaca que las conjeturas que sirven de fundamento al acuerdo de inicio no resultan, en su opinión ajustadas a la realidad de los hechos y la documentación presentada demuestra que son inexactas.

2. Según la entidad financiera, la interpretación efectuada por la AEPD afecta a varios principios del derecho sancionador:

En su opinión:

"(…) el Acuerdo de Inicio considera (i) que mi mandante no ha adoptado desde el diseño medidas técnicas y organizativas adecuadas; (ii) que mi representada no ha adoptado tales medidas; y (iii) que no se cumple el principio de seguridad, por no haberse adoptado las citadas medidas."

a. Presunta vulneración del principio non bis in idem:

En opinión de CaixaBank, en el acuerdo de inicio, la AEPD ha considerado que en este caso se ha producido una insuficiencia de medidas de seguridad, lo que implicaría una triple vulneración del RGPD:

- No se habrían adoptado las medidas técnicas y organizativas adecuadas (art 32.1 del RGPD).
- La ausencia o insuficiencia de dichas medidas, conduce a apreciar que CaixaBank no habría cumplido las exigencias derivadas del artículo 25.1 del RGPD.
- Se habría vulnerado el artículo 5.1 f) del RGPD, del que el artículo 32 del RGPD no es sino una mera concreción.

A continuación, analiza diversas concurrencias, que, según su opinión, se producen:

Concurrencia de los artículos 5.1 f) y 32 del RGPD:

Para ello reproduce varios extractos del acuerdo de inicio. A continuación, concluye que, en su opinión, el mencionado acuerdo impone dos sanciones diferentes como consecuencia de unos mismos hechos: la carencia de medidas de seguridad. Produciéndose una reiteración sancionadora, proscrita por el derecho administrativo sancionador.

Afirma que, de seguirse el criterio mantenido por la AEPD en el acuerdo de inicio, cualquier vulneración de un precepto del RGPD implicaría la comisión no solo de la infracción de dicho precepto, sino la del principio de protección de datos del que la norma vulnerada trajera causa.

Concurrencia de los artículos 25 y 32 (y 5.1 f) del RGPD:

CaixaBank reproduce un extracto para ilustrar una supuesta reiteración sancionadora en relación con las imputaciones del artículo 25 y del artículo 32.

A continuación, destaca que teniendo en cuenta el alcance del cumplimiento del principio de privacidad desde el diseño según la AEPD y el Comité Europeo de Protección de Datos, si se siguiera el razonamiento reflejado en el acuerdo de inicio cualquier vulneración de la normativa de protección de datos por parte de un responsable conllevaría necesariamente la vulneración del principio de protección de datos desde el diseño.

Según CaixaBank, salvo en aquellos supuestos en los que quepa apreciar que se ha prescindido del cumplimiento de las obligaciones establecidas en el artículo 25, la san-

ción simultánea de unos hechos por considerar inadecuadamente cumplido uno de los principios del artículo 5 del RGPD y por vulneración del artículo 25 del RGPD, implicaría una vulneración del principio de non bis in idem.

CaixaBank concluye afirmando que en el acuerdo de inicio la AEPD considera que un mismo hecho (supuesta insuficiencia de medidas de seguridad que han generado un incidente específico y concreto), sería constitutivo de tres infracciones del mismo bien jurídico protegido: la adecuada garantía de los derechos y libertades de los interesados.

Se estaría sancionando, por una parte, la ausencia de las medidas que la AEPD considera necesario adoptar ***(…)***, el incumplimiento del principio de seguridad (que exige la adopción de tales medidas) y, finalmente, el que dichas medidas no fueran adoptadas desde el diseño del tratamiento.

El acuerdo de inicio emplea una argumentación similar a la hora de razonar la supuesta comisión de las tres infracciones y son similares las circunstancias que la AEPD ha considerado concurrentes en los tres supuestos (fundamentos de derecho VI, IX y XII).

La entidad bancaria entiende que la conducta sancionada es la misma y el hecho sancionado también. Afirma que pretende sancionarse la ausencia de la medida, la falta de planificación de la misma y el resultado producido.

Concluye que concurriría una triple identidad de sujeto, hecho y bien jurídico protegido, debiendo aplicarse el principio de non bis in idem (o non ter in idem). En su caso, procedería imponer una sola de las tres sanciones (artículo 32 RGPD).

b. Subsidiariamente, existencia de concurso medial entre las tres conductas imputadas:

En opinión de CaixaBank cada una de las tres infracciones supuestamente cometidas se encontraría subsumida y embebida en las otras, dando lugar a un concurso medial (artículo 29.5 Ley 40/2015, de 1 de octubre).

Considera que no puede sancionarse a dicha entidad por todas las infracciones, dado que la comisión de la supuesta infracción del artículo 25.1 el RGPD implicaría necesariamente la comisión de la infracción del artículo 32.1 del RGPD, dando lugar este último incumplimiento a la supuesta vulneración del artículo 5.1 f) del RGPD.

La entidad bancaria entiende que se estaría imponiendo una triple sanción por unos mismos hechos. A continuación, afirma:

"(…) la falta de aplicación de las medidas a las que se refiere el artículo 32.1, y por ende la supuesta infracción del artículo 5.1 f) traería necesaria e inseparablemente causa de la supuesta 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, su falta de aplicación y el principio mismo que la adopción de esa medida pretende proteger, 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.

Por ello, o bien se están sancionado triplemente unos mismos hechos o bien dos de las infracciones sólo pueden ser, necesariamente, consecuencia de la primera"

A continuación, cita la Sentencia 339/2015 de 25 de septiembre de 2015 de la Audiencia Nacional (rec. 262/2014), que a su vez cita la Sentencia del Tribunal Supremo de 8 de febrero de 1999 (rec.9/1996).

CaixaBank concluye que en el supuesto de que se entienda que se han cometido las infracciones mencionadas en el acuerdo de inicio, resultaría de aplicación el artículo 29.5 de la LRJSP, de forma que todas las infracciones deberían subsumirse en aquella de la que las restantes traen causa.

3. Sobre el supuesto incumplimiento de las obligaciones de protección de datos desde el diseño:

CaixaBank afirma que no ha vulnerado el artículo 25 del RGPD.

a. Alcance del principio de protección de datos desde el diseño:

La entidad bancaria hace referencia a las Directrices 4/2019 del Comité Europeo de Protección de Datos, reproduciendo parte de las mismas para concluir:

"(…) el EDPB concibe la Privacidad desde el Diseño como un proceso holístico, que comprende la evaluación de todos y cada uno de los aspectos del tratamiento, a fin de garantizar el cumplimiento de los principios y garantías establecidos en el artículo 5 del RGPD. De este modo, sólo en caso de que las autoridades de control pudieran apreciar que un responsable del tratamiento no ha llevado a cabo ese proceso, en toda su extensión, o únicamente lo han desarrollado como mero formalismo, sin aplicar el proceso al tratamiento concreto de datos personales objeto de análisis, cabría apreciar el incumplimiento de lo dispuesto en el artículo 25.

Es decir, la obligación de cumplimiento del artículo 25.1 del RGPD no es concebida por el EDPB como una obligación de resultado, en el sentido de que pueda considerarse que los resultados derivados de su realización sean conformes con lo establecido en el RGPD, sino como una obligación de análisis, de forma que si un responsable del tratamiento ha llevado adecuadamente a cabo el mismo, aun cuando el resultado pudiera ser erróneo a juicio de la autoridad de control, no existiría una vulneración del principio de Privacidad desde el Diseño, sino, en su caso, de alguno de los principios establecidos en el artículo 5 del RGPD o de las normas en que dichos principios se concretan.

Por decirlo gráficamente, y como ya se ha apuntado anteriormente, es posible que de la realización del análisis del tratamiento efectuado por un responsable se derive un alcance del cumplimiento del deber de transparencia que posteriormente no sea considerado suficiente por parte de la autoridad de control, entendiendo ésta que la información facilitada a los interesados no es la suficiente. Sin embargo, ello no implicaría que la entidad en cuestión no hubiera cumplido su obligación de adoptar las medidas necesarias para el cumplimiento del principio de transparencia, sino que dicho principio no se consideraría por la AEPD respetado plenamente. Es decir, el resultado de esa apreciación sería una vulneración de los artículos 5.1 a), 13 y 14 del RGPD, pero no una vulneración de su artículo 25. No cabría sancionar la falta de privacidad desde el diseño, sino el supuesto incumplimiento del principio o de la norma en que se concreta.

Y esta circunstancia es la que concurre en el presente caso: mi mandante ha analizado y valorado plenamente todas las medidas que correspondía adoptar para garantizar el cumplimiento de los principios establecidos en el artículo 5 del RGPD.

Cuestión distinta, negada por mi representada, será que la AEPD aprecie que una de las medidas de seguridad adoptadas por mi mandante es insuficiente. En ese caso podrá apreciarse que no se han adoptado las medidas adecuadas, pero en ningún caso esa supuesta insuficiencia podrá considerarse como un incumplimiento de lo preceptuado por el artículo 25.1 del RGPD."

b. Contenido del acuerdo de inicio:

Según CaixaBank el fundamento de derecho VII del acuerdo de inicio expone, de forma meramente aparente, los motivos por los cuales la AEPD entiende que dicha entidad no ha dado cumplimiento al principio de privacidad desde el diseño.

Estima que es meramente aparente, ya que dicho fundamento consiste única y exclusivamente en una descripción de lo que a juicio de la AEPD debe considerarse el principio de protección de datos desde el diseño.

A continuación, reproduce extractos del fundamento de derecho VII.

En opinión de CaixaBank, el acuerdo de inicio parece dar a entender que dicha entidad no ha llevado a cabo ningún tipo de actividad en que haya valorado lo riesgos para los derechos y libertades que podrían derivarse del ***(…)*** en relación con el cual se produjo el incidente.

Por otra parte, una vez detectada la brecha, la medida adoptada, consistente en ***(…)***, es considerada *"un mero parche".*

Todo ello, según CaixaBank, lo razona la AEPD sobre la única y exclusiva base de las conclusiones del informe de actuaciones previas de investigación, que dicha entidad considera haber desvirtuado mediante la documentación aportada junto al escrito de alegaciones.

CaixaBank considera que dicha entidad no ignoró los riesgos que se generaban como consecuencia de ***(…)***, que la medida adoptada no es un *"mero parche"* que no resolviera de forma definitiva la incidencia

Según dicha entidad financiera:

"De este modo, no resulta posible, como se pretende por el Acuerdo de Inicio, considerar que mi mandante no tuvo presente en ***(…)*** *y en el momento posterior a la brecha de seguridad,* ***(…)*** *que minimizasen el impacto o los riesgos que el tratamiento de los datos podría generar en los derechos de los interesados y, particularmente, en su derecho a la protección de datos personales."*

CaixaBank concluye que en el supuesto analizado no se ha producido quiebra alguna de las obligaciones de protección de datos desde el diseño exigibles a CaixaBank. Dicha entidad ha desarrollado una *"amalgama de normas internas y procedimientos"* encaminados al cumplimiento de dicho objetivo, aportados junto con su escrito de alegaciones al acuerdo de inicio.

4. Sobre la supuesta vulneración del artículo 32 del RGPD:

CaixaBank reproduce un extracto del fundamento de derecho X, que según su punto de vista, incurre nuevamente en el maximalismo de entender que producido un incidente cuya probabilidad de concurrencia es prácticamente inexistente, dicha circunstancia determina que la referida entidad no ha adoptado medidas de seguridad sufi-

cientes para preservar los derechos de los interesados y garantizar la confidencialidad y disponibilidad de los datos.

A continuación, dicha entidad bancaria afirma:

"De este modo, la AEPD en el Acuerdo vincula el supuesto incumplimiento de lo dispuesto en el artículo 32 con la producción del resultado que desafortunadamente se produjo como consecuencia de la concurrencia de una serie de factores que, como se ha indicado, resultaban imprevisibles.

Y en este punto, respetuosamente considera CAIXABANK 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. Es decir, la apreciación de la existencia de medidas de seguridad en este caso no depende, como parece hacer depender el Acuerdo de Inicio, del hecho de que se haya producido o no un incidente de seguridad, sino de la existencia de dichas medidas y la realización de actuaciones por mi representada encaminadas a su determinación."

Posteriormente, hace referencia a la Sentencia del Tribunal Supremo de 15 de febrero de 2022 (recurso de casación: 7359/2020) que señala que la obligación impuesta por la normativa de protección de datos personales, de adoptar medidas técnicas y organizativas encaminadas a garantizar la confidencialidad, disponibilidad e integridad de la información, es una obligación de medios y no de resultado y reproduce parte de su fundamento de derecho tercero.

CaixaBank estima que el expediente sancionador debería ser archivado, ya que las premisas sobre las que se apoya la AEPD para considerar que se ha producido una supuesta vulneración del artículo 32 del RGPD decaen ante la realidad de los hechos.

Insiste en que el acuerdo de inicio sustenta su reproche en dos de las conclusiones del informe de actuaciones previas de investigación (***(…)***) lo que, según la interpretación de CaixaBank, conducía a la pretensión de que ***(…).***

La entidad bancaria afirma que ambas conclusiones han sido desmontadas en el escrito de alegaciones y gracias a la documentación aportada junto al mismo.

Critica que el acuerdo de inicio afirme categóricamente que CaixaBank no contaba con unas medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo ***(…).***

A continuación, insiste una vez más en una posible vulneración del principio de non bis in idem.

5. Sobre la supuesta vulneración del principio de seguridad:

Según la interpretación de CaixaBank, el fundamento de derecho V del acuerdo de inicio funda su reproche en relación con una supuesta vulneración del artículo 5.1f) del RGPD en tres argumentos que, en la práctica, pueden resumirse en dos:

"En primer lugar, se indica que la conducta es sancionable porque el incidente "ha revelado un problema que afectaba al diseño ***(…)****". Y ello conduce al Acuerdo a añadir:*

"(…)."

Así, concluye el citado fundamento de derecho indicando que "lo que en principio parecía una brecha de confidencialidad, va más allá al ser también una brecha de disponibilidad. Pero, además, lo que se ha comprobado a partir de las actuaciones previas de investigación es que ***(…)".***

CaixaBank afirma haber acreditado en su primera alegación que ninguna de las circunstancias que el acuerdo de inicio considera evidentemente ocurridas han tenido lugar.

1. Existe una única reclamación.

2. La solución dada por la entidad el ***FECHA.1 no puede ser calificada como un *"mero parche",* dado que resulta imposible la repetición del mismo ***(…).***

3. No existe una vulneración del principio de seguridad como pretende la AEPD.

Vuelve a insistir en la vulneración del principio de non bis in idem.

A continuación, CaixaBank niega que en el caso analizado se haya producido una brecha de disponibilidad, añadiendo:

"(…)."

Cita dos documentos aportados junto al escrito de alegaciones al acuerdo de inicio.

CaixaBank vuelve a insistir en la conveniencia de archivar el procedimiento sancionador.

6. Sobre la supuesta vulneración del principio de proporcionalidad:

Subsidiariamente, hace referencia a que dicho principio ha de ser tenido en consideración a la hora de determinar la sanción a imponer.

Hace referencia al contenido de la Sentencia del Tribunal Supremo de 20 de noviembre de 2001 (recurso de casación: 7686/1997) en relación con el principio de proporcionalidad.

En opinión de CaixaBank, la AEPD debe valorar que nos encontramos ante una sola reclamación formulada por un solo cliente de CaixaBank, no referida a sus propios datos, sino a los de un tercero, relacionada con un supuesto determinado y concreto: el acceso a un documento ajeno al reclamante. Dos de las infracciones establecidas por el RGPD para la conducta mencionada son de las incluidas en el artículo 83.4.

La entidad financiera destaca que la AEPD no duda en imponer a dicha entidad tres sanciones, subsumibles unas en otras, por una cuantía total de cinco millones de euros, acudiendo para determinar el importe de la misma a criterios, en su opinión, completamente genéricos, que rechaza de plano.

Además, los criterios utilizados para la agravación de una de las infracciones son literalmente reproducidos en las demás, concluyendo que los argumentos resultan perfectamente intercambiables entre los fundamentos de derecho VI, IX y XII.

a. Respecto a la supuesta gravedad de la conducta:

CaixaBank afirma que el acuerdo de inicio toma en consideración en los fundamentos de derecho VI, IX y XII, tres elementos esenciales que considera concurrentes para la agravación de la conducta:

*1. La AEPD aprecia que nos encontramos ante **(…):***

Dicho reproche sería, según interpreta el acuerdo de inicio CaixaBank, la justificación esencial de la imputación que se realiza por la supuesta vulneración del artículo 25.1 del RGPD.

La entidad financiera afirma que la identificación de un supuesto *fallo **(…)*** no solo es constitutivo de uno de los tipos sancionadores, sino que agrava la responsabilidad en los otros dos (vulneración del principio non bis in idem).

2. Prolongación del incidente en el tiempo:

La entidad financiera destaca que no consigue determinar si el acuerdo de inicio hace referencia a la brecha de datos personales objeto de la reclamación ***(…).***

3. Afectación potencial del incidente a todos los clientes de CaixaBank:

Considera inadmisible la referencia que efectúa el acuerdo de inicio a las Directices 4/2022 del Comité Europeo de Protección de Datos.

b. Supuesta negligencia en la actuación de CaixaBank:

Destaca que el acuerdo de inicio prácticamente reproduce los motivos que justifican la aplicación de esta agravante, volviendo a hacer referencia a la íntima conexión, que desde su punto de vista, existe entre las tres infracciones.

1. La AEPD considera que la solución aplicada para resolver la incidencia era un "mero parche":

CaixaBank afirma haber acreditado que la ***(…)*** no era una solución temporal, sino definitiva, que evitaba que la incidencia pudiera volver a producirse.

La entidad financiera destaca que la solución de la incidencia se produjo en un breve plazo desde el momento en el que se produjo el incidente, ya que ***(…).***

Según CaixaBank el hecho reflejado en el párrafo anterior impide que puedan ser admitidos los argumentos que vinculan la supuesta negligencia en la actuación de la entidad bancaria con la duración temporal de la infracción. Además, dicha circunstancia ya se aprecia como agravante en el apartado relativo a la naturaleza y gravedad de la infracción.

c. Vinculación de la actividad de CaixaBank con la realización de tratamientos de datos:

La entidad bancaria considera que el acuerdo de inicio reproduce literalmente en la motivación de los fundamentos de derecho VI, IX y XII que la sanción debe agravarse como consecuencia de la vinculación de CaixaBank con la realización de tratamientos de datos.

El acuerdo de inicio considera dicha circunstancia para reforzar la potencial afectación a los hechos y, posteriormente, se agrava la conducta desde el punto de vista de la supuesta negligencia y, finalmente, se considera que es en sí otra agravante, lo que supone una triple agravación derivada de un mismo hecho.

Según destaca, a juicio de la AEPD, cuando una entidad financiera comete una supuesta infracción su conducta ha de verse triplemente afectada por el mero hecho de

que pertenezca al sector financiero, lo que difícilmente puede considerarse acorde al principio de proporcionalidad.

CaixaBank concluye que la imposición de tres sanciones de la cuantía reflejada en el acuerdo de inicio solo puede considerarse desproporcionada y vulneradora del principio de proporcionalidad, especialmente si se tiene en cuenta que se fundan en la detección de un solo incidente.

Finalmente, CaixaBank solicita el archivo del procedimiento sancionador o, subsidiariamente, la imposición de una advertencia o apercibimiento o una reducción significativa de la cuantía establecida Enel acuerdo de inicio.

Asimismo, invoca la confidencialidad y el secreto empresarial de los documentos aportados.

OCTAVO: PERIODO DE PRÁCTICA DE PRUEBA

Con fecha 7 de junio de 2023 se acuerda abrir un periodo de práctica de prueba.

Se acuerda, asimismo:

- Dar por reproducidos, a efectos probatorios, la reclamación interpuesta por D. ***A.A.A.*** y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, así como los obtenidos y generados durante la fase de actuaciones previas de investigación y el informe de actuaciones previas de investigación, que forman parte del procedimiento ******PROCEDIMIENTO.1.***

- Dar por reproducido, a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por CAIXABANK, S.A., y la documentación que a ellas acompaña.

Se practican las siguientes diligencias de prueba:

a. Ante la reclamada:

Práctica de prueba I:

1. En el mismo escrito de fecha 7 de junio de 2023 en el que se comunica la apertura de un periodo de práctica de prueba, se requiere que remita la siguiente información y documentación en relación con la brecha de datos personales, que ha permitido la visualización por parte del reclamante del comprobante de una transferencia realizada por un tercero en el ***apartado correspondiente a (…):***

> - Indicar la fecha en la que CaixaBank determinó la causa de la brecha de datos personales, que ha permitido que ***(…).*** Aportar acreditación documental fechada y firmada.
>
> - Indicar la fecha en la que ***(…).*** Aportar acreditación documental fechada y firmada.
>
> -Aportar el documento que visualizaba el ordenante de la transferencia (…).

- En el escrito de esa entidad de fecha 13 de diciembre de 2022, remitido tras un requerimiento del inspector, se indicaba:

"(…)."

Aportar certificado fechado y firmado acreditativo de toda la información contenida en el registro de incidentes de CaixaBank relativa a la brecha de datos personales por la que el reclamante visualizó el comprobante de la transferencia realizada por otro cliente de esa entidad bancaria, así como el informe que sobre dicha brecha elaboró dicha entidad bancaria fechado y firmado.

Asimismo, aportar la primera comunicación fechada y firmada dirigida al Delegado de Protección de Datos de esa entidad bancaria relacionada con la brecha de datos personales analizada en este expediente y a la que se hace referencia en el párrafo anterior.

- En relación con el sistema ***(…)***, que, según su escrito de 13 de diciembre de 2022 de esta entidad financiera, ***(…)***, indicar y acreditar el periodo de tiempo (previo al ******FECHA.1***) durante el cual estuvo ***(…)***.

- Indicar detalladamente qué sucede una vez que ***(…)*** aportado por esta entidad financiera junto con su escrito de alegaciones. Una vez que el cliente visualiza ***(…)***.

- Indicar la causa por la que esa entidad bancaria decidió ***(…)***. Aportar documento fechado y firmado donde se refleje que la desactivación se produjo en dicha fecha y la causa por la que se decidió llevar a cabo dicha desactivación.

- Indicar si como consecuencia de la brecha de datos personales, que permitió al reclamante tener acceso al comprobante de una transferencia realizada por otro cliente de esa entidad bancaria, se ha llevado a cabo por parte de esa entidad alguna medida diferente (…). En caso de respuesta afirmativa, aportar:

1. Descripción de la medida llevada a cabo.
2. Fecha en la que se realizó dicha medida
3. Aportar documentación fechada y firmada que acredite dicha medida.

- Indicar si esa entidad, a partir de la fecha en la que detectó la brecha de datos personales analizada, ha llevado a cabo alguna medida destinada a ***(…).*** En caso afirmativo:

1. Descripción de la medida llevada a cabo.

2. Fecha en la que se adoptó dicha medida

3. Aportar documentación que acredite la medida adoptada fechada y firmada

- Indicar si se ha llevado a cabo por parte de dicha entidad bancaria, a partir de la fecha en la que detectó la brecha de datos personales analizada, alguna medida destinada a ***(…).***

1. Descripción de la medida llevada a cabo.
2. Fecha en la que se adoptó dicha medida.
3. Aportar documentación que acredite la medida adoptada fechada y firmada.

- Aportar los análisis de riesgos y las definiciones de requisitos de seguridad (…)***,*** que estuvieron involucrados en la brecha de datos personales que está siendo analizada en este expediente, en lo que a la brecha, que ha permitido al reclamante visualizar el comprobante de la transferencia realizada por otro cliente, se refiere (se solicitan los elaborados antes del 1 de febrero de 2021 y, en su caso, los elaborados con posterioridad a dicha fecha). Los documentos habrán de presentarse fechados y firmados y en el caso de haber distintas versiones, aportar todas ellas.

- En el documento ***(…)*** se indica:

Artículo 1. (…)
(…)
b) (…).

Acreditar documentalmente los mecanismos que había implantados en ***(…).***

- Indicar la causa por la que dicha entidad realizó dos ***(…)*** en fechas tan próximas ***(…).*** En el supuesto de haber realizado otro u otros ***(…)*** desde el 1 de febrero de 2021 hasta la actualidad, aportarlos fechados y firmados.

- (…).

- Aportar, fechados y firmados, los siguientes documentos en la versión vigente en esa entidad bancaria a fecha 1 de febrero de 2021:

(…).

(…).

(…). (En este caso, aportar, en su caso, el documento que sobre esta misma materia estuviera vigente a fecha 1 de febrero de 2021).

(…).

2. Con fecha 13 de junio de 2023 se recibió una solicitud de CaixaBank de ampliación del plazo conferido para la práctica de la prueba I en 5 días hábiles adicionales, concediéndose la ampliación de plazo solicitada.

3. El día 28 de junio de 2023 se recibió un escrito de CaixaBank en respuesta a la solicitud de prueba de 7 de junio de 2023, acompañado de diversa documentación.

Práctica de prueba II:

1. Examinada la documentación presentada por CaixaBank, el 10 de julio de 2023 se requiere a CaixaBank para que remita la siguiente información y documentación:

> - Copia de la reclamación presentada por D. ***A.A.A.*** (el reclamante) en la oficina de atención al cliente de CaixaBank el 31 de octubre de 2021 *registrada* ***(…)***, junto con la documentación, que en su caso la acompañase.
>
> - En relación con los ***DOCUMENTOS (…),*** certificado fechado y firmado en el que se indique la fecha ***(…).***
>
> - Certificado fechado y firmado en el que se indique el dato/s modificado/s por D. ***A.A.A.*** (el reclamante) el 1 de febrero de 2021 al realizar la actualización de datos de contacto.
>
> - En el escrito de esa entidad financiera de 28 de junio de 2023 se indica que el ***FECHA.1 ***(…).***
>
> - En el escrito de apertura del periodo de práctica de pruebas se requería:
>
> ***"(…)"***
>
> ***(…):***
>
> ***"****En primer lugar, es preciso señalar lo siguiente:*
>
> ***i) (…)***
>
> ***ii) (…).***
>
> ***(…)."***
>
> En el escrito de 13 de diciembre de 2022, elaborado por esa entidad bancaria en contestación a un requerimiento de información del inspector, se afirmaba: (el subrayado es nuestro)
>
> ***"PLAN DE ACCIÓN Y ELIMINACIÓN DE RIESGO***
>
> ***(…)."***
>
> Por otra parte, en el escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023 esa entidad financiera destacaba: (el subrayado es nuestro).

"(…)."

A la vista de los extractos de los escritos de esa entidad financiera que acaban de ser reproducidos, se solicita que se aporte un escrito fechado y firmado en el que se aclare ***(…).***

- En el escrito de 13 de diciembre de 2022, elaborado por esa entidad financiera en contestación a un requerimiento de información del inspector, figura la siguiente información:

"(…)."

A la vista de la documentación remitida por esa entidad financiera, aclarar *si la información* ***(…).***

Asimismo, aclarar *si la información* ***(…).***

2. Con fecha 14 de julio de 2023 se recibió una solicitud de CaixaBank de ampliación del plazo conferido para la práctica de la prueba II en 3 días hábiles adicionales.

Con esa misma fecha se remitió a la parte reclamada un escrito en el que se comunicaba que se acordaba no ampliar el plazo para aportar la documentación e información requeridas en la práctica de pruebas II en tres días hábiles adicionales, dado que con dicho plazo adicional se superaría el plazo de 30 días para la apertura del período de prueba contemplado en el artículo 77.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

3. El día 18 de julio de 2023 se recibió un escrito de CaixaBank en respuesta a la solicitud de prueba de 10 de julio de 2023, acompañado de diversa documentación.

Práctica de prueba III:

1. Examinado el ***contenido del documento (…)***, el 12 de julio de 2023 se requiere a CaixaBank para que remita certificado fechado y firmado en el que se acredite:

- (…).

- (…).

2. Con fecha 14 de julio de 2023 se recibió una solicitud de CaixaBank de ampliación del plazo conferido para la práctica de la prueba III en 1 día hábil adicional.

Con esa misma fecha se remitió a la parte reclamada un escrito concediendo la ampliación de plazo solicitada.

3. El día 18 de julio de 2023 se recibió un escrito de CaixaBank en respuesta a la solicitud de prueba de 12 de julio de 2023.

b. Ante la Inspeccion de la AEPD:

1. Con fecha 17 de julio de 2023 se remite al Coordinador de la Inspección una nota interior en la que se indica lo siguiente:

"(…) El día 28 de junio de 2023 se recibió un escrito aportado por CAIXABANK, S.A., cuya copia se acompaña, ***(…):***

"(…)"

Se solicita, que la vista de la información aportada por CAIXABANK, S.A. en este expediente, elabore, con carácter urgente, informe acerca de la probabilidad de que se produjera ***(…).***

Asimismo, se solicita que indique si ese cálculo de probabilidad se podría aplicar al número o ***(…)****."*

2. El día 18 de julio de 2023 se recibe un informe del Inspector solicitado por la instructora en el marco de la práctica de la prueba, cuyo contenido se reproduce a continuación:

"INFORME SOLICITADO POR LA INSTRUCTORA DEL PS/00020/2023 EN EL MARCO DE LA PRÁCTICA DE LA PRUEBA

ANTECEDENTES

Fecha de entrada de la reclamación: 10 de mayo de 2022
Reclamante: ***A.A.A.*** *(en adelante, la parte reclamante)*
Reclamado: ***CAIXABANK, S.A.*** *(en adelante, la parte reclamada)*
Hechos según manifestaciones de la parte reclamante:
La parte reclamante es cliente de la parte reclamada. Manifiesta que, ***(…)****, en concreto,* ***(…)****" figura un documento (de fecha 1 de febrero de 2021) relativo a una transferencia de un tercero (en la que figuran numerosos datos personales de dicho tercero, tales como DNI, domicilio postal, número de cuenta bancaria, etc) realizada a otra persona desconocida.*

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

CAIXABANK, S.A. con NIF A08663619 con domicilio en ***DIRECCIÓN.1*** *VALÈNCIA (VALENCIA)*

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

- *En relación a la* ***(…)****, los representantes de la entidad informan que (…)*

Facilitan además que en el momento ***(…)****, esto implica* ***(…)***

(…)

- ***(…):***

(…).

(…).

Hay que tener en cuenta que los valores de probabilidad dan el valor medio lo que implica que, aunque el sistema tiene **(…).**

(…).

CONCLUSIONES

(…).

B.B.B.
INSPECTOR "

3. Con fecha 18 de julio de 2023 se elabora una diligencia que da por reproducido, a efectos probatorios, el informe de la misma fecha elaborado por el inspector, cuyo contenido ha sido reflejado en el apartado anterior.

OCTAVO: PROPUESTA DE RESOLUCIÓN

Con fecha 19 de septiembre de 2023 se formuló propuesta de resolución, proponiendo:

"PRIMERO: Que por la Directora de la Agencia Española de Protección de Datos se sancione a CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 5.1.f) del RGPD tipificada en el artículo 83.5.a) y calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD, con una multa de 2.000.000 € (dos millones de euros).

SEGUNDO: Que por la Directora de la Agencia Española de Protección de Datos se sancione a la entidad CAIXABANK, S.A, por una infracción del Artículo 25 del RGPD, tipificada en el artículo 83.4 a) y calificada como grave a efectos de prescripción en el artículo 73 d) de la LOPDGDD, con una multa de 1.500.000 € (un millón quinientos mil euros).

TERCERO: Que por la Directora de la Agencia Española de Protección de Datos se sancione a la entidad CAIXABANK, S.A, por una infracción del Artículo 32 del RGPD, tipificada en el artículo 83.4 a) y calificada como grave a efectos de prescripción en el artículo 73 f) de la LOPDGDD, con una multa de 1.500.000 € (un millón quinientos mil euros).

CUARTO: Que por la Directora de la Agencia Española de Protección de Datos se proceda a requerir a CAIXABANK, S.A., que en virtud del artículo 58.2.d) del RGPD, implante las medidas correctoras necesarias para adecuar su actuación a la normativa

de protección de datos personales en el plazo que se determine, así como que informe a esta Agencia en el mismo plazo sobre las medidas adoptadas."

NOVENO: ALEGACIONES A LA PROPUESTA DE RESOLUCIÓN

Notificada la propuesta de resolución conforme a las normas establecidas en la LPACAP, la parte reclamada presentó escrito de alegaciones a la propuesta de resolución el 6 de octubre de 2023, en el que, en síntesis, manifesta lo siguiente:

CaixaBank reitera la totalidad de las alegaciones formuladas al acuerdo de inicio en su escrito de 20 de febrero de 2023.

En opinión de la entidad bancaria, la propuesta de resolución reitera lo que ya había sido argumentado por la AEPD en el acuerdo de inicio, argumentación que consideran errónea, sin atender a lo alegado por CaixaBank.

CaixaBank expone los motivos por los que, en su opinión, debería procederse al archivo del expediente:

I. La entidad bancaria estima que la propuesta de resolución realiza una serie de consideraciones inexactas:

1.La parte reclamada considera que dicha propuesta parte de un informe elaborado por el Inspector el 18 de julio de 2023, aportado junto con dicha propuesta, en el que se calcula *la probabilidad de concurrencia de los hechos* que dieron lugar a la brecha de datos personales analizada en el presente expediente.

En relación con dicho informe, CaixaBank considera que:

a. La metodología utilizada carece del adecuado rigor científico.

b. No tiene en cuenta que ***(…).***

c. Los datos utilizados (…) (fecha en la que se produjo la brecha de datos personales objeto del expediente), ***(…)***. En esa fecha, (…) y la entidad bancaria afirma que no podía producirse una brecha de datos personales.

d. La probabilidad calculada sería ***(…)***, no la real.

2. La Propuesta de resolución obvia que la ***(…)*** era, en opinión de CaixaBank, una medida suficiente para impedir que la brecha de datos personales pudiera volver a producirse.

3. La AEPD establece un concepto de brecha de disponibilidad que no se corresponde con el fijado por la propia AEPD y los órganos competentes en el marco de la Unión Europea.

En opinión de CaixaBank, se equipara a brecha de disponibilidad de datos lo que únicamente es una falta de disponibilidad en un servicio prestado de manera voluntaria a sus clientes (***(…)***).

Asimismo, afirma que el reclamante nunca vio limitada su posibilidad de acceso a dichos datos.

4. La AEPD asimila la solicitud de modificación de los datos de contacto por parte del reclamante con el derecho de rectificación, pero al propio tiempo con-

sidera que el hecho de que el interesado no reciba la acreditación de la modificación realizada hasta **(...)** supone una vulneración de la normativa de protección de datos. A pesar de que dicha normativa establece un plazo de un mes para dar respuesta a la solicitud de rectificación.

5. La AEPD indica, de forma novedosa en la propuesta de resolución, que CaixaBank carece de un procedimiento adecuado para la atención de las reclamaciones de sus clientes en materia de protección de datos, a pesar de disponer únicamente de un caso en el que dicho procedimiento no ha sido cumplido y de no haber requerido a la entidad bancaria sobre la existencia de dicho procedimiento. En opinión de la entidad bancaria, se habría vulnerado la doctrina sentada en la Sentencia de la Audiencia Nacional de 23 de diciembre de 2022, al convertir lo ocurrido en un caso concreto en una vulneración sistemática.

II. CaixaBank insiste en que la propuesta vulnera el principio non bis in idem.

III. La parte reclamante vuelve a destacar que, en su opinión, existe un concurso medial entre las tres infracciones imputadas a la entidad bancaria.

En este sentido, destaca que la propuesta efectúa un razonamiento que conduce a considerar que los principios del derecho sancionador y la doctrina del Tribunal Constitucional relativa a la aplicación de las garantías del derecho penal al derecho administrativo sancionador no resultan de aplicación en este caso, por el simple hecho de que dichos principios no se encuentran expresamente recogidos en la normativa de protección de datos.

Asimismo, CaixaBank afirma que la AEPD sienta una doctrina contraria a la previamente adoptada en otras resoluciones en las que había apreciado la concurrencia del concurso medial.

IV. En opinión de la entidad bancaria, ninguna de las tres infracciones contempladas en la propuesta de resolución resulta conforme a derecho.

Artículo 25 del RGPD:

CaixaBank afirma que respeta plenamente el principio de privacidad desde el diseño en toda actuación que conlleva el tratamiento de datos de carácter personal, así como al tramitar reclamaciones dirigidas a dicha entidad por parte de sus clientes o de cualquier interesado.

Considera que las medidas que utiliza (…) son medidas encaminadas a garantizar, desde el diseño, la seguridad de los datos, la integridad de los documentos y evitar los riesgos para los derechos y libertades de los interesados.

Destaca que las medidas sucesivamente adoptadas por CaixaBank no suponen sino la asunción del principio de privacidad desde el diseño y el refuerzo de las garantías de los derechos de los interesados.

Niega que se pueda apreciar la concurrencia de responsabilidad por su parte a partir de supuestas “dudas” en relación con dichas medidas, ya que se vulneraría el principio de presunción de inocencia.

Artículo 32 RGPD:

Considera que el razonamiento sobre la supuesta ausencia de medidas de seguridad parte del cálculo realizado por el Inspector el 18 de julio de 2023.

Artículo 5.1 f):

En opinión de la entidad bancaria, la supuesta vulneración del principio de confidencialidad trae causa, única y exclusivamente, de la ausencia de medidas de seguridad, no sería sino un resultado no querido consecuencia de la adopción por parte de CaixaBank de las medidas de seguridad adecuadas. La parte reclamante considera que se utilizaría esta vía para dejar sin aplicación la doctrina del Tribunal Supremo que considera la obligación de medidas de seguridad como una obligación de medios y no de resultado.

V. CaixaBank afirma haber adoptado las medidas técnicas y organizativas adecuadas para evitar que la brecha de datos personales vuelva a producirse en el futuro.

Asimismo, destaca que la propuesta de resolución se refiere a la necesaria adopción por su parte de medidas correctoras sin especificar cuáles son dichas medidas, lo que implica una clara situación de indefensión para la entidad bancaria.

VI. La parte reclamada insiste de nuevo en la vulneración del principio de proporcionalidad.

Considera que se aplican unas circunstancias que, en su opinión, no concurren en el caso analizado. Además. estima que dichas circunstancias se ven afectadas por el cálculo efectuado por el Inspector.

En opinión de la parte reclamada, la propuesta no tiene en cuenta que la posibilidad de reiteración del incidente es completamente imposible desde hace casi dos años antes de iniciarse el procedimiento sancionador e incluso antes de haberse formulado la reclamación por parte del interesado.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

ÍNDICE DE HECHOS PROBADOS

A los efectos de facilitar la lectura de los hechos probados consignados en la resolución indicaremos que:

- Del hecho probado primero al hecho probado vigésimo octavo se consignan los hechos probados referidos a la reclamación presentada por el reclamante.
- Del hecho probado vigésimo noveno al hecho probado cuadragésimo primero se consignan los hechos probados relativos a ***(…).***
- Del hecho probado cuadragésimo segundo al hecho probado cuadragésimo quinto se consignan los hechos probados relativos ***al (…).***
- Del hecho probado cuadragésimo sexto al hecho probado quincuagésimo se consignan los hechos probados relativos ***a (…).***
- El hecho probado quincuagésimo primero se refiere a la ***(…).***

- Del hecho probado quincuagésimo segundo al hecho probado quincuagésimo tercero se consignan los hechos probados referidos ***(…).***

PRIMERO:

D. ***A.A.A.*** (el reclamante), cliente de CaixaBank, realizó el día 1 de febrero de 2021, fecha en la que se produjo la brecha de datos personales, una actualización de sus datos de contacto. ***(…)***.

SEGUNDO:

La actualización de datos de contacto llevada a cabo por D. ***A.A.A.*** el día 1 de febrero de 2021 consistió en:

- Dar de baja el ***Teléfono (…) ***TELÉFONO.1***

- Dar de alta el ***Teléfono (…) ***TELÉFONO.2***

- Dar de *alta* el ***Teléfono (…) ***TELÉFONO.3***

En el certificado de CaixaBank de 18 de julio de 2023 se indica:

> ***"(…)"***

TERCERO:

La actualización de datos de contacto se realizó.

Sin embargo, ***(…):***

En este sentido, CaixaBank en su escrito de 13 de diciembre de 2022 afirma:

> *"(…) los documentos* ***(…).***
>
> ***(…)."***

CUARTO:

(…)***.***

QUINTO:

En esa misma fecha (1 de febrero de 2021), en la que se produjo la brecha de datos personales, D. ***C.C.C.***realizó una transferencia, ***(…)***, dirigida a un tercero, cliente de otra entidad bancaria. Dicha transferencia se efectuó correctamente.

En el escrito de CaixaBank de 13 de diciembre de 2022 se indica:

*"efectivamente se hizo (…)**. La operación fue correcta."*

SEXTO:

En el comprobante de la transferencia realizada por D. ***C.C.C.,*** que pudo visualizar el reclamante, figuraban numerosos datos:

- Nombre de la entidad bancaria ***(…).***
- Fecha en la que se realizó la solicitud de emisión de transferencia***: (…)***
- Hora en la que se realizó la operación bancaria***: (…)***
- Número de referencia de la operación bancaria
- Nombre***,*** apellidos, NIF del ordenante de la transferencia, así como su domicilio.
- IBAN de la cuenta corriente desde la cual se realizó la transferencia***.***
- ***(…)*** *o* código bancario***.***
- Importe de la transferencia***.***
- Concepto por el que se realizó la transferencia***.***
- Nombre y Apellidos del beneficiario de la transferencia***.***
- IBAN de la cuenta bancaria del beneficiario de la transferencia***.***
- ***(…)*** *o* código bancario***.***
- Datos de la entidad de destino***: (…)***
- Justificante electrónico de evidencia de la autorización realizada a través de ***(…).***

En consecuencia, el reclamante pudo tener acceso a datos de carácter personal (nombre y apellidos, tanto del ordenante como del beneficiario de la transferencia, NIF y domicilio del ordenante, IBAN de las cuentas bancarias de origen y destino de la transferencia). Así como múltiples datos relativos a la operación bancaria realizada.

SÉPTIMO:

CaixaBank destaca que, a pesar de la brecha de datos personales, D. ***C.C.C.*** (ordenante de la transferencia) pudo visualizar (…) el comprobante de la transferencia que había realizado desde un primer momento.

En el escrito de 28 de junio de 2023, elaborado en contestación a la petición de prueba I, CaixaBank indica:

> ***"(…)".***

OCTAVO:

El día en el que tuvieron lugar ambas operaciones bancarias y se produjo la brecha de datos personales (1 de febrero de 2021), en CaixaBank se realizaron ***(…).***

En el certificado de CaixaBank de 18 de julio de 2023, elaborado en respuesta a la solicitud de práctica de prueba III, se indica lo siguiente:

> ***"1. (...)."***

NOVENO:

El reclamante tuvo disponible *en el apartado denominado* ***"(…)" (…)*** el comprobante de la transferencia realizada por D. ***C.C.C.***a un tercero, cliente de otra entidad bancaria, pudiendo acceder al contenido de dicho documento ***desde el (…).***

En el hecho probado sexto se reflejan qué datos personales figuraban en dicho comprobante.

DÉCIMO:

El reclamante no tuvo disponible *en el apartado denominado* ***(…)*** el comprobante de la actualización de datos de contacto realizada *hasta el* ***(…).***

UNDÉCIMO:

El día 31 de octubre de 2021 el reclamante presentó una reclamación ante la oficina de atención al cliente de CaixaBank, que fue registrada con el número ******REGISTRO.1*** con el siguiente texto:

"Hola Tengo un documento Que aparece en mi ***(…)*** *el 01/02/2021 confidencial de otro cliente Caixa haciendo aparecer todas las informaciones personal y confidencial de las personas por una transferencia Pido reclamación porque es una divulgación grave de información personal y como indemnización pido la valor de la transferencia que aparece en este documento* ******CANTIDAD €*** *Saludo"*

- El comprobante de la transferencia de 1 de febrero de 2021 realizado por D. ***C.C.C.***, que también acompañaba a la reclamación trasladada a la AEPD por el Banco de España, cuyo contenido ha sido reflejado en el hecho probado decimocuarto.

- ***(…).***

(…)"

(…)

En contestación a la solicitud de la práctica de prueba II, CaixaBank ha aportado, además de la documentación a la que se acaba de hacer referencia, una captura de pantalla en la que figura la siguiente información (DOCUMENTO NÚMERO 1):

(…).

En el campo destinado a reflejar la reclamación figura una información preliminar:

(…)

DUODÉCIMO:

El 2 de noviembre de 2021 a las 14:32 el reclamante recibió, en su dirección de correo electrónico, el siguiente mensaje automático procedente de la oficina de atención al cliente de CaixaBank.

Título del mensaje

(…)

Texto del mensaje:

"(…)"

(…)

DECIMOTERCERO:

El reclamante recibió respuesta a la reclamación de fecha 31 de octubre planteada mediante un escrito de CaixaBank de fecha 10 de noviembre de 2021, ***(…),*** en el que se hacía referencia a una supuesta disconformidad con unos recibos cargados en la cuenta bancaria del reclamante y no autorizados:

En dicho escrito, se indicaba:

> ***"****Respuesta a su queja o reclamación*
>
> ***Núm. Ref. Reclamación: ***REGISTRO.1*** [Coincidente con el número asignado a la reclamación que presentó el reclamante en CaixaBank reflejado en el hecho probado duodécimo].
>
> *Distinguido señor:*
>
> *Nos dirigimos a usted en respuesta a su reclamación, la cual muestra disconformidad con unos recibos cargados en su cuenta y no autorizados.*
>
> *Ante todo, deseamos explicarle que en CaixaBank nos esforzamos por poner a su disposición los medios necesarios para atenderle con la máxima profesionalidad, y para ello invertimos todos nuestros esfuerzos para lograr este objetivo. Así, pues, lamentamos que la percepción del servicio recibido no haya cumplido con sus expectativas. Le confirmamos que, en todo caso, su opinión es de gran valor para CaixaBank ya que, sin duda, permitirá a la entidad mejorar el servicio de calidad que desea ofrecer a sus clientes.*
>
> *En este sentido, una vez realizadas las comprobaciones oportunas, debemos comunicarle que CaixaBank se limita a cargar los recibos conforme a lo que indica el emisor de la orden de pago. Por lo que deberá dirigirse la compañía emisora del recibo para solicitarle la orden de domiciliación correspondiente.*
>
> *Por lo que entendemos que su pretensión ha quedado satisfecha y damos por concluida nuestra actuación en este asunto, quedando a su disposición para cualquier cuestión que precise.*
>
> *Esperando haberle podido facilitar una respuesta e información útil, deseamos manifestarle nuestro agradecimiento por la confianza depositada en CaixaBank y por la oportunidad que nos ofrece de mejorar la calidad de nuestro servicio.*
>
> *En caso de disconformidad con esta decisión, puede plantear su reclamación ante el Servicio de Reclamaciones del Banco de España, mediante escrito presentado en la dirección postal (…) o de manera telemática (…)*
>
> *Sin otro particular, reciba un cordial saludo"*

DECIMOCUARTO:

El 10 de febrero de 2022 a las 10:42:29 tuvo entrada en el Departamento de Conducta de Entidades del Banco de España una reclamación presentada por D. ***A.A.A.*** en la que indicaba:

"CaixaBank no respeta las normas de la confidencialidad de datos
tengo un documento de datos personal de otra persona que no tiene que ver conmigo en este documento de transferencia hay información como NIE número cuenta bancaria…
*Este documento aparece **(…)** el 1febreo 2021*
reclamo valor de la transferencia que aparece por falta grave a este norma
cuando he hecho reclamacion a la caixa como siempre no contesta realemente al problema enonciado"

Acompaña a dicha reclamación diversa documentación, entre ellos:

1. El comprobante de la transferencia realizada por D. ***C.C.C.,*** cuyo contenido ha sido reflejado en el hecho probado sexto.

2. La respuesta automática enviada por CaixaBank el 2 de noviembre de 2021 al recibir la reclamación de D. ***A.A.A.*** de fecha 31 de octubre de 2021, reproducida en el hecho probado duodécimo.

3. La respuesta a la queja o reclamación de CaixaBank de 10 de noviembre de 2021, derivada de la reclamación presentada el día 31 de octubre de 2021, reflejada en el hecho probado decimotercero.

DECIMOQUINTO:

El 5 de mayo de 2022 el Departamento de Conducta de Entidades del Banco de España remitió a esta Agencia la reclamación de fecha 10 de febrero de 2022 presentada por D. ***A.A.A.,*** por entender que su objeto afectaba esencialmente a actividades relacionadas con la protección de datos.

DECIMOSEXTO:

El 7 de junio de 2022 la AEPD trasladó la reclamación solicitando información a CaixaBank. El acuse de recibo relativo a dicho traslado acredita que CaixaBank aceptó la notificación el 8 de junio de 2022.

DECIMOSÉPTIMO:

(…).

Por una parte, en el escrito de CaixaBank de 28 de junio de 2023, elaborado en contestación a la práctica de prueba I, se indica:

"(…)."

Por otra, junto con dicho escrito de 28 de junio de 2023, CaixaBank ha aportado un correo electrónico titulado ***(…)*** *con el siguiente texto:*

" (…)

(…)"

DECIMOCTAVO:

El 22 de julio de 2022 CaixaBank envió un escrito al reclamante al objeto de dar respuesta a la reclamación que había presentado el 31 de octubre de 2021.

Dicho escrito muestra que la entidad bancaria en ese momento *estaba tratando de determinar la causa* que había permitido a D. ***A.A.A.*** acceder el al comprobante de una transferencia que había realizado otro cliente de CaixaBank a un tercero cliente de otra entidad bancaria.

En el escrito se indica que en esa fecha (22 de julio de 2022) ya no era accesible el justificante de la transferencia realizada por D. ***C.C.C.*** a través del ***(…).***

Contenido del escrito dirigido al reclamante:

"(…):

(…)."

En esa misma fecha, 22 de julio de 2022, CaixaBank dirigió a esta Agencia otro escrito, cuyo contenido es muy similar al enviado al reclamante, que se reproduce parcialmente:

"(…):

(…)"

DECIMONOVENO:

A fecha 22 de julio de 2022 ***Don A.A.A.***, el reclamante, no tenía su disposición ***(…)*** el comprobante de la actualización de datos de contacto que había realizado el día 1 de febrero de 2021***.***

VIGÉSIMO:

El 4 de agosto de 2022 CaixaBank (casi dos meses después de haber sido consciente de la brecha de datos personales) realizó un primer informe sobre la brecha de datos personales objeto de la reclamación. Indicando que la brecha de datos personales:

1. (…)
2. (…),
3. (…).

En dicho informe, entre otros aspectos, se indica:

"(…)

(…)"

VIGÉSIMO PRIMERO:

El 12 de agosto de 2022 el reclamante no disponía aún del justificante de la ***(…)*** que había realizado el 1 de febrero de 2021, fecha en la que se produjo la brecha de datos personales.

En esa misma fecha, 12 de agosto de 2022, se recibió en la AEPD un escrito del reclamante, enviando copia de un escrito de esa misma fecha dirigido al servicio de atención al cliente de CaixaBank con el siguiente texto:

"Hola

He recibido la respuesta de este reclamación
Primero reconocéis el error y eso me alegro
Pero sigue una error que compromete los la protección de datos de los clientes caixa y si yo he recibo este documento quien ha recibido el documento de ***(…)*** *con mis datos bancarias y personal?*

Segundo dices que es una error puntual
Pero el documento ha estado generado el 1 feb 2021
He hecho la reclamación al banco de España el 10 feb 2022 y a la fecha del 22 julio 2022 que a partir de este día este documento no aparece ningún documentos ajeno a los operativas realizadas
Entonces por una error puntual de divulgación de datos protegidas se ha quedado casi 1 año y 5 meses con la posibilidad de acceder este documento

Tercero cito: 1 feb 2021 realizó l operativa: ***(…)*** *en este caso porque no puedo acceder a este documento relativo a este operación con el bueno documento correspondiente*
Cuando verifico ***(…)***
Te adjunto foto del periodo de este operación que tengo actualmente y el que he tomado antes simplemente ***(…)***

Pero si yo he hecho una operación a este fecha tendré que aparecer ***(…)*** *y yo pido que me envías el documento relacionado a este* ***(…)***

(…) *por para decir que el problema está areglado cuando tenéis que rectificar y poner me el bueno documento que corresponde a este operación*

Eso significa una cosa es que el problema no está arreglado y pues más fácil de hacer ***(…)*** *si es eso cómo analizáis el problema* ***(…)*** *….*

Esperando una respuesta rapido con compensación financiera"

VIGÉSIMO SEGUNDO:

El ******FECHA.2*** el reclamante tuvo disponible ***(…)*** el documento que le permitía comprobar la actualización de datos de contacto que había realizado el 1 de febrero de 2021, fecha en la que se produjo la brecha de datos personales.

CaixaBank en su escrito de 28 de junio de 2023, elaborado en contestación a la práctica de la prueba I de fecha 7 de junio de 2023, indica:

"(…)"

VIGÉSIMO TERCERO:

El 4 de octubre de 2022 CaixaBank consideraba que se había producido ***(…).***

En este sentido, la AEPD recibió la contestación de CaixaBank al requerimiento de información del Inspector de 23 de septiembre de 2022 en la que se indica, entre otros aspectos, lo siguiente:

*"**a) (…):***

(…).

b) (…)."

VIGÉSIMO CUARTO:

(…) de la brecha de datos personales.

(…). Dicha entidad financiera destaca en su escrito de 28 de junio de 2023, en contestación a la práctica de prueba I:

"(…)"

VIGÉSIMO QUINTO:

El 21 de noviembre de 2022 el inspector remitió a CaixaBank un segundo requerimiento de información, en el que, entre otras cuestiones, se requería:

"Se requiere que comuniquen a esta Agencia

Informe completo del análisis realizado sobre el incidente.

*Explicación detallada de **(…)**. Se deberá aportar acreditación documental.*

*Descripción **(…).** Se deberá aportar acreditación documental."*

VIGÉSIMO SEXTO:

El 12 de diciembre de 2022 CaixaBank realizó ***(…)*** (elaborado un día antes de dar respuesta al segundo de requerimiento de información del Inspector).
Indicando que la brecha de datos personales:

1. (…)
2. (…)
3. (…).

(…):

"(…)

(…)

VIGÉSIMO SÉPTIMO:

El 13 de diciembre de 2022 CaixaBank informó a esta Agencia de que la brecha de datos personales, que calificaba únicamente como de pérdida de confidencialidad, se había producido ***(…).***

(…).

A continuación, se reproducen dos extractos del escrito elaborado por CaixaBank el 13 de diciembre de 2022 relativos a esta cuestión:

(…)

En el escrito de CaixaBank de 13 de diciembre de 2022 se indica:

(…)

Posteriormente, en el escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023 elaborado por CaixaBank en relación con esta cuestión se destacaba:

(…)

VIGÉSIMO OCTAVO:

A fecha 13 de diciembre de 2022 ***(…):***

En el escrito de CaixaBank de 13 de diciembre de 2022 se destaca:

(…)

VIGÉSIMO NOVENO:

Tanto en el escrito de CaixaBank de fecha 13 de diciembre de 2022 como en el escrito de CaixaBank de alegaciones al acuerdo de inicio de fecha 20 de febrero de 2023 CaixaBank afirmó que la acción llevada a cabo como consecuencia de la brecha de datos personales, como solución y medida de robustez del sistema, fue ***(…).***

A continuación, se reproduce un párrafo del escrito de CaixaBank de 13 de diciembre de 2022:

(…)

Asimismo, se reproduce el apartado denominado ***(…)*** del escrito de CaixaBank de 13 de diciembre de 2022:

(…)

En relación con esta cuestión, en el DOCUMENTO NÚMERO 7, que acompaña al escrito de alegaciones al acuerdo de inicio de CaixaBank de 20 de febrero de 2023 se indica:

(…)

TRIGÉSIMO:
CaixaBank afirma que en el momento en el que se produjo la brecha de datos personales, ***(…)***

En el escrito de 13 de diciembre de 2022 se indica:

(…)

TRIGÉSIMO PRIMERO:
(…)

En el escrito de CaixaBank de 28 de junio de 2023, elaborado en respuesta a la práctica de prueba I, se indica:

(…)

TRIGÉSIMO SEGUNDO:
(…)

En el escrito de 28 de junio de 2023, elaborado con motivo de la práctica de prueba I, se indica:

(…)

TRIGÉSIMO TERCERO:
CaixaBank afirma que ***(…).***

En este sentido, en el escrito de 28 de junio de 2023, en respuesta a la práctica de prueba I, se indica:

(…)

TRIGÉSIMO CUARTO:
(…).

(…).

(…)

TRIGÉSIMO QUINTO:
CaixaBank afirma que, ***(…).***

En este sentido, en el escrito de 18 de julio de 2023, elaborado en contestación a la práctica de prueba II, se destaca:

(…)

TRIGÉSIMO SEXTO:
(…)***.***

En relación con esta cuestión, en el escrito de 18 de julio de 2023, elaborado en contestación a la práctica de prueba II, se señala:

(…):

(…)[1]

TRIGÉSIMO SÉPTIMO:
(…)***:***

1. (…).

2. (…).

3. (…).

Se reproducen tres párrafos del escrito de 18 de julio de 2023, elaborado en contestación a la práctica de prueba II

(…)

TRIGÉSIMO OCTAVO:
El inspector estima ***(…).***

En este sentido, en el informe de actuaciones previas de investigación de fecha 18 de enero de 2023 se indica:

"La forma de solucionar la incidencia, ***(…).***

TRIGÉSIMO NOVENO:
(…)***:***

1.(…).

2.(…).

3. (…).

Se reproducen tres párrafos del escrito de 18 de julio de 2023, elaborado en contestación a la práctica de prueba II

(…):

(…)

- ***(…).***

(…).

CUADRAGÉSIMO:
(…).

Se reproducen los siguientes párrafos del escrito de 18 de julio de 2023, elaborado en contestación a la práctica de prueba II

(…)

CUADRAGÉSIMO PRIMERO:
CaixaBank describe en su escrito de 13 de diciembre de 2022 ***(…)***

(…)

CUADRAGÉSIMO SEGUNDO:
Para guardar la documentación justificativa de la operativa bancaria ***(…)***

(…)

En relación con esta cuestión, en el escrito de CaixaBank de 13 de diciembre de 2022 se refleja:

(…)

(…)

(…).

En relación con esta cuestión, el DOCUMENTO NÚMERO 7, que acompaña al escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023, CaixaBank destaca:

(…)

(…)

CUADRAGÉSIMO TERCERO:
A fecha 13 de diciembre de 2022 en CaixaBank ***(…)***

En el escrito de CaixaBank de 13 de diciembre de 2023 se indica:

(…)

(…).

(…)

(…)

Asimismo, en el escrito de CaixaBank de 28 de junio de 2023, elaborado en respuesta a la práctica de prueba I, se indica:

"(…)."

CUADRAGÉSIMO CUARTO:

El inspector considera que ***(…).***

El informe de actuaciones previas de investigación de 18 de enero de 2023 indica:

"(…)".

CUADRAGÉSIMO QUINTO:

(…)***.***

(…)***:***

En el escrito de CaixaBank de 28 de junio de 2023, elaborado en respuesta a la práctica de prueba I, se indica:

"(…).

(…)."

CUADRAGÉSIMO SEXTO:

A fecha 13 de diciembre de 2022 CaixaBank consideraba que la probabilidad ***de (…)*** o de repetición de la casuística (brecha de datos personales) era ***(…)***.

En el escrito de esa misma fecha CaixaBank indica:

"(…).

(…)"

Asimismo, expone:

"(…)

(…)"

CUADRAGÉSIMO SÉPTIMO:

El inspector en el informe de actuaciones previas de investigación de 18 de enero de 2023 destacó que, dado el número de clientes de CaixaBank y el número de operaciones que se realizan en dicha entidad bancaria, ***(…).***

En este sentido, en el mencionado informe se indica:

"Del análisis de la información facilitada se desprende que el origen del incidente ***(…).***

CUADRAGÉSIMO OCTAVO:

CaixaBank afirma que ***(…).***

(…).

(…):

***"(…**)".*

CUADRAGÉSIMO NOVENO:

El 17 de julio de 2023 se solicitó que se elaborara informe a la Inspección de la AEPD en el marco de la práctica de prueba:

En la nota interior de la misma fecha se indicaba:

"(…):

(…)."

QUINCUAGÉSIMO:

En contestación a la solicitud de informe en el marco de la práctica de la prueba, reflejada en el hecho probado cuadragésimo noveno, el inspector elaboró un informe, incluido en la Diligencia de fecha de 18 de julio de 2023, en el que concluía que, ***(…),*** Se reproduce parte del contenido de dicho informe:

"• *En relación a la frecuencia con que se puede producir este error, los representantes de la entidad informan que*

"(…)."

QUINCUAGÉSIMO PRIMERO:

CaixaBank ha certificado que ***(…)*** en dicha entidad financiera. Este dato se ha obtenido ***del (…)***, aportado el 28 de junio de 2023 en contestación a la práctica de prueba I.

QUINCUAGÉSIMO SEGUNDO:

El 28 de junio de 2023 CaixaBank acredita las fechas en las que se han realizado análisis de riesgos de seguridad en el ***(…)*** (relacionado con la brecha de datos personales objeto de la reclamación):

"(…)."

QUINCUAGÉSIMO TERCERO:

En relación con las *revisiones* ***(…)***, de acuerdo con la información facilitada por CaixaBank en su escrito de 28 de junio de 2023 cabe afirmar que:

A fecha 1 de febrero de 2021, fecha en la que se produjo la brecha de datos personales, no estaba vigente el ***(…).***

En dicha fecha (1 de febrero de 2021) tampoco estaba vigente el ***(…)***.

(…).

(…).

En relación con esta cuestión, en el escrito de CaixaBank de 28 de junio de 2023, elaborado en contestación a la práctica de prueba I, se indica:

"(…)"

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, 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 íter de la reclamación*

II íter de la reclamación

Antes de proceder al análisis de las alegaciones formuladas por CaixaBank, se considera necesario examinar el íter de la reclamación. Haciendo referencia a otras actuaciones, ya sea de la parte reclamada o de la AEPD, que permiten comprender la brecha de datos personales que ha dado lugar a este procedimiento sancionador:

01/02/21 El reclamante llevó a cabo una actualización de sus datos de contacto. Realizó dicha operación ***(…).***

Ese mismo día, D. ***C.C.C.***, otro cliente de CaixaBank, efectuó una transferencia ***(…)***, dirigida a un tercero, cliente de otra entidad bancaria.

(…).

(…).

(…).

(…).

(…).

Como consecuencia de ello, el reclamante tuvo ***(…).,*** en el que figuraban numerosos datos de carácter personal, tanto del ordenante de la transferencia como del beneficiario de la misma, así como otros datos relativos a la operación financiera realizada. Sin embargo, no tuvo disponible el ***(…)*** el 1 de febrero de 2021.

20/02/21 ***(…).***

La desactivación se produjo ***(…).***

21/06/21 CaixaBank realizó ***(…).***

31/10/21 El reclamante presentó una reclamación ante la oficina de atención al cliente de CaixaBank. ***(…)***

02/11/21 El reclamante recibió en su dirección de correo electrónico ***(…).***

10/11/21 CaixaBank *envió* ***(…).***

09/02/22 CaixaBank realizó ***(…).***

10/02/22 (Cuando ya se había cumplido un año desde que se había producido la brecha de datos personales) El reclamante presentó una reclamación, muy semejante a la ya planteada ante CaixaBank el ***(…)***, al Departamento de Conducta de Entidades del Banco de España.

05/05/22 El Departamento de Conducta de Entidades remitió la reclamación a la AEPD, con entrada en el Registro General de la Agencia el 10/05/22.

07/06/22 La AEPD remitió el traslado de la reclamación y una solicitud de información a CaixaBank, que recibió dicho documento el 8 de junio de 2022.

08/06/22 Fecha en la que CaixaBank y su ***(…).***

22/07/22 CaixaBank envió al ***(…).***

(…).

04/08/22 CaixaBank *elaboró* ***(…).***

- ***(…).***

- ***(…).***
- ***(…).***
- ***(…).***

10/08/22 Admisión a trámite de la reclamación.

12/08/22 El reclamante envió un correo electrónico al Servicio de Atención al Cliente de CaixaBank y remitió una copia del mismo a la AEPD.

En dicho escrito destacaba que ***(…)*** había podido acceder al justificante de la transferencia realizada por otro cliente de CaixaBank. Asimismo, solicitaba que se le enviase el comprobante de la actualización de datos que había realizado el 1 de febrero de 2021.

23/09/22 Primer requerimiento de información formulado por el Inspector a CaixaBank, comunicando a la AEPD el resultado del análisis realizado sobre el incidente y si del mismo se había detectado que pudiera haber una brecha de seguridad que afectase a otros clientes.

04/10/22 Escrito de CaixaBank dando respuesta al requerimiento de información del Inspector en el que se indica que se trataba de **(…)**

05/10/22 CaixaBank ***(…).***

21/11/22 Segundo requerimiento de información formulado por el Inspector. En el que se solicita:
“

- ***(…)***

- ***(…).***

12/12/22 CaixaBank realizó un segundo informe de la brecha de datos personales.

Consideraba que la causa era un error técnico: ***“(…).”***

En el apartado denominado “Plan de acción” se indica:

- ***(…).***
- ***(…).***
- ***(…).***

13/12/22 Escrito de CaixaBank contestando al segundo requerimiento de información formulado del Inspector, destacando que se ha producido ***“(…)”.***

10/05/23 CaixaBank *comenzó a utilizar* ***(…).***

16/05/23 CaixaBank *realizó* ***(…).***

01/06/23 En CaixaBank ***(…).***

07/06/23 En la práctica de prueba I se solicita información sobre diversas cuestiones, entre ellas:

"(…)."

20/06/23 El reclamante *tuvo* ***(…)*** el comprobante de la actualización datos de contacto que había realizado el 1 de febrero de 2021.

17/07/23 El Inspector elaboró un informe, partiendo de la media de operaciones por segundo de 1 de junio de 2023.

Del contenido de dicho íter se desprenden varias conclusiones:

1.La brecha de datos personales que tuvo lugar el 1 de febrero de 2021 pasó desapercibida a CaixaBank durante un prolongado periodo de tiempo.

(…).

2. El comprobante de la transferencia realizada por D. ***C.C.C. (…).***

3. Detectada la brecha de datos personales por CaixaBank, ***(…).*** En dicho informe se destacaba que la brecha se había producido como consecuencia de (…).

Dicha entidad bancaria *realizó* ***(…).***

3. ***(…).***

A pesar de determinar dicha causa definitiva, ***(…).***

4. El reclamante no tuvo disponible ***(…)*** el comprobante de la actualización de datos que había realizado el 1 de febrero de 2021 ***hasta el ***FECHA.2 (…). (…)*** la práctica de la prueba I, enviada por la AEPD el día 7 de junio de 2023, ***(…).***

III Alegaciones al acuerdo de inicio y a la propuesta de resolución

A lo largo de los fundamentos de derecho de esta resolución se va a ir dando respuesta a las alegaciones formuladas por CaixaBank tanto al acuerdo de inicio como a la propuesta de resolución.

Tal y como se refleja en esta resolución, en un primer momento, las actuaciones de esta AEPD iban encaminadas a tratar de determinar las circunstancias que habían llevado a que se produjera una brecha de datos personales, que había permitido que un cliente de CaixaBank hubiera tenido acceso a los datos personales de dos personas, que figuraban en el comprobante de una transferencia realizada por otro cliente de dicha entidad bancaria.

No obstante, a través de las actuaciones previas de investigación y ligado a la reclamación presentada, y tal y como se ha acreditado a lo largo de este procedimiento, la AEPD ha tenido conocimiento de deficiencias del procedimiento que

afectaban, tanto a medidas de seguridad adoptadas por la entidad como a aspectos de diseño que vulnerarían la privacidad desde el diseño.

A pesar de que la entidad bancaria en sus alegaciones insista en que todo se reduce a una única reclamación de uno de sus clientes. Dicha reclamación ha sacado a la luz diversas cuestiones relacionadas tanto con el artículo 32 del RGPD como con el artículo 25 de dicho Reglamento, deficiencias del procedimiento, que se consideran sancionables por sí mismas.

Por otra parte, se desea destacar que el escrito de alegaciones a la propuesta de resolución no ha rebatido los hechos probados, que figuraban en dicha propuesta y que han sido reproducidos en esta resolución. Únicamente cuestiona el hecho probado trigésimo segundo, considerando que, si bien lo indicado en el mismo puede considerarse cierto, se efectúa una interpretación en el mismo que considera incompleta.

Contestación a la supuesta vulneración del principio de non bis in idem:

Alega CaixaBank que el contenido del acuerdo de inicio implicaría una supuesta vulneración del principio de non bis in idem (en su opinión, incluso cabría apreciar un supuesto de non ter in idem), reiterando dicha alegación en su escrito de alegaciones a la propuesta de resolución.

En primer lugar, los artículos 5.1 f), 32 y 25 se tipifican de manera diferenciada en el RGPD. Asimismo, se califican de manera diferenciada, a los efectos de la prescripción, en la LOPDGDD y gozan, cada uno de ellos, de entidad propia.

En cuanto a la supuesta concurrencia de los artículos 5.1 f) y 32 del RGPD:

En su escrito de alegaciones al acuerdo de inicio CaixaBank afirma:

"(…) el Acuerdo de Inicio impone dos sanciones diferenciadas, por carecerse de medidas de seguridad y porque se ha producido, por carecer de tales medidas, una brecha de confidencialidad y, según afirma, lo que posteriormente se desmentirá, disponibilidad de los datos.

De este modo, la AEPD considera unos mismos hechos constitutivos de infracción de un principio de los previstos en el artículo 5.1 del RGPD y de su concreción o materialización, llevada a cabo, en este caso, en el artículo 32 del RGPD. Se sanciona así no disponer de medidas y una brecha por no disponer de medidas, lo que implica una reiteración sancionadora proscrita por el derecho administrativo sancionador.

Y es que, de seguirse el razonamiento aquí mantenido, cualquier vulneración de un precepto del RGPD implicaría la comisión no sólo de la infracción de dicho precepto, sino de la del principio de protección de datos del que la norma vulnerada trajera causa. Así, por ejemplo, la vulneración de los artículos 6 a 10 del RGPD implicaría asimismo una vulneración del principio de licitud o la de los artículos 13 y 14 una vulneración del principio de transparencia, lo que, sin embargo, no se recoge en las resoluciones de la AEPD que, sin embargo, no dudan en considerar simultáneamente vulnerados los artículos 5.1 f) y 32 de dicho texto legal."

En relación con las alegaciones que acaban de ser reproducidas, resulta necesario traer a colación la diferencia entre la vulneración del art. 5.1.f) y del artículo 32 del RGPD, la diferente tipificación en apartados distintos del art. 83 del RGPD y la diferente calificación de ambos a los efectos de la prescripción en la LOPDGDD.

El art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad o de integridad de los datos personales, lo que puede producirse o no por ausencia o deficiencia de las medidas de seguridad.

Este principio tan sólo determina el cauce a través del cual puede lograrse el mantenimiento de la confidencialidad e integridad cuando explicita *"mediante la aplicación de medidas técnicas y organizativas apropiadas"*, que no son estrictamente de seguridad.

Existen 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. De seguridad. Sólo de seguridad.

Además, su objetivo es garantizar un nivel de seguridad adecuado al riesgo mientras que en el caso del artículo 5.1.f) del RGPD, se debe garantizar la confidencialidad e integridad. Como puede observarse, los dos artículos persiguen fines distintos, aunque puedan estar relacionados.

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 par-*

ticipan 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 explicitado en el procedimiento sancionador enjuiciado no se ha vulnerado el principio non bis in idem, puesto que, si bien entendido grosso modo los hechos se detectan consecuencia de una brecha de datos personales, la infracción del art. 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y disponibilidad, la infracción del art. 32 del RGPD se reduce a la deficiencia de las medidas de seguridad (solo de seguridad) detectadas, presentes independientemente de la brecha de datos personales. De hecho, si estas medidas de seguridad que tenía implantadas CaixaBank se hubieran detectado por la AEPD sin que se hubiera producido la pérdida de confidencialidad, únicamente habría sido sancionada por el art. 32 del RGPD.

Como hemos indicado, mediante el art. 5.1.f) del RGPD se sanciona una pérdida de confidencialidad y disponibilidad y mediante el art. 32 del RGPD la deficiencia de las medidas de seguridad implantadas por el responsable del tratamiento. Medidas de seguridad deficientes, añadimos, que infringen el RGPD, independientemente de que no se hubiera producido la brecha de datos personales.

En relación con la supuesta concurrencia de los artículos 25 y 32 del RGPD:

El artículo 25.1 del RGPD dispone:

"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."

1. Como puede observarse, dicho artículo 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 interesados.

Por su parte, el considerando 78 del RGPD prevé:

> *"78) 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." (el subrayado es nuestro).*

Por tanto, las medidas a las que hace referencia el artículo 25 del RGPD no son exclusivamente medidas de seguridad, como sucede en el caso del artículo 32 del RGPD.

Se pretende que la empresa u organización tenga integrada dentro de la misma, de su organización, de su funcionamiento ordinario, la protección de datos de carácter personal. Que no se trate de un apéndice, de un añadido adicional in fine, sino de una parte integrante y relevante dentro de la misma desde antes incluso de iniciarse materialmente el tratamiento de datos personales.

De esta forma, se apuesta porque la protección de datos de carácter personal sea tenida en consideración desde un primer momento, desde la toma de decisiones o del momento de la planificación.

Como puede observarse, se establece una obligación que imbuye a toda la organización y que implica un continuo proceso de revisión y retroalimentación, con el fin de verificar si las medidas técnicas y organizativas existentes, de todo tipo, e implementadas por la organización resultan adecuadas con el fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados. De esta forma, en caso de no resultar adecuadas, podrían ser modificadas, o en su caso, reforzadas, incorporando nuevas medidas que garanticen una más adecuada protección de los datos de carácter personal.

Tal y como se ha indicado anteriormente, el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad o de integridad de los datos personales.

Cabe apreciar, que la perspectiva o el ángulo a través del cual se contempla la realidad es diferente de lo previsto en el artículo 25 del RGPD.

En este sentido, el RGPD articula un sistema completo destinado a garantizar la protección de los datos de carácter personal de los ciudadanos. Para ello, va centrando su atención en distintos aspectos que deben ser examinados por los responsables y, si así lo prevé el precepto, por los encargados de tratamiento.

Cada artículo constituye un ángulo desde el que observar la realidad con el fin de articular un conjunto de medidas que garanticen una adecuada protección de los datos de carácter personal.

Se trata de ángulos complementarios. Todos ellos deben ser tenidos en cuenta y respetados, ya que son necesarios para articular una protección acorde con lo dispuesto en el RGPD.

En sus alegaciones al acuerdo de inicio, CaixaBank indica:

> *"(…) si se sigue el razonamiento del Acuerdo de Inicio cualquier vulneración de la normativa de protección de datos por parte de un responsable conllevaría necesariamente la vulneración del principio de protección de datos desde el diseño, puesto que esa vulneración derivaría del inadecuado cumplimiento de este principio.*
>
> *Así, una vulneración, por ejemplo, del principio de transparencia implicaría, a juicio de la AEPD un incumplimiento del artículo 25.1, dado que no se ha adoptado adecuadamente desde el diseño la medida consistente en informar a los interesados. Y lo mismo sucedería con cualquiera de los principios citados por el artículo 5 del RGPD (se incumpliría el artículo 25.1 por elegir una base jurídica inadecuada del tratamiento, por no haber evitado desde el diseño tratar más datos de los adecuados, pertinentes y necesarios para el tratamiento, por no adoptar desde el diseño medidas tendentes a garantizar su exactitud, por no haber adoptado desde el diseño reglas para conservarlos por más tiempo del estrictamente necesario, por no realizar una evaluación de impacto en la protección de datos que la AEPD considere necesaria, etc.)."*

No se comparte el razonamiento expuesto por CaixaBank, ya que de ser la situación tal y como dicha entidad bancaria describe, la gran mayoría de las resoluciones sancionadoras de la AEPD considerarían vulnerado el artículo 25. 1 del RGPD, y esto no es así.

Cuando la AEPD tiene conocimiento de una reclamación y decide abrir un expediente sancionador, valora, a la vista de las circunstancias que concurren en el caso concreto, qué infracción o posibles infracciones del RGPD se habrían cometido.

Al examinar el contenido de la reclamación, que ha dado lugar a este procedimiento, se ha considerado que lo reflejado en la misma se ajustaba a una posible vulneración de tres artículos del RGPD: el artículo 5.1 f), el artículo 32 y el artículo 25, que posteriormente se ha visto confirmada.

En respuesta a estos tres párrafos, CaixaBank alega en sus alegaciones a la propuesta de resolución:

"Y el hecho de que los hechos sean enjuiciados desde una supuesta pluralidad de perspectivas en nada afecta al hecho de que, en definitiva, la AEPD considere que la supuesta insuficiencia de la medida de seguridad concreta es la que determina la vulneración del principio de privacidad desde el diseño, lo que conduce nuevamente a la conclusión, ya mencionada en las alegaciones al Acuerdo de Inicio de que, si se sigue el razonamiento de la AEPD, cualquier vulneración del RGPD implicaría, simultáneamente, dicha vulneración y un insuficiente cumplimiento del principio de privacidad desde el diseño.

La AEPD pretende contradecir lo que acaba de indicarse del siguiente modo:

"No se comparte el razonamiento expuesto por CaixaBank, ya que de ser la situación tal y como dicha entidad bancaria describe, la gran mayoría de las resoluciones sancionadoras de la AEPD considerarían vulnerado el artículo 25. 1 del RGPD, y esto no es así. Cuando la AEPD tiene conocimiento de una reclamación y decide abrir un expediente sancionador, valora, a la vista de las circunstancias que concurren en el caso concreto, qué infracción o posibles infracciones del RGPD se habrían cometido.

Al examinar el contenido de la reclamación, que ha dado lugar a este procedimiento, se ha considerado que lo reflejado en la misma se ajustaba a una posible vulneración de tres artículos del RGPD: el artículo 5.1 f), el artículo 32 y el artículo 25. Por las razones expuestas, no se entiende vulnerado el principio de non bis in idem."

En definitiva, la AEPD viene a indicar que lo señalado por mi representada no ha lugar porque en el presente caso se ha considerado procedente considerar infringidos los tres preceptos mencionados mientras en otros casos no lo considera. A nuestro juicio, el razonamiento carece de sentido, dado que parece simplemente razonarse que el administrado ha de estar y pasar por lo que la AEPD considere procedente en cada momento concreto, siendo así que semejante conclusión es la que se utiliza para rebatir el argumento, mantenido por CAIXABANK, de que en este caso su proceder ha sido inadecuado. Es decir, frente a ese argumento, la AEPD se limita a indicar, sin razonarlo, que no ha lugar a invocar que el proceder es inadecuado porque la AEPD no comparte ese parecer."

cualquier vulneración del RGPD implicaría, simultáneamente, dicha vulneración y un insuficiente cumplimiento del principio de privacidad desde el diseño.

Las resoluciones de la AEPD muestran claramente que esta Agencia no considera que cualquier vulneración del RGPD implique, de forma simultánea, la vulneración del artículo 25 del RGPD, como pretende dar a entender CaixaBank.

Por otra parte, la valoración de cada reclamación, de cara a decidir si se incoa o no un expediente sancionador se efectúa partiendo los hechos del caso concreto que se examina.

Por las razones expuestas en este fundamento de derecho, no se entiende vulnerado el principio de non bis in idem.

IV Contestación a la alegación relativa a la supuesta existencia de un concurso medial entre las tres infracciones imputadas a CaixaBank:

A continuación, se reproducen varios párrafos de las alegaciones formuladas por CaixaBank al acuerdo de inicio, en los que se argumenta la supuesta existencia de un concurso medial entre las tres infracciones imputadas a dicha entidad:

> *"Por otra parte, en el negado supuesto de que por esa AEPD no se apreciase la concurrencia de los requisitos exigibles para la aplicación del principio non bis in idem en el presente procedimiento, 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, cada una de ellas se encontraría subsumida y embebida en las otras, 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 adelante, "LRJSP"), según el cual:*
>
> *"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".*
>
> *Siendo ello así, no puede en ningún caso sancionarse a mi mandante todas las infracciones, dado que la comisión de la supuesta infracción del artículo 25.1 del RGPD implicaría necesariamente la comisión de la infracción del artículo 32.1 de dicha norma, dando lugar este último incumplimiento a la supuesta vulneración del artículo 5.1 f) del RGPD.*
>
> *Y es que la AEPD considera (…), que mi mandante no ha cumplido la obligación impuesta en el artículo 25.1 del RGPD y al propio tiempo considera que mi mandante han incumplido el artículo 32.1 del RGPD, dado que no ha aplicado "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo", lo que determina a su vez una vulneración del principio de seguridad, consagrado en el artículo 5.1 f) del RGPD.*
>
> *Es decir, y sin perjuicio de que como se ha indicado anteriormente, entiende mi mandante que se estaría imponiendo una triple sanción por unos mismos hechos, de lo que no cabría duda es de que la falta de aplicación de las medidas a las que se refiere el artículo 32.1, y por ende la supuesta infracción del artículo 5.1 f) traería necesaria e inseparablemente causa de la supuesta 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, su falta de aplicación y el principio mismo que la adopción de esa medida pretende proteger, 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.*
>
> *Por ello, o bien se están sancionado triplemente unos mismos hechos o bien dos de las infracciones sólo pueden ser, necesariamente, consecuencia de la primera.*

Según establece la jurisprudencia (por todas, la Sentencia 339/2015 de 25 de septiembre de 2015 de la Audiencia Nacional -recurso 262/2014- que cita la Sentencia del Tribunal Supremo de 8 de febrero de 1999, -recurso 9/1996-) "la aplicación del concurso medial exige una necesaria derivación de unas infracciones respecto de las demás y viceversa, por lo que es indispensable que las unas no puedan cometerse sin ejecutar las otras". Así, debe existir "una relación tal entre las infracciones concernidas que una de ellas derive necesariamente de la otra, de modo que no sea posible la comisión de una sin ejecutar la otra" (por todas, la Sentencia de la Audiencia Nacional de 26 de diciembre de 2013, -recurso 416/2012).

Pues bien, como se ha indicado, es evidente que se produce tal relación entre las tres infracciones que pretenden imputarse contra mi mandante, como se ha indicado con anterioridad."

En primer lugar, el artículo 29 de la LRJSP no resulta de aplicación al régimen sancionador impuesto por el RGPD.

1.El RGPD es un sistema completo.

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

En relación, específicamente y también, con el régimen sancionador dispuesto en el mismo, resultan de aplicación sus disposiciones de manera inmediata, directa e íntegra previendo un sistema completo y sin lagunas que ha de entenderse, interpretarse e integrarse de forma absoluta, completa, íntegra, dejando así indemne su finalidad última que es la garantía efectiva y real del derecho fundamental a la Protección de Datos de Carácter Personal. Lo contrario determina la merma de las garantías de los derechos y libertades de los ciudadanos.

De hecho, una muestra específica de la inexistencia de lagunas en el sistema del RGPD es el artículo 83 del RGPD que determina las circunstancias que pueden operar como agravantes o atenuantes respecto de una infracción (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, previstas en el art. 58, apartado 2, letras a) a h) y j) de RGPD, 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 correctivas 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 es 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.No hay laguna legal, no hay aplicación supletoria del art. 29 del RGPD.

Amén de lo expuesto, significar que no hay laguna legal respecto de la aplicación del concurso medial previsto en el artículo 29 de la LRJSP. 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 escrito de alegaciones a la propuesta de resolución formula alegaciones en relación a lo que acaba de ser indicado e insiste en la existencia de un claro caso de concurso medial.

En contestación a estas segundas alegaciones efectuadas por CaixaBank en relación con la aplicación del concurso medial en los términos del artículo 29 de la LRJSP, 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. No hay laguna legal, no hay aplicación supletoria del art. 29 del RGPD.*
>
> *Amén de lo expuesto, significar que no hay laguna legal respecto de la aplicación del concurso medial previsto en el artículo 29 de la LRJSP. 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."*

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 CaixaBank, 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 tres 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 CaixaBank, la comisión de tres infracciones diferenciadas, tipificadas de forma diferenciada, no existiendo, además, en el caso concreto, concurso medial.

Por todo lo expuesto, se desestima la presente alegación.

Por otra parte, esta Agencia, a la vista de lo sucedido en el supuesto concreto examinado, afirma que no cabe apreciar en el mismo concurso medial.

Como se ha indicado anteriormente, el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad o de integridad de los datos personales, lo que puede producirse o no como consecuencia de la deficiencia de las medidas de seguridad.

En este caso se ha producido una vulneración del artículo 5.1.f) del RGPD, pero la misma no deriva necesariamente de la deficiencia de las medidas de seguridad. La realidad analizada resulta mucho más compleja.

Sirva de ejemplo la falta de disponibilidad del comprobante de la actualización de datos de contacto realizada por el reclamante el 1 de febrero de 2021:

En un primer momento, se produjo un ***(…).***

En ese momento, ***(…)*** Por este motivo, ***(…)*** y la entidad bancaria no detectó que se había producido una brecha de datos personales.

Sin embargo, una vez que la brecha fue detectada por CaixaBank (…), la pérdida de disponibilidad se prolongó en el tiempo, no siendo posible afirmar que viniera determinada únicamente por razones técnicas. El reclamante ***(…).***

Tal y como se ha destacado en el fundamento de derecho II (Íter de la reclamación) , para que la disponibilidad del justificante de actualización de datos finalmente se produjera, fue determinante la recepción por parte de la entidad bancaria del escrito de esta Agencia de fecha 7 de junio de 2023, relativo a la apertura de un periodo de práctica de prueba I, en el que ***(…).***

En conclusión, no cabe afirmar que la supuesta infracción del artículo 5.1 f) traiga *"necesaria e inseparablemente causa de la supuesta falta de concepción o diseño de las mismas en el momento de terminar los medios y fines del tratamiento".*

En cuanto a los artículos 25 y 32 del RGPD, tal y como se analizará posteriormente, cabe considerar que ambos artículos habrían sido vulnerados, si bien, no cabe afirmar que la vulneración del artículo 25 derive necesariamente de la del artículo 32 o viceversa.

Tal y como se indicará posteriormente, se considera que determinadas cuestiones que cabría considerar infracciones del artículo 25 del RGPD resultarían sancionables aún en el caso de no haberse producido una brecha de datos personales. Por ejemplo, el diseño del procedimiento que articula la tramitación de escritos presentados por los interesados a CaixaBank que afectan a la protección de datos de carácter personal. Otro ejemplo, el diseño adoptado tras ***(…)*** CaixaBank ignoraba la existencia de la brecha de datos personales.

A modo de conclusión, se han expuesto detenidamente las razones por las que se desestima las alegaciones formuladas por CaixaBank relativas al concurso medial.

A mayor abundamiento, tampoco resultaría adecuada su aplicación a un caso complejo, con tantos matices, como el que está siendo examinado en este procedimiento sancionador.

V Análisis de la vulneración del Artículo 5.1 f) del RGPD

CaixaBank en sus alegaciones considera que no se ha producido una vulneración del artículo 5.1 f) del RGPD, no se comparte dicha afirmación.

A continuación, va a analizarse el supuesto objeto de este procedimiento sancionador desde un ángulo o perspectiva concreta: la prevista en el artículo 5. 1 f) del RGPD.

El referido artículo prevé:

> *"1. Los datos personales serán:*
>
> *f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."*

El contenido de dicho artículo habría sido vulnerado:

Por una parte, se ha producido una brecha de datos personales, que ha provocado la pérdida de confidencialidad de unos datos de carácter personal relativos a dos personas:

1. El ordenante de la transferencia: otro cliente de CaixaBank.

2. El beneficiario de la misma: un tercero, cliente otra entidad bancaria.

En el hecho probado sexto se enumeran los datos personales que figuraban en el comprobante de la transferencia y que han sido desvelados.

Por otra, el reclamante no ha tenido a su disposición el comprobante de la actualización de datos de contacto que había realizado el 1 de febrero de 2021 hasta el ***(…)*** (brecha de disponibilidad), con la consiguiente falta de disponibilidad de os datos personales del reclamante que figuran en el mismo, tal y como se refleja en la siguiente tabla:

FECHA	Qué sucede en esa fecha	Situación del reclamante
01/02/21	Actualización de datos de contacto. ***(…).***	El reclamante no tuvo disponible ***(…)*** el comprobante de la actualización de datos de contacto realizada el 1 de febrero de 2021.
20/02/21	***(…).***	El reclamante continúa sin tener disponible **(…)** el comprobante de la actualización de datos de contacto realizada el 1 de febrero de 2021.
21/06/21	CaixaBank realizó un ***(…).***	
31/10/21	El reclamante ***(….)*** .	
02/11/21	El reclamante recibió ***(…)***	
10/11/21	CaixaBank *envió* ***(…)***	
09/02/22	CaixaBank realizó ***(…)***	
10/02/22	El reclamante ***(…)*** reclamación, muy semejante a la ya planteada ante CaixaBank ***(…)***, al Departamento de Conducta de Entidades del Banco de España.	
05/05/22	El Departamento de Conducta de Entidades remitió la reclamación a la AEPD, con entrada en el Registro General de la Agencia el 10/05/22.	El reclamante continúa sin tener disponible **(…)** el comprobante de la actualización de datos de contacto realizada el 1 de febrero de 2021.
08/06/22	CaixaBank recibió el traslado y la solicitud de información de la AEPD. ***(…).***	

22/07/22	CaixaBank verificó que ***(...)***. CaixaBank dirigió un escrito al reclamante destacando esta circunstancia y un escrito, con un contenido muy similar, a la AEPD en respuesta al traslado y la solicitud de información.	
04/08/22	CaixaBank *elaboró* ***(...)***.	
10/08/22	Admisión a trámite de la reclamación.	
12/08/22	El reclamante envió un correo electrónico al Servicio de Atención al Cliente de CaixaBank y remitió una copia del mismo a la AEPD. En el mismo mostraba su disconformidad con la forma en la que CaixaBank estaba gestionando su reclamación. Asimismo, solicitaba que el comprobante de la actualización de datos de contacto realizada el 01/02/21 ***(...)***.	
23/09/22	Primer Requerimiento de información a CaixaBank por parte del Inspector.	
04/10/22	Escrito de CaixaBank en respuesta al requerimiento de información. ***(...)***.	
05/10/22	CaixaBank ***(...)***.	
21/11/12	Segundo requerimiento de información formulado por el Inspector.	
12/12/22	CaixaBank ***(...)***.	
13/12/22	Escrito de CaixaBank en respuesta al segundo requerimiento de infracción. ***(...)***.	
27/01/23	Acuerdo de inicio	
07/06/23	Práctica de prueba I, enviada por la AEPD el día 7 de junio de 2023, ***(...)***.	
20/05/23	***(...)***	CaixaBank afirma que en esta fecha el reclamante tuvo disponible ***(...)*** el comprobante de la actualización de datos de contacto que había realizado el 1 de febrero de 2021**.**

En el escrito de alegaciones a la propuesta de resolución CaixaBank niega la existencia de una brecha de disponibilidad. En este sentido, destaca:

> *"La Propuesta de Resolución realiza a lo largo de sus fundamentos de derecho diversas consideraciones acerca de la existencia en este caso de una brecha*

de disponibilidad de los datos personales del Reclamante, puesto que no pudo disponer del documento justificativo de la modificación efectuada ante mi representada de sus datos de contacto.

(…)

Como puede comprobarse, la Propuesta de Resolución en ningún momento indica que el interesado no haya tenido acceso a sus datos personales y que los mismos no hayan estado disponibles tanto para él como para mi representada, sino que califica los hechos como brecha de disponibilidad como consecuencia del hecho de que ***(…)*** *el documento comprobante de dicha actualización.*

Y en este punto, es preciso indicar que una brecha de disponibilidad en materia de protección de datos ha de referirse a la accesibilidad a lo datos y no a los comprobantes *relacionados con los mismos. Así, la propia AEPD en su Guía para la notificación de brechas de seguridad, accesible en su página web en el enlace https://www.aepd.es/documento/guia-brechas-seguridad.pdf, indica que "una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos".*

En el mismo sentido, el Grupo de Trabajo del artículo 29 (en adelante, "GT29") en sus "Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679", adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018, en términos que posteriormente se reiteran expresamente por el Comité europeo de Protección de Datos (en adelante, "EDPB") en sus "Directrices 9/2022 sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el RGPD", señala que se produce una violación de la disponibilidad "cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos", añadiendo que "un incidente de seguridad que provoque la no disponibilidad de los datos personales durante un período de tiempo es también un tipo de violación, ya que la ausencia de acceso a los datos puede tener un impacto significativo en los derechos y las libertades de las personas físicas".

*Es decir, para que nos encontremos ante una brecha de disponibilidad la misma debe referirse a los datos personales, de forma que los mismos (*no los documentos o comprobantes del tratamiento, sino los propios datos*) no puedan ser accesibles para los interesados o para el responsable del tratamiento y, en definitiva, para quienes estén legitimados para llevar a cabo dicho acceso.*

Sin embargo, la Propuesta de Resolución se refiere única y exclusivamente a la accesibilidad del documento, no negando en ningún momento que los datos han permanecido accesibles para el interesado en (…) ni que aquél podía obtener el certificado de su modificación acudiendo a las oficinas de CaixaBank.

Y esta confusión entre el dato personal y el documento se deriva de la propia prueba que fue requerida a mi representada por parte de la AEPD (…)

Por tanto, existe una, permítasenos, inadecuada aplicación por la AEPD del concepto de brecha de disponibilidad: los datos siempre han permanecido accesibles y disponibles para el interesado, que podía de modo permanente, con-

*sultar los mismos en su propia **(…)**. Este hecho no se niega en ningún momento en la Propuesta de Resolución, que únicamente se refiere a la accesibilidad del documento.*

Y sentado lo anterior, considera mi representada que la AEPD lleva a cabo una interpretación extensiva del concepto de brecha de disponibilidad de datos personales que determina la aplicación por la misma de disposiciones que no guardan relación con la normativa de protección de datos personales, lo que, considera CAIXABANK supone una extralimitación en el uso de sus competencias.

(…) entiende mi representada que la AEPD se excede en el ejercicio de sus competencias, porque ¿qué normativa obliga a CaixaBank a publicar on-line el justificante de la operación?

¿Qué pasaría si este servicio de gestor documental on-line no se ofreciera a los clientes y simplemente se enviara por correo postal, lo que era la practica estándar del sector hasta ahora? ¿Se estaría incumpliendo alguna norma?

*La respuesta no puede ser otra que no pasaría nada, porque ni la normativa bancaria, aplicable a la actividad de mi representada, ni la de protección de datos, ni ninguna otra, imponen a CAIXABANK **(…).***

*La AEPD ha tomado una buena práctica de CAIXABANK, que supone una mejora destinada a facilitar la experiencia de sus clientes, y la ha convertido en una obligación legal susceptible de sanción. ¿Esto significa que, **(…)**?*

(…)

De ello cabe deducir que la AEPD considera procedente la imposición a mi representada de obligaciones documentales adicionales a las establecidas en la normativa bancaria y que además resulta competente para conocer de la posible causación al interesado de unos supuestos perjuicios, que no guardan relación alguna con su derecho fundamental a la protección de datos, dado que no existe duda, y la AEPD reconoce que el interesado pudo acceder permanentemente a los datos, aunque ese acceso no haya tenido lugar en la ubicación que la AEPD parece considerar más oportuna.

CAIXABANK considera que en este caso esta interpretación resulta excesiva: si los datos se encuentran disponibles, los perjuicios que pudieran llegar a causarse al interesado por no disponer de un documento justificante que, por otra parte, CAIXABANK no tiene la obligación de emitir, se dilucidarían en sede judicial ante los órganos de la jurisdicción civil.

Entiende respetuosamente mi representada que la AEPD no puede considerar que cualquier prejuicio, de cualquier naturaleza, que sólo de una forma remota y extensiva pueda llegar a guardar relación con la existencia de un tratamiento de datos personales (no con la vulneración de su normativa reguladora, sino con la existencia de algún tipo de tratamiento) pueda justificar su intervención, aun cuando la cuestión no guarde relación con la protección de datos personales."

En respuesta a dicha alegación, cabe destacar que, relación con la disponibilidad, la *Guía para la notificación de brechas de datos personales"* elaborada por la AEPD, indica lo siguiente:

> *"Disponibilidad: Una brecha afecta a la disponibilidad de los datos personales cuando han estado inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos. Esta situación puede ocurrir por sucesos que afecten a los datos personales en sí mismos o también por sucesos que afecten a los sistemas utilizados para su tratamiento. Por ejemplo, incluye casos de cifrado de datos personales o de los sistemas de información causado por malware de tipo ransomware, pérdida de documentación en papel con datos personales o la imposibilidad de acceder a un almacenamiento de datos (acceso físico o lógico).*
>
> *Para el responsable del tratamiento es importante determinar si la disponibilidad se ha podido recuperar o está en vías de recuperación, dado que recuperar los datos y los sistemas de tratamiento es la vía para mitigar el daño que pueden producir este tipo de brechas de datos personales. Para ello, los responsables de tratamiento deben establecer estrategias y procedimientos de recuperación ante situaciones de este tipo, incluyendo procedimientos de copia de seguridad, recuperación ante incidentes y estrategias de gobernanza de los datos.*
>
> *Ejemplo: En brechas de disponibilidad causadas por malware tipo ransomware en las que el responsable de tratamiento pueda descartar con certeza la exfiltración de datos y se pueden reestablecer los datos personales y medios de tratamiento sin que afecte significativamente a los servicios prestados, se puede considerar que el riesgo se ha mitigado adecuadamente. En el caso de que la recuperación de los datos y/o tratamientos se prolongue en el tiempo afectando significativamente a los servicios prestados, por ejemplo, al no existir o no funcionar sistemas de respaldo de datos y procesos, se puede concluir que el riesgo no solo no ha quedado mitigado, sino que se está materializando y causando perjuicios de diversa consideración a los interesados."* (el subrayado es nuestro).

En cuanto al caso concreto objeto de examen, el comprobante de la actualización de datos realizada por el reclamante el 1 de febrero de 2021 contenía datos de carácter personal.

Tal y como CaixaBank destaca en sus alegaciones a la propuesta de resolución, dichos datos de carácter personal debían ser accesibles para quienes estaban legitimados para llevar a cabo dicho acceso: el responsable del tratamiento y el reclamante.

CaixaBank prestaba un servicio al reclamante, que era su cliente. Desde la perspectiva de la protección de datos de carácter personal, los datos de carácter personal tenían que estar disponibles para el cliente.

En el escrito de alegaciones al acuerdo de inicio CaixaBank afirmaba:

> *"Sin embargo, dicho sea con el debido respeto, la citada brecha de disponibilidad no tuvo lugar en la práctica: el Reclamante vio modificados sus datos de contacto desde el mismo momento de realizar la solicitud de modificación, como podía comprobar en cualquier momento mediante la contrastación de sus datos personales* ***(…)****. Del mismo modo, la acreditación de la solicitud efectuada estuvo en todo momento a disposición del interesado, que podía haberla solicitado de CAIXABANK aun cuando, es cierto, no pudiera acceder a ella* ***(…)****, durante el período de tiempo mencionado en el Acuerdo."*

Afirma CaixaBank que el cliente podía haber contrastado en cualquier momento que la actualización de datos de contacto realizada el 1 de febrero de 2021 se había llevado a cabo. No a través del comprobante, que no estuvo disponible para el reclamante hasta el ***(…)*** (hecho probado décimo), sino efectuando otras consultas en (…) o solicitándolo a la entidad bancaria.

A continuación, vamos a acompañar al reclamante en dichas comprobaciones.

Una vez realizada la actualización de datos de contacto, el reclamante accede al apartado de su ***(…)***.

Sabemos con seguridad lo que el reclamante visualizaba en este apartado, ya que aportó una imagen junto con su reclamación a CaixaBank de 31 de octubre de 2021 (DOCUMENTO NÚMERO 3, que acompañaba al escrito de CaixaBank de fecha 18 de julio de 2023, elaborado en respuesta a la práctica de la prueba II)

En el hecho probado undécimo se ha incluido la descripción de dicha imagen:

- ***(…).***

(…)

(…)

Por esta vía, el reclamante no podía acceder al comprobante de la actualización de datos de contacto que había realizado ***(…)***, ya que ***(…)*** el comprobante de la transferencia realizada el día 1 de febrero por D. ***C.C.C.*.**

La única información a la que podía acceder era la siguiente:

- Que se trataba de una actualización de datos de contacto.
- Que se había realizado el 1 de febrero.
- Que el ***(…)***.

El problema es que los datos que podía visualizar no se correspondían con el contenido del comprobante al que accedía (transferencia realizada por D. ***C.C.C.***).

Tal y como destaca el hecho probado vigésimo primero el 12 de agosto de 2022 el reclamante no disponía aún del comprobante de la actualización de datos de contacto realizada el 1 de febrero de 2021 y en un escrito dirigido al servicio de atención al cliente de CaixaBank, de esa misma fecha, indicaba:

> *"Pero sigue una error que compromete los la protección de datos de los clientes caixa y si yo he recibo este documento quien ha recibido el documento* de ***(…)*** de contrato *mío con mis datos bancarias y personal?*

La posibilidad de tener acceso a un comprobante con los datos personales de otras dos personas, que no conocía, producía en el reclamante una pérdida de confianza en relación con el tratamiento de sus datos bancarios realizado por parte de CaixaBank.

En este punto, en opinión de CaixaBank, el reclamante tenía que haber buscado otras vías en su ***(…)*** para efectuar la comprobación de la actualización de sus datos de contacto realizada el 1 de febrero de 2021.

A través de dicha vía, la entidad bancaria afirma que habría podido comprobar que los ***(…)***.

No obstante, la información disponible a través de esta compleja vía combinada (consulta del ***(…)*** y el apartado de su ***(…)*** donde figuraba el ***(…)***), no le permitía disponer de todos los datos que figuraban en el comprobante.

CaixaBank, por su parte, en calidad de responsable del tratamiento, sí tenía acceso a totalidad de la información. La referida información figura en el documento 2, que acompañaba a su escrito de 13 de diciembre de 2022, elaborado en contestación al segundo requerimiento de información del Inspector.

En el mencionado documento figuran numerosos datos de carácter personal. Destacaremos tres de ellos: ***(…)***.

El reclamante no tenía disponibles esos tres datos de carácter personal.

El examen que efectúa la AEPD parte de un enfoque basado en los riesgos en los derechos y libertades de los interesados, poniendo el foco en la persona física cuyos datos están siendo tratados.

En este sentido, cabe recordar que el considerando 75 del RGPD, que parte de un enfoque amplio de los riesgos para los derechos y libertades de las personas físicas, prevé:

> *(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en par-*

ticular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; (…)" (el subrayado es nuestro)

Partiendo del enfoque descrito, se insiste en que el reclamante no tenía disponibles todos sus datos personales.

Por una parte, al no disponer del comprobante de la actualización de datos de contacto, se encontraba en una situación peor que cualquier otro cliente de la misma entidad bancaria que hubiera realizado la misma operación (actualización de datos de contacto) y sí hubiera podido acceder ***(…)*** al comprobante de dicha operación y a todos sus datos personales contenidos en el mismo.

El comprobante de una operación financiera tiene una gran importancia. Actúa como un espejo, que refleja el contenido de la operación bancaria que se ha efectuado.

- Por una parte, permite al cliente de la entidad bancaria verificar, nada más realizar la operación, que la misma se ha realizado de forma correcta. Permitiéndole, en caso contrario, reaccionar.
- Por otra, permite al cliente de la entidad bancaria acreditar frente a la propia entidad bancaria o frente a terceros, su firma, el día, la fecha y la hora exactas en que realizó la operación bancaria, así como el contenido de la misma.

Por otra, la falta de dicho comprobante le impedía, a su vez, disponer de algunos de sus datos de carácter personal, provocando una pérdida de control y disposición sobre datos de carácter personal que le concernían. Por ejemplo, no podía comprobar su exactitud, verificar que su firma era efectivamente su firma y que figuraba correctamente reflejada en el documento.

Tampoco podía acreditar frente a terceros ***(…)*** en el que había realizado la actualización de datos personales de 1 de febrero.

Dicha acreditación podía ser relevante, ya que se estaba modificando el ***(…).***

(…).

(…).

Como puede observarse, los derechos y libertades del reclamante podían verse afectados.

No se comparte la argumentación aportada por CaixaBank en su escrito de alegaciones a la propuesta de resolución, ya que implicaría que la entidad bancaria no tendría ningún incentivo de cara a garantizar la resiliencia del sistema o una rápida restauración. Circunstancia que contradice claramente lo dispuesto en el RGPD y lo indicado

en la *"Guía para la notificación de brechas de datos personales"* elaborada por la AEPD. En la que se indica:

> *"(…) el artículo 32.1 enumera específicamente un conjunto no exhaustivo de medidas de seguridad que se podrían contemplar para gestionar el riesgo mediante medidas de seguridad en un tratamiento, como son:*
>
> *• Medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad*
>
> *• Medidas para garantizar la resiliencia de los sistemas y servicios de tratamiento, y para dotar de capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico."* (el subrayado es nuestro).

Por los motivos expuestos, se rechaza la alegación formulada por CaixaBank.

Tal y como se indicará posteriormente, la actualización de datos de contacto que llevó a cabo el reclamante es una suerte de derecho de rectificación, que realiza directamante el cliente. Siendo necesario que se la entidad bancaria le facilite, tan pronto como ha firmado, un comprobante de la operativa bancaria realizada en el lugar diseñado para ello (en este caso, en el ***(…)***.

En relación con esta cuestión CaixaBank ha formulado diversas alegaciones relativas a que se considere que la actualización de datos de contacto realizada por el reclamante sea considerada como una suerte de derecho de rectificación, sintetizadas en la página 20 de su escrito de alegaciones a la propuesta de resolución:

> *"Incluso en el supuesto en que se considerase que la solicitud de modificación es "una suerte de derecho de rectificación" al que debía haberse dado respuesta, CAIXABANK había puesto a disposición del solicitante un sistema de acceso remoto, directo y seguro a los datos personales que garantizaba, de modo permanente, el acceso a su totalidad, habiendo informado adecuadamente al interesado acerca de este* ***(…)****, por lo que no puede considerarse que el acceso al mismo resulta una carga inapropiada para el interesado. Además, una vez* ***(…)****, CAIXABANK facilitaba a los interesados el documento correspondiente en un* ***(…)****, sensiblemente inferior al mes al que se refiere el artículo 12.3 del RGPD."*

En primer lugar, tal y como acaba de exponerse, ***(…)*** el reclamante no tenía acceso a todos sus datos de carácter personal.

En segundo lugar, cabe afirmar que la actualización de datos de contacto, ***(…)***, presenta claras semejanzas con el derecho de rectificación. No deja de ser un medio dispuesto por la entidad para que sus clientes puedan rectificar sus datos personales. Por este motivo, la propuesta de resolución hacía referencia a *"una suerte de derecho de rectificación".*

Si la entidad bancaria ha decidido diseñar un sistema en base al cual ***(…)***, esta Agencia no acierta a comprender la causa por la que el comprobante de una operación ban-

caria de estas características tenga que recibirse un mes más tarde (recordemos que el plazo de un mes en relación con el ejercicio de derechos del RGPD por un interesado es una previsión de máximos, las organizaciones deben dar respuesta al interesado lo antes posible).

Por otra parte, los párrafos reproducidos por CaixaBank en su escrito de alegaciones a la propuesta de resolución han sido sacados de contexto.

En dichos párrafos, relativos al fundamento de derecho VII, se estaba argumentando que el diseño ***(…)***, se había elaborado partiendo de un enfoque centrado en los intereses de la entidad bancaria y no del cliente. Se consideraba que, al efectuar dicho diseño, CaixaBank estaba trasladando al cliente un problema derivado de su operativa interna, considerando normal que dicho cliente no dispusiera del comprobante de la actualización bancaria que acababa de realizar hasta ***(…)*** después de haberla llevado a cabo.

En conclusión, a pesar de las alegaciones formuladas por CaixaBank cabe entender vulnerado el contenido del artículo 5.1 f) del RGPD.

VI Análisis de la vulneración del Artículo 32 del RGPD

En esta ocasión, va a analizarse el supuesto objeto de este procedimiento sancionador desde un otro ángulo o perspectiva diferente: si las medidas técnicas y organizativas de seguridad adoptadas fueron adecuadas.

CaixaBank en su escrito de alegaciones al acuerdo de inicio considera que tampoco se habría producido una vulneración del artículo 32 del RGPD. Una vez más, no se comparte la valoración realizada por la entidad bancaria.

El artículo 32 regula las medidas de seguridad aplicadas.

A continuación, se va a proceder a examinar el caso concreto objeto de este expediente sancionador.

1. *(…):*

De la información facilitada por CaixaBank en sus escritos de 13 de diciembre de 2022, 20 de febrero y 18 de julio de 2023 se desprende que ***(…)*** era clave, tanto para evitar que se produjese la brecha de datos personales como ***(…)***, que permitiera que detectar que algo anómalo acababa de suceder.

En el escrito de CaixaBank de 13 de diciembre de 2022 se indica, tal y como está recogido en los hechos probados vigésimo séptimo y cuadragésimo sexto:

> ***"(…).***
>
> ***(…)***
>
> ***(…).***
>
> ***(…)***
>
> ***(…)***

(…)

Por otra parte, en el escrito ***(…)***, DOCUMENTO NÚMERO 7 aportado por CaixaBank junto con su escrito de alegaciones, reflejado en el hecho probado vigésimo noveno se indica:

> "**MEDIDAS ADOPTADAS PARA MEJORAR LA ROBUSTEZ Y ELIMINACIÓN DE RIESGOS**
>
> ***(…)***

Asimismo, el contenido del escrito elaborado por CaixaBank el día 18 de julio de 2023 en relación con esta cuestión figura en el hecho probado trigésimo quinto. A continuación, se refleja exclusivamente la parte de su contenido relativa al periodo en el que se produjo la brecha de seguridad:

> ***"- (…):***
>
> ***(…).:***
>
> ***1. (…).***
>
> ***2. (…).***
>
> ***(…)."***

El último párrafo destaca que las dos transacciones u operaciones bancarias se realizaban. En el caso analizado:

- La actualización de datos de contacto del reclamante (primer documento).
- La transferencia realizada por D. ***C.C.C.***(segundo documento).

Por tanto, ***(…).***

(…)

(…)

(…)***.***

Posteriormente, el ******FECHA.1 (…).*** *Sin emb*argo, la brecha de datos personales objeto de examen en este expediente, y esto es importante, continuó pasando desapercibida ***(…).***

(…).

En el escrito de alegaciones a la propuesta de resolución, CaixaBank destaca:

> *"La AEPD intenta minorar el efecto de la medida adoptada, considerando que la misma se llevó a cabo con una intención distinta a la que generó el resultado: suprimir la posibilidad de ocurrencia de la brecha. A tal efecto, se remite al hecho probado séptimo, que entendemos que debe ser considerado el trigésimo segundo, dado que el séptimo no guarda relación con la* ***(…).***

*"CaixaBank decidió **(…)."***

Si bien lo indicado en este hecho probado puede considerarse cierto, debe no obstante indicarse que la interpretación del citado hecho efectuada por la AEPD resulta incompleta, de forma que las conclusiones alcanzadas como consecuencia del mismo pueden considerarse, con el debido respeto, sesgadas.

*Y es que una cosa es que mi representada no hubiera tenido conocimiento del hecho concreto motivador de la reclamación que dio origen al presente expediente y otra distinta que no quepa considerare que la **"(…)** no tuviera como objetivo, al margen de otros, el incremento de la seguridad de dichos sistemas.*

*Es decir, la AEPD utiliza el texto reproducido para tratar de considerar acreditado, aunque sin que conste elemento alguno que lo ampare, que la revisión efectuada por mi representada tenía como único y exclusivo **(…)**, considerando que dicha mejora en modo alguno podía tomar como elemento relevante la mejora de la seguridad de los mismos o la adopción de medidas que pudieran encaminarse a no ya minimizar, sino excluir, el (remoto) riesgo que los clientes de CAIXABANK podían sufrir en sus bienes y derechos. La AEPD simplemente adivina cual era la motivación de CaixaBank.*

Pero incluso, en el negado supuesto en que mi representada no hubiera tenido en cuenta dichos (remotos) riesgos, lo que CAIXABANK niega de plano, resultaría irrelevante la motivación que hubiera conducido a la adopción de la medida mencionada, siempre y cuando la misma hiciera desaparecer los citados riesgos.

Y es que, considera mi mandante, no es dable a la AEPD negar la relevancia de una medida para garantizar el derecho fundamental a la protección de datos por el mero hecho de que la misma no se haya adoptado el procedimiento que la AEPD considere oportuno, dado que lo importante es la minoración (en este caso eliminación) de los riesgos que el tratamiento puede producir en los interesados.

*La AEPD minimiza el efecto de la medida que se ha indicado haciendo referencia **(…)**. Sin embargo, y además de que es preciso indicar que la medida **(…)** del Reclamante se produjo en el mismo momento en que fue solicitada, no siendo relevante, desde el punto de vista de la normativa de protección de datos, que el **(…)** de la misma **(…)**, tal y como se analiza en la primera de las alegaciones contenidas en este escrito."*

En contestación a dicha alegación, se destaca que en el escrito de CaixaBank de 13 de diciembre de 2022, elaborado en contestación al segundo requerimiento de información del Inspector, la parte reclamaba afirmaba:

*"Por lo que se refiere a las acciones llevadas a cabo como consecuencia de este suceso concreto, tal y como se ha indicado, como solución y medida de robustez se **(…)**."*

Dicha contestación daba a entender a la AEPD que ***(…)*** había sido una acción adoptada por la entidad bancaria con el fin de solucionar la brecha de datos personales que se había producido el 1 de febrero de 2021.

El problema es que tal y como destaca el hecho probado trigésimo segundo ***(…)***, por lo que resultaba materialmente imposible que tal acción adoptada por la entidad bancaria se hubiera adoptado para solución a la brecha de datos personales.

El escrito de CaixaBank de 28 de junio de 2023, elaborado en contestación a la práctica de prueba I, aclaró que ***(…).***

Es decir, dicha ***(…)*** no fue una acción específica, adoptada por CaixaBank con el fin de solucionar la brecha de datos personales, de la que aún no era consciente.

Ignoramos la motivación que llevó a realizar dicha ***(…).***

Lo que sí que pone de manifiesto este hecho es que cuando el **(…)**, en un primer momento, eliminó el comprobante de la transferencia realizada por D. ***C.C.C. (…)***. Posteriormente, a medida que la AEPD actuaba (nuevo requerimiento de información de Inspector, acuerdo de inicio de expediente sancionador y tres prácticas de prueba) fue adoptando algunas medidas adicionales.

En el escrito de alegaciones a la propuesta de resolución, CaixaBank destaca:

> *"La segunda de las consideraciones guarda relación con el relato fáctico efectuado en el fundamento de derecho II de la Propuesta de Resolución, y en particular con las consecuencias derivadas de la modificación producida en los sistemas de mi representada en fecha* ******FECHA.1****.*
>
> *En efecto, la Propuesta enumera una secuencia fáctica de los hechos que considera relevantes en el presente procedimiento, deduciendo de los mismos una serie de conclusiones relacionadas con la supuesta tardanza de mi representada en conocer la existencia de la brecha de seguridad producida en este caso. Sin embargo, considera CAIXABANK que dichas conclusiones resultan, con el debido respeto, inexactas, por cuanto únicamente toman en consideración aspectos que pudieran resultar conducentes a apreciar la responsabilidad de mi mandante, sin tener en cuenta otros que resultan especialmente relevantes en el presente procedimiento, siendo el más importante de los mismos el anteriormente apuntado, acaecido el* ******FECHA.1*** *y consistente en la* ***(…).***
>
> *Y, entiende CAIXABANK que, si pretenden extraerse conclusiones objetivas de la secuencia fáctica producida en este caso, dicho hecho resulta capital, por cuanto, como se ha acreditado a lo largo del procedimiento y la propia Propuesta de Resolución reconoce,* ***(…)*** *(y desde la citada fecha), dado que es materialmente imposible que un cliente de mi representada* ***(…)****. Es decir, a partir de* ******FECHA.1****, la generación de una brecha de seguridad como la descrita en este procedimiento es materialmente imposible, por lo que no será tampoco posible la ruptura de la confidencialidad de los documentos generados como consecuencia de las transacciones ordenadas por los clientes de CAIXABANK.*
>
> *Y es que, al margen del supuesto de hecho enunciado, la Propuesta de Resolución, aun reconociéndolo, parece prestar poca atención y otorgar poca relevancia a un hecho de tal trascendencia que ha dado lugar a que cualquier reclamación similar a la formulada en este caso (recordemos que se trata de una*

única reclamación) devenga materialmente imposible desde una fecha casi dos años anterior a la adopción del Acuerdo de Inicio del presente procedimiento.

Y este hecho es un hecho indubitado que, sin perjuicio de cualesquiera valoraciones que pueda realizar la AEPD debería constar como conclusión del relato fáctico incorporado al fundamento de derecho II de su Propuesta de Resolución."

En primer lugar, la propuesta de resolución no reconoce que ***(…)*** imposibilitara materialmente que los hechos que dieron lugar a la brecha pudieran repetirse en el futuro. Sería afirmar que el riesgo existente tras la ***(…)*** era igual a cero y esta Agencia no lo considera así, tal y como se expondrá en esta resolución.

En segundo lugar, afirma CaixaBank, que la ***(…)*** es un hecho capital, ya que, en opinión de dicha entidad financiera, la brecha de datos personales era materialmente imposible ***(…).***

En relación con dicha alegación cabe afirmar que:

1.Si el ***(…)*** tenía una importancia capital, resulta sumamente negligente que (…)***.***

2.Asimismo, resulta llamativo que cuando, ***(…)*** y no como consecuencia de una ***(…),*** no hay elementos que indiquen que respondiera a una actuación proactiva de protección de datos.

3. También llama la atención que, a pesar de esta involucrado en la brecha de seguridad un elemento esencial y de capital importancia como ***(…)***, la entidad bancaria no determinara la causa de la brecha de datos personales hasta el ***(…)***).

4. Afirma CaixaBank que, tras ***(…)***, la brecha de datos personales es materialmente imposible.

Tal y como se expondrá en el fundamento de derecho VII, el diseño actual del sistema se apoya en ***(…)***. Si dicho ***(…)*** podría volver a producirse la brecha de datos personales.

CaixaBank ha considerado que (***…***), es la solución. Sin embargo, como se analizará posteriormente, ***(…)***, de tal manera que el problema no se ha solucionado en su raíz y, como consecuencia de ello, el riesgo sigue latente.

2. (…):

Dicho identificador único va a ser analizado en su condición de medida de seguridad.

La brecha de datos personales muestra que ***(…)*** ya que en el escrito de CaixaBank de 13 de diciembre de 2022 se destaca, recogido en el hecho probado vigésimo séptimo:

"(…)"

En relación con ***(…)***, el escrito de CaixaBank de 13 de diciembre de 2022 indica:

"(…).

(…).

(…)

(…)

(…)"

(…)***.***

Como puede apreciarse, ***(…)*** y esto provocó que el reclamante pudiera acceder al contenido de un justificante o resguardo de una transferencia realizada por otro cliente de dicha entidad bancaria.

En el escrito de alegaciones a la propuesta de resolución CaixaBank afirma:

> *"En relación con la supuesta vulneración del artículo 32 del RGPD, la AEPD viene a considerar en su fundamento de derecho VI que* ***(…).***
>
> *Y en este sentido, resulta necesario remitirnos a lo indicado en la primera de nuestras alegaciones:* ***(…)"***

En contestación cabe destacar que:

Como va a exponerse en el fundamento de derecho VII ***(…).***

Por otra parte, lo expuesto en este fundamento de derecho permite apreciar importantes carencias desde el punto de vista de medidas de seguridad en el momento en el que se produjo la brecha de datos personales objeto de este expediente.

Teniendo en cuenta todas estas circunstancias, no resulta posible afirmar, en modo alguno, que los riesgos hayan quedado reducidos a cero.

En el escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023 CaixaBank invoca la Sentencia del Tribunal Supremo de 15 de febrero de 2022.

Posteriormente, en el escrito de alegaciones a la propuesta de resolución, en la alegación relativa a una supuesta vulneración del principio de non bis in idem, CaixaBank vuelve a citar en su descargo la Sentencia del Tribunal Supremo nº 188/2022 de fecha 15 de febrero de 2022, aduciendo que en la misma determina que las medidas de seguridad son de medios y no de resultado, cuestión no discutida por la AEPD.

En primer lugar, hemos de señalar que esta sentencia se dicta al amparo de la normativa anterior al RGPD, en la que, conforme al sistema previsto en la LOPD y en el RLOPD, las medidas de seguridad estaban perfectamente estandarizadas. Hemos pasado de un sistema con medidas de seguridad estándar y estáticas para cualquier responsable a medidas de seguridad propias para cada organización (adaptadas a sus características e idiosincrasia), que considera los riesgos específicos de la entidad de que se trate; además ahora son dinámicas, de tal forma que no se agota con la implementación de las medidas de seguridad adecuadas al riesgo al inicio de los tratamientos, sino que debe de ir adaptándose a los riesgos que vayan apareciendo.

La nueva regulación prevista en el RGPD amplía notablemente las obligaciones del responsable del tratamiento y su ámbito de acción y responsabilidad, extendiéndose

ahora de manera clara a las actuaciones realizadas por sus encargados del tratamiento, que quedan dentro de su ámbito de responsabilidad.

En la sentencia no se delibera sobre la adecuación de las medidas de seguridad de la entonces responsable del fichero, esto es ***(…)***, dado que no fueron examinadas por la AEPD; se denunció a un encargado del tratamiento, quien no tenía implementadas las medidas de seguridad adecuadas, obligación que devenía de manera clara del art. 79 y siguientes del RLOPD, en la que se indicaba cuáles, en concreto, eran las medidas de seguridad que, conforme al Título VIII del citado Reglamento, debían implantar los encargados. No obstante lo anterior, además, la sentencia indica que no fue utilizado el sistema de forma adecuada, lo que hubiera evitado la filtración.

Y todo ello sin que ni en la resolución sancionadora ni en la sentencia se indique ni se deduzca que ***(…)*** tenía, por tanto, medidas de seguridad adecuadas o inadecuadas conforme al entonces Título VIII del RLOPD, ni que el hecho de que no fueran adecuadas le eximía de su responsabilidad recayendo sobre el encargado del tratamiento.

Segundo que, la Sentencia del Tribunal Supremo citada considera, en relación con una infracción del art. 9 de la LOPDP que "*la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado".*

Sobre ello precisa que "*No basta con diseñar los medios técnicos y organizativos necesarios también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de la diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso*".

En el supuesto que se está examinando en este procedimiento sancionador se considera que no había implantadas unas medidas de seguridad adecuadas al riesgo en los derechos y libertades de los interesados, aunque no hubiera habido brecha de datos personales.

Como se ha expuesto, ***(…).***

Por otra parte, ***(…).***

En conclusión, resultaría acreditada una infracción del artículo 32 del RGPD por la falta de medidas de seguridad adecuadas en el procedimiento establecido por la entidad bancaria.

- En relación con las medidas de seguridad (…):
    - (…), fecha en la que se produjo la brecha de datos personales.
    - El 1 de febrero de 2021 se realizaron ***(…),*** una actualización de datos de un cliente y una transferencia de otro cliente a un tercero.

- Cada las operaciones bancarias afectadas tenía que tener ***(…).***
- (…)***.***
- ***(…).***
- ***(…).***

- En relación con las medidas de seguridad ***(…)***:
  - ***(…).***
  - ***(…).***
  - ***(…).***
  - ***(…).***
  - Examinado el procedimiento implantado en la entidad se constata que no existían medidas de seguridad adecuadas en el sistema ***(…).***

VII Análisis de la vulneración del Artículo 25 del RGPD

En esta ocasión, va a analizarse el supuesto objeto de este procedimiento sancionador desde un tercer ángulo o perspectiva diferente: si fue respetado el principio de privacidad desde el diseño.

Se va a examinar en cuatro apartados:

1. Contenido del principio de privacidad desde el diseño y los condicionamientos internos para su cumplimiento.

2. Análisis del diseño del procedimiento que articula la tramitación de escritos presentados por los interesados de CaixaBank que afectan a la protección de datos de carácter personal.

3. Diseño del sistema de generación de la ruta de guardado (también denominada path HCP) de documentos relativos a la operativa bancaria de CaixaBank.

4. Análisis del diseño de lo que sucede en el sistema cuando se genera un código de error tras haber desactivado el versionado de archivado.

1. Contenido del principio de privacidad desde el diseño y los condicionamientos internos para su cumplimiento.

Tal y como se ha destacado en el fundamento de derecho III:

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 interesados.

El RGPD pretende lograr con la aplicación de sus disposiciones la protección de los derechos de los interesados. Por tanto, el foco debe dirigirse siempre a la identificación y evaluación de los riesgos en los derechos y libertades de los interesados, con la posterior adopción de medidas técnicas y organizativas de todo tipo destinadas a evitar su materialización. En este marco, las actuaciones han de ser preventivas y no reactivas, puesto que lo contrario el responsable del tratamiento no va a ser capaz de adelantarse a la materialización de los riesgos.

a) Enfoque en los riesgos de los derechos y libertades de los interesados.

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 y, en definitiva, el objetivo que pretende la normativa de protección de datos.

Partiendo de esto, cabe apreciar un claro ejemplo de que la perspectiva del riesgo que ha manejado CaixaBank en el caso analizado en este expediente sancionador no ha sido correcta. No ha estado focalizada en los interesados (que son todas las personas físicas cuyos datos personales trata, como responsable o como encargado del tratamiento, y no sólo respecto de sus clientes o empleados) sino en los riesgos para su propia organización.

Esta falta de enfoque adecuado originó que CaixaBank no identificara claramente a los afectados y que cada vez se considera a un afectado diferente:

1.En un primer momento, ***(…)***.

2.En un segundo momento, ***(…).***

3.(…).

Si no se identifica correctamente a los interesados o a los sujetos afectados (dato imprescindible para poder efectuar una identificación y valoración correcta de los riesgos que entraña el tratamiento para sus derechos y libertades), resulta imposible efectuar una adecuada protección de datos partiendo del contenido del artículo 25 del RGPD.

Esto se puede comprobar a través de los diferentes escritos de CaixaBank:

- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***

Por otro lado, también constituye un ejemplo de la falta del enfoque de riesgos en los derechos y libertades de las personas físicas y el incumplimiento del artículo 25 del RGPD, la falta absoluta de dicho enfoque impuesto por el RGPD en el procedimiento presentado por CaixaBank en sus alegaciones a la propuesta de resolución a los efectos de su defensa, en relación con la resolución de las reclamaciones presentadas por sus clientes, que luego se examinará pormenorizadamente.

Amén de que desconocemos la fecha de implantación de dicho procedimiento de resolución de reclamaciones, este no tiene un enfoque en la protección de los datos personales, sino que tiene una perspectiva bancaria, de seguros y de consumo. Tremendamente significativo es que en el procedimiento presentado no aparezca ni una sola vez la palabra “datos personales” o “protección de datos de carácter personal”.

Así, por una parte, es un procedimiento claramente inadecuado para proteger los derechos y libertades de los interesados, pues ninguna consideración a los riegos en los derechos y libertades de los interesados en protección de datos se considera por la entidad.

Pero, por otra parte, y lo más grave, es que, si este es el procedimiento que presentan para acreditar que cumplen con la normativa de protección de datos, si este es el procedimiento del que disponen, entonces no existe realmente un procedimiento para resolver las reclamaciones en materia de protección de datos.

b) Proactividad y no reactividad.

La Privacidad desde el diseño (en adelante, PDD) exige ser proactivo (tal y como se destaca en la Guía de Privacidad desde el Diseño de la AEPD) y no reactivo. Si la em-

presa u organización actúa de forma reactiva, como ha sucedido en este caso, no hay PDD.

Como ejemplo, ***(…).***

(…).

CaixaBank ha ido actuando de forma reactiva, no de forma proactiva, solventando las cuestiones, tanto de la reclamación como de los procedimientos diseñados, que se le iban requiriendo o planteando, no actuando de forma sistémica, previsora y global, tal y como exige la PDD. Esto ha ocurrido así porque CaixaBank no había realizado una protección de datos desde el diseño y por defecto. No tenía un protocolo establecido que permitiera tratar estos casos. Había definido sus procedimientos desde una perspectiva interna enfocada en el negocio y no en los datos personales y en las consecuencias que la falta de confidencialidad, integridad o disponibilidad que podrían ocurrir.

Volviendo al caso concreto de la reclamación, a raíz de la cual se ha analizado el procedimiento, por ejemplo, así lo reflejan los siguientes aspectos:

- El comprobante de la actualización de datos de contacto efectuada por el reclamante ***(…)*** no estuvo disponible ***(…).***
- ***(…)***
- ***(…).***
- ***(…).***
- ***(…).***

La actuación reactiva de CaixaBank sobrepasa en todo caso el supuesto concreto ya que, como hemos visto, también ha mudado cuestiones relativas al procedimiento que tenía establecido respecto de la ruta de guardado y la incidencia de los ceros a la izquierda. Y todo ello como consecuencia de la detección de este fallo en el diseño del procedimiento por la AEPD y puesto de manifiesto en el acuerdo de inicio.

Además, no ha previsto tampoco un procedimiento de resolución de las reclamaciones en materia de protección de datos, que debía estar pensado, planificado e implantado antes de que cualquier reclamación de protección de datos se presentase por un interesado. Es decir, en lugar de prever actuaciones ex ante que protejan los datos personales de los interesados se ha pasado a unas actuaciones ex post utilizando un procedimiento destinado a resolver reclamaciones que nada tienen que ver con la protección de datos de carácter personal, y, por ello determinando el incumplimiento del artículo 25 del RGPD.

CaixaBank no cuenta con un procedimiento adecuado para gestionar las reclamaciones de los interesados en materia de protección de datos (se configura como un servicio de atención al cliente con carácter general sin prever cuestiones en materia de protección de datos), con lo que, cuando reciben una reclamación cualquiera, se limitan aplicar el procedimiento que tienen establecido para resolver reclamaciones de clientes relativas a aspectos financieros, de seguros y de consumo.

Ello se pone de manifiesto, no sólo de la simple lectura de dicho documento cuya fecha y firma no constan, sino por el hecho indubitado de que no existe referencia algu-

na ni al RGPD ni a la LOPDGDD (si bien se citan otras disposiciones normativas aplicables a tal procedimiento) ni se menciona ni una vez la expresión “datos personales” o “protección de datos de carácter personal”.

Con lo único que cuentan actualmente, en atención a lo presentado en la fase de alegaciones a la propuesta de resolución, es con un procedimiento de reclamaciones de clientes en materia financiera, de seguros y de consumo y no con un procedimiento en materia de protección de datos. Por ello los interesados siguen estando desprotegidos.

No es el enfoque que persigue el RGPD, que exige unas actuaciones proactivas por parte de los responsables, como queda establecido en los principios (artículo 5.2 del RGPD).

2. Análisis del diseño del procedimiento que articula la tramitación de escritos presentados por los interesados de CaixaBank que afectan a la protección de datos de carácter personal.

En relación con esta cuestión, el RGPD otorga a las empresas un amplio margen de libertad a la hora de configurar su organización interna.

No impone una manera concreta en la que tengan que tramitar internamente los escritos que reciban de los interesados en materia de protección de datos de carácter personal. Si bien, exige que la actuación de las mismas sea respetuosa en todo momento con lo previsto en dicho Reglamento.

Para ello, resulta necesario que el procedimiento diseñado sea eficaz.

Ha de dar preferencia o prioridad a las reclamaciones, quejas, cuestiones, etc. planteadas por los interesados en materia de protección de datos. No debemos olvidar que se trata de un derecho fundamental, que debe ser protegido por el responsable del tratamiento, artículo 25.1 del RGPD in fine.

La AEPD no duda de que CaixaBank deba atender a diario otras cuestiones distintas a la protección de datos personales que plantean sus clientes. Sin embargo, aún en estas circunstancias, ha de garantizar que los escritos y reclamaciones relacionados con la protección de datos personales son debidamente atendidos, de forma ágil y correcta.

La falta de procedimiento de gestión de reclamaciones de los interesados en materia de protección de datos se acredita en la propuesta de resolución y se corrobora en la resolución en atención al procedimiento aportado por CaixaBank junto con las alegaciones a la propuesta de resolución a los efectos de su defensa.

Se desconoce, pues no se indica por CaixaBank, desde cuándo está vigente dicho procedimiento, desde cuándo es público, así como quién lo aprobado y conforme a qué parámetros.

Mas lo cierto es que, a los efectos de procurar su defensa, este es el procedimiento que nos indican que tienen establecido a los efectos de resolver las reclamaciones de los interesados en materia de protección de datos.

El referido procedimiento regula tanto el procedimiento de tramitación de las reclamaciones de los clientes de CaixaBank, como el Servicio de Atención al Cliente de dicha entidad financiera para resolver reclamaciones en materia financiera, de seguros y de consumo.

No se duda de la idoneidad de dicho procedimiento desde un punto de vista financiero, relativo a seguros o a consumo. Sin embargo, no resulta adecuado desde el punto de vista de la tramitación del reclamaciones o escritos relativos a la protección de datos de carácter personal, por una razón simple, ya que la protección de datos personales no ha sido considerada a la hora de elaborar y diseñar el referido procedimiento.

Las referencias normativas que figuran en el artículo 1 tienen relación con el ámbito financiero, de seguros y de litigios en materia de consumo, no con la protección de datos de carácter personal. No hay ninguna mención al RGPD, ni a la LOPDGDD, ni a los datos personales ni a la protección de datos de carácter personal.

Hay un artículo (artículo 22) relativo al Defensor del Partícipe y del Asociado, pero resulta llamativo que en el procedimiento de tramitación de reclamaciones no se mencione en ninguna ocasión al Delegado de Protección de Datos de CaixaBank. Tampoco está prevista la comunicación al Delegado de Protección de Datos ni en un momento previo, ni en un momento ulterior a la recepción de una reclamación de protección de datos por parte de un interesado.

Los artículos 2 letra f) y 6 letra c) hacen referencia a los Servicios de Reclamaciones de los supervisores (el Banco de España, la Comisión Nacional del Mercado de Valores y la Dirección General de Seguros y Fondos de Pensiones). No se menciona en ningún momento a la AEPD.

En el artículo 11 (Plazo para resolver la reclamación) se destaca que, en caso de disconformidad con la resolución del Servicio de Atención al Cliente, o si no se dicta ningún pronunciamiento dentro de los plazos previstos, el reclamante podrá acudir al Servicio de Reclamaciones del/los supervisores que correspondan (en referencia a los indicados en el párrafo anterior). Desde esta perspectiva, dado que es procedimiento que están aplicando, resulta comprensible que, a modo de ejemplo, en el caso concreto que se que originó la investigación y posterior tramitación de este expediente, el escrito de contestación de CaixaBank de 10 de noviembre de 2021 remitiera al reclamante al Banco de España, en lugar de a la AEPD, que es la competente en materia de protección de datos de carácter personal. Posteriormente, el Banco de España, envió la reclamación a esta Agencia.

El artículo 7 regula la configuración del Servicio de Atención al Cliente destacando en su apartado 4 que han de adoptarse las acciones necesarias para que el personal adscrito al mismo disponga de un conocimiento adecuado de la normativa sobre transparencia y protección de los clientes de servicios financieros. En este punto, resulta llamativa la total ausencia de referencia a la protección de datos de carácter personal.

Dicho personal va a ocuparse de la detección y tramitación de la reclamación, además de los conocimientos indicados, deberá tener conocimientos relativos a la protección de datos de carácter personal.

En conclusión, este procedimiento de gestión de reclamaciones de clientes en materia financiera, de seguros y de consumo no es un procedimiento adecuado en materia de protección de datos a los efectos de gestionar las reclamaciones de los; interesados que, en sí mismos y en los términos del RGPD, no han sido considerados en ningún momento y cuyos riesgos no están presentes, ni identificados, ni valorados en dicho procedimiento.

A continuación, vamos a repasar el procedimiento remitido y que aplica CaixaBank para tratar las reclamaciones en materia de protección de datos, y para ser más ilustrativos nos vamos a apoyar en la reclamación que fue el origen de la investigación:

1. (…).

2. (…).

(…):

a. (…).

b. (…).

c. (…).

d. (…).

3. ***(…):***

(…).

El RGPD ha supuesto el paso desde una concepción reactiva a una filosofía proactiva, reflejada en el artículo 5.2 del RGPD.

Como se destacaba anteriormente, la empresa u organización puede configurar su procedimiento para la tramitación de escritos presentados por los de clientes de CaixaBank que afectan a la protección de datos de carácter personal como considere que es más adecuado para su organización, pero se vuelve a insistir en que es importante que el mismo sea adecuado, eficaz y garantice el cumplimiento de lo dispuesto en el RGPD y en la LOPDGDD.

Dicho procedimiento debería ser un cauce que garantizase que, por ejemplo:

1. Cualquier escrito en materia de protección de datos sea detectado tan pronto como sea presentado.

2. El contenido del mismo sea puesto en conocimiento del Delegado de Protección de Datos de la empresa u organización (DPD), para garantizar que pueda ejercer su función como asesor cualificado desde un primer momento.

3. La tramitación se ajuste a lo planteado por el interesado.

4. La cuestión o cuestiones planteadas en el escrito se resuelvan de forma ágil y efectiva.

5. Existe un control posterior de la adecuación y eficacia respecto de la gestión de la reclamación en materia de protección de datos. Así como un seguimiento de la reclamación.

> Revisando, en su caso, el procedimiento diseñado, al objeto de adoptar medidas técnicas y organizativas de todo tipo que permitan cumplir adecuadamente con los requisitos del RGPD y una protección efectiva de los derechos y libertades de los interesados.

En conclusión, el examen del procedimiento establecido por CaixaBank para tratar aquellas cuestiones relacionadas con las quejas de los clientes y que ha presentado junto con sus alegaciones a la propuesta de resolución y que aplica para las reclamaciones de los interesados en materia de protección de datos, muestra que no está enfocado en el riesgo en los derechos y libertades de los interesados. Tampoco cumple con unas pautas mínimas, como las expuestas en el apartado anterior, para que fuera adecuado y eficaz. Asimismo, el procedimiento aplicado por CaixaBank para las reclamaciones de protección de datos (que es el relativo a reclamaciones financieras, de seguros y de consumo) no tiene previsto ningún tipo de sistema de control posterior, que permita detectar los posibles errores en las fases anteriores a fin de corregirlos lo antes posible.

El diseño escogido, no sería respetuoso con la privacidad desde el diseño, y supone una vulneración del artículo 25 del RGPD.

Tal y como se destacaba en el fundamento de derecho III, la investigación de la brecha de datos personales por parte de la AEPD ha sacado a la luz un problema interno de la organización, que es sancionable aún en el supuesto de que no se hubiera producido ninguna brecha de datos personales.

No cabe pensar que nos encontremos ante un caso puntual, ya que no hay un procedimiento interno para resolver las reclamaciones de los interesados en materia de protección de datos. A modo de ejemplo, la tramitación del escrito del reclamante de 12 de agosto de 2022, en el que expresaba su deseo de tener disponible el comprobante de la actualización de datos de contacto realizada el 1 de febrero de 2021 ***(…)***, corre la misma suerte que la reclamación de ***(…),*** a pesar de ser la segunda reclamación que se formulaba sobre la misma cuestión versando, asimismo, sobre el tratamiento de datos de carácter personal.

CaixaBank formula una alegación relativa al hecho de la que propuesta de resolución efectúe un análisis del diseño del procedimiento que articula la tramitación de escritos presentados por los clientes de CaixaBank que afectan a la protección de datos de carácter personal.

En relación con esta cuestión, en síntesis, destaca:

> *"La AEPD, de forma novedosa en la propuesta de resolución, y probablemente al apreciar la posibilidad de que pudiera considerarse que en el presente supuesto existe un claro bis in idem, afirma sin aportar prueba al respecto, que CAIXABANK carece de un procedimiento adecuado para la atención de las reclamaciones de sus clientes en materia de protección de datos, aun cuando únicamente dispone de un caso en que dicho procedimiento no se haya cumplido. Y todo ello sin requerir una sola vez a mi representada acerca de la existencia de dicho procedimiento. Se vulnera así la doctrina sentada en la sentencia de la Audiencia Nacional de 23 de diciembre de 2022, convirtiendo lo ocurrido en un caso concreto en vulneración sistemática, aun cuando tal circunstancia no se encuentre probada."*

En relación con la "*forma novedosa*" a la que hace referencia la parte reclamada, el acuerdo de inicio ya indica la existencia de una posible infracción del artículo 25 del RGPD por la falta de protección de datos desde el diseño y por defecto, a raíz de los indicios y evidencias obtenidas durante las actuaciones previas de investigación.

Además, y para mayor claridad se hace referencia en dicho acuerdo a la posible infracción del artículo 25 del RGPD, el fundamento de derecho VII advertía: *"Por todo ello, de conformidad con las evidencias de las que se dispone en este acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción (…)".*

Consecuencia de la instrucción del procedimiento y en atención a lo constatado en los hechos probados, se acredita la existencia de una infracción del artículo 25 del RGPD en relación con el procedimiento de gestión de las reclamaciones de los interesados en protección de datos, por su ausencia y aplicación subsidiaria de un procedimiento concebido para otra finalidad (ámbito financiero, de seguros y de consumo).

A mayor abundamiento, El Tribunal Constitucional (en adelante TC) ha venido señalando que *"el contenido esencial del derecho constitucional a ser informado de la acusación se refiere a los hechos considerados punibles que se imputan al acusado"* (STC 95/1995). Por el contrario, y a diferencia de lo que acontece con los hechos, el TC, en Sentencia 145/1993 advierte que la comunicación al presunto infractor de la calificación jurídica y de la eventual sanción a imponer no integra el contenido esencial del derecho a ser informado de la acusación. Hasta tal punto es importante la puesta en conocimiento de los hechos constitutivos de la infracción administrativa, que el TC ha declarado que las exigencias del artículo 24.2 de la CE se satisfacen fundamentalmente con la sola comunicación de los hechos imputados para poder defenderse sobre los mismos (STC 2/1987 y 190/1987). En esta línea el Tribunal Supremo, Sentencia de 3 de marzo de 2004, señala que *"la finalidad primordial del acuerdo de inicio es informar sobre los hechos imputados y no sobre la calificación jurídica, de lo que se encargará la propuesta de resolución".* (El subrayado es nuestro).

Destaca la entidad bancaria que la afirmación relativa al diseño del mencionado procedimiento se ha efectuado por parte de la AEPD sin haber aportado prueba al respecto.

No se comparte dicha afirmación. En el fundamento de derecho VII (Análisis de la posible vulneración del Artículo 25 del RGPD) se analiza esta cuestión en el apartado 1 haciendo referencia a los siguientes aspectos:

- Fundamento de derecho II (Íter de la reclamación).
- Hechos probados undécimo, duodécimo, decimotercero y decimoquinto.
- DOCUMENTO NÚMERO 1 aportado por CaixaBank el 18 de julio de 2023, en contestación a la práctica de la prueba II.

Además, lo acreditado por la AEPD en la propuesta de resolución ha sido corroborado en atención al procedimiento de reclamaciones de los clientes de CaixaBank aportado junto con las alegaciones a la propuesta de resolución.

Todo lo anterior evidencia la carencia de un procedimiento, protocolo o pautas adecuadas y eficaces, respetuosas con el RGPD, tanto para identificar y valorar los riesgos existentes en materia de protección de datos, lo que podría evitar que sucedieran inci-

dentes que atentaran contra los derechos y libertades de los interesados como para, y una vez que estos se hayan producido intentar tramitar las posibles reclamaciones (incluyendo su control y seguimiento posterior).

Esta AEPD considera que la entidad bancaria debería revisar dicho procedimiento partiendo de una perspectiva centrada en la protección de datos de carácter personal o bien diseñar un procedimiento específico, lo que desee, lo importante es que haya un procedimiento y que el mismo sea eficaz y adecuado a la normativa de protección de datos.

Asimismo, entre otras cuestiones, que deberá determinar conforme a su responsabilidad proactiva, debería asegurarse que los medios humanos del Servicio de Atención al Cliente de la entidad bancaria cuentan con conocimientos suficientes en materia de protección de datos de carácter personal.

Estas recomendaciones se formulan teniendo en cuenta que la parte reclamada afirma gestionar un *"ingente volumen de reclamaciones dirigidas a CaixaBank, que solo en materia de protección de datos personales* ***(…)****, a las que hay que añadir* ***(…)****."*

En su escrito de alegaciones a la propuesta de resolución, la entidad bancaria hace referencia a un *"(desafortunado) hecho puntual".*

Tal y como se indicaba al principio de este fundamento de derecho, hacia donde no miras, no ves.

No se trata de un error o fallo en el procedimiento, se trata de que existe una carencia del mismo, que como se ha indicado puede establecerse desde un procedimiento diferenciado o no, un protocolo o unas pautas que sean respetuosas con los derechos y libertades de los interesados y adecuadas a la normativa de datos personales. La realidad revela la carencia de ese procedimiento ideado por la organización (en este caso, CaixaBank). Esa forma de actuar no se ajusta a lo dispuesto en el artículo 25 del RGPD.

Tal y como se ha destacado, la ausencia de un procedimiento adecuado al que se ha hecho referencia se puede ver reflejada a través de las distintas actuaciones que CaixaBank realiza.

La entidad bancaria concluye sus alegaciones a la propuesta de resolución en relación con este punto haciendo referencia a la Sentencia de la Audiencia Nacional de 23 de diciembre de 2022 (recurso 104/2021).

En primer lugar, la mencionada sentencia ha sido recurrida en casación.

En segundo lugar, el fundamento de derecho quinto de la misma da respuesta a una alegación relativa a la total desconexión del objeto del procedimiento en que recayó la resolución y las reclamaciones formuladas.

Dicha desconexión, tal y como se ha expuesto, no existiría en dicho caso. Tanto la reclamación presentada por D. ***A.A.A.*** en el Departamento de Conducta de Entidades del Banco de España el 10 de febrero de 2022, como su escrito de 12 de agosto de

2022 están íntimamente relacionadas con cómo atiende CaixaBank los escritos presentados por sus clientes que afectan a la protección de datos de carácter personal.

Por otra parte, dicho apartado de la propuesta sí se apoya en elementos de prueba y en pruebas practicadas durante la tramitación del expediente, tal y como se acaba de exponerse.

3. Diseño del sistema de generación de la ruta de guardado (también denominada path HCP) de documentos relativos a la operativa bancaria de CaixaBank:

Antes de proceder a dicho análisis, es necesario destacar que nos encontraríamos ***(…).***

(…).

(…).

Como consecuencia de ello, el comprobante de la transferencia ***(…).***

3.1. Cómo se genera la ***(…):***

A continuación, se procede al análisis del diseño del sistema creado por CaixaBank para ***(…)***.

Partiendo de las explicaciones sobre el ***(…)***, reflejadas en el hecho probado cuadragésimo segundo, cabe destacar lo siguiente:

(…)

(…)

(…)

Como puede observarse:

1. (…).

2. ***(…):***

- ***(…)***
- ***(…)***

3.2***. (…):***

- CaixaBank había optado ***(…).***

  Era posible la coincidencia de (…) en el mismo milisegundo.

- En cuanto al valor aleatorio, CaixaBank había ***(…)***

  (…):

  (…)

- ***(…).***

3.3. Diseño del sistema (…) existente en la actualidad:

- (…)

3.4 *Probabilidad de que dicha* **(…):**

Tal y como se ha reflejado en el hecho probado cuadragésimo octavo, CaixaBank considera que es ***(…).***

En la Diligencia de 18 de julio de 2023, que forma parte del expediente, se destaca que:

"(…)."

En el Informe solicitado por la Instructora del PS/00020/2023 en el marco de la práctica de la prueba de fecha 18 de julio de 2023, elaborado por el Inspector, cuyo contenido ha sido reproducido en el hecho probado quincuagésimo, se destaca:

"• (…)

CONCLUSIONES

(…)

En el escrito de alegaciones a la propuesta de resolución CaixaBank ha formulado varias alegaciones relativas al informe del Inspector que acaba de ser reproducido. De forma resumida, destaca:

> *"La valoración efectuada por el Inspector en su Informe, obrante como Anexo a la Propuesta de Resolución, además de carecer por completo de rigor desde el punto de vista del cálculo de probabilidades, resulta inadecuada, toda vez que parte del* ***(…)*** *en la actualidad, sin tomar en consideración que sólo un número reducido de dichas operaciones generan documentos y que el volumen de actividad de mi representada cuando se produjo la brecha detectada era sensiblemente inferior al actual, habiéndose aportado esta cifra por mi representada en respuesta al tercer requerimiento de prueba efectuado por esa AEPD."*

En relación con dichas alegaciones cabe destacar:

La estadística es una rama de las matemáticas que facilita aproximaciones, al objeto de tratar de determinar lo que puede llegar a suceder en la realidad. En este sentido, conviene recordar que CaixaBank realizó en el escrito de alegaciones al acuerdo de inicio un cálculo aproximado (considerando la franja horaria en la que la actividad bancaria podía ser mayor ***(…)***).

El Inspector, por su parte, efectuó, de una forma muy sencilla, el cálculo de (…)**.** Dicho cálculo también podría haberse efectuado utilizando fórmulas matemáticas mucho más complejas, lo cual no le resta validez al cálculo matemático efectuado.

Al objeto de desacreditar el cálculo efectuado por el Inspector, CaixaBank ha utilizado argumentos cuyo contenido no se comparte en absoluto y, en ocasiones, pueden inducir a confusión.

Por ejemplo, en su escrito de alegaciones a la propuesta de resolución la parte reclamada destaca, en relación con el informe del Inspector de 18 de julio de 2023:

> *"(iii) ha usado datos que no coinciden con la fecha en que se produjo la brecha a la que se refiere el presente expediente, pese a haberse requerido esa información por parte de la Instructora; y "*

Pues bien, tengamos como referencia que la fecha de la brecha de datos personales se produjo el 1 de febrero de 2021.

Así, en el marco de la práctica de la prueba, tras el envío a CaixaBank de la práctica de la prueba III, se solicita informe al Coordinador de la Inspección con fecha 17 de julio de 2023, a la vista de la información aportada previamente por CaixaBank en el expediente.

Hemos de resaltar que no se tenía información en ese momento sobre el número de transacciones por segundo que se realizaron en CaixaBank a fecha 1 de febrero de 2021, ni había sido aún aportada al expediente por la parte reclamada.

De hecho, en la Nota interior de fecha 17 de julio de 2023, enviada al Coordinador de la Inspección precitada, solicitando informe se indicaba lo siguiente:

> ***"(…)"***
>
> *Se solicita, que la vista de la información aportada por CAIXABANK, S.A. en este expediente, elabore, con carácter urgente, informe acerca de la probabilidad de que se produjera una* ***(…).***
>
> *Asimismo, se solicita que indique si ese cálculo de probabilidad se podría aplicar al número o la media de operaciones por segundo correspondiente a otra fecha distinta del 1 de junio de 2023."*

Como puede comprobarse, la solicitud del informe se efectúa, a la vista de la información aportada previamente por CaixaBank en el expediente.

Por otra parte, el 18 de julio de 2023, día en el que el Inspector elaboró su informe, aún no se había recibido el certificado de CaixaBank indicando el número de transacciones por segundo que se realizaron en CaixaBank a fecha 1 de febrero de 2021.

El mencionado certificado fue firmado por D. ***D.D.D.*** ese mismo día (18 de julio de 2023) a las 19:04:09 (tal y como consta en el propio certificado). Se presentó en el Registro de la AEPD ese mismo día a las 19:47:02 y fue registrado al día siguiente (19 de julio de 2023) a las 09:24:39.

Encontramos otro ejemplo de estas técnicas de defensa, cuando CaixaBank afirma que "*sólo una parte, y muy reducida, de las operaciones que se realizan en la operativa bancaria de CAIXABANK* ***(…)***"

Por una parte, obsérvese que dicha cantidad *"muy reducida"* a la que hace referencia el escrito de las alegaciones a la propuesta de resolución resulta totalmente indeterminada. A pesar de ello, CaixaBank no duda en afirmar en el escrito de alegaciones a la propuesta de resolución:

"todas estas operaciones deberían haber sido excluidas a limine del cálculo efectuado por el inspector."

Por otra, es un nuevo ejemplo de cómo trata de minimizarse un riesgo. Así, la parte reclamada ***(…)***. Se quiere trasladar la idea de que es tan reducido el riesgo, que resulta casi inexistente. Lo cual, como veremos, es falso.

CaixaBank ahora afirma que ***(…)*** en dicha entidad bancaria es reducido. Aunque fuera así, si entre estas operaciones se encuentran las transferencias, como sucede en la práctica, el volumen diario de este tipo de operaciones en CaixaBank es muy elevado. Y ello en atención, entre otros parámetros, al número de clientes de la entidad, una de las mayores de España.

(…).

De esta forma, independientemente ***(…).***

Segundo, porque el sistema está mal diseñado al no focalizarse en los riesgos en los derechos y libertades de los interesados, lo que hace que, en todo caso, el riesgo esté presente independientemente ***(…).***

En cualquier caso, dejando aparte las técnicas de defensa que acaban de ser indicadas, ***(…)***, como pretende dar a entender la parte reclamada.

Las alegaciones relativas a si el cálculo del Inspector era o no exacto no puede desviar la atención sobre el hecho de que ese riesgo existe, sea en mayor o menor medida. A modo de ejemplo, se puede citar el caso de la reclamación presentad ante la Agencia en el que se evidencia que no nos encontramos ante una mera posibilidad, ya que la brecha de datos personales se materializó en la práctica.

En relación con esta cuestión, la Guía para la notificación de brechas de datos personales destaca lo siguiente:

> *"En cuanto a la probabilidad, no se trata de determinar la probabilidad de que la brecha de datos personales se materialice, porque obviamente en esta situación la brecha ya se habría materializado, sino determinar si existe la posibilidad de que las consecuencias se materialicen con un nivel de severidad alto o muy alto. Para determinarlo, se deberá tener en cuenta las medidas técnicas y organizativas aplicadas antes de que se produjera la brecha y las acciones tomadas a posteriori para evitar que el daño se materialice."* (el subrayado es nuestro)

Volviendo al diseño del sistema por parte de CaixaBank, una entidad bancaria, de su relevancia, disponía, tanto de capacidad como de medios suficientes como para haber llevado actuaciones encaminadas a garantizar que el diseño del sistema por el que había optado fuera robusto:

- ***(…).***
- ***(…).***

Por otra parte, ***(…).*** En este caso, ignoramos si el 1 de febrero de 2021 el sistema se encontraba en el momento de máxima carga cuando se produjo la brecha de datos personales, pero lo que sí sabemos con seguridad es que dicha brecha de datos personales tuvo lugar.

CaixaBank trata de convencernos de que la probabilidad de que se produjera la brecha de datos personales era infinitesimal, eso podría llevar a la parte reclamada a afirmar que la brecha de datos personales era imprevisible y quedar exonerada de toda responsabilidad.

Si partimos del diseño por el que había optado CaixaBank, no cabe afirmar que la brecha de datos personales fuera imprevisible.

1.(…).

2. (…).

3.(…).

Partiendo de estos tres elementos, no cabe afirmar que la brecha de datos personales fuera imprevisible.

A lo ya expuesto, cabe añadir un cuarto elemento:

4. (…).

En conclusión, los cuatro elementos expuestos muestran que la brecha de datos personales no era imprevisible. Lo que sí cabe apreciar es una clara falta de previsión por parte de la entidad bancaria a la hora de diseñar su sistema.

(…).

Son cuestiones que se apuntan y que invitan al análisis por parte de la entidad bancaria.

4. Análisis del diseño de lo que sucede en el sistema cuando se genera un código de error tras haber desactivado el versionado de archivado:

CaixaBank afirma que la solución al problema generado por la brecha de datos personales ***(…).***

En la práctica de prueba II se solicitó a CaixaBank ***(…).***

CaixaBank ha indicado que ***(…).***

4.1 *Evolución del diseño relativo* ***(…):***

Vamos a analizar ***(…).*** Para ello se va a analizar el procedimiento utilizado por la entidad bancaria, a través de las actuaciones realizadas y, como ejemplo, se va a utilizar la reclamación presentada ante la Agencia:

4.1.1. Período de tiempo durante el cual el ***(…).***

Las dos operaciones bancarias (en el caso analizado, actualización de datos de contacto del reclamante y transferencia de D. ***C.C.C.***) se ejecutaban y registraban. Sin embargo, ***(…).***

(…), produciéndose la brecha de datos personales.

(…).

4.1.2. Período comprendido ***(…).***

Periodo posterior a la ***(…).***

Primer documento (en nuestro caso, la actualización de datos de contacto). ***(…).***

Segundo documento (en nuestro caso, la transferencia) ***(…).***

La solución prevista por CaixaBank ***(…)***:

A. (…).

> CaixaBank afirma que el cliente tendría el comprobante de la actualización de datos de contacto ***(…).***

Con esta solución se generaba el comprobante de la actualización de datos de contacto, pero el cliente no podía disponer del mismo ***(…).***

La entidad bancaria está trasladando un problema derivado de su operativa interna al cliente, que no puede disponer del comprobante de la operación que acaba de realizar ***(…).***

El diseño adoptado no resulta transparente. ***(…)***

En segundo lugar, el hecho de no poder disponer del comprobante de la actualización de datos de contacto ***(…).***

Aparentemente ***(…)***, pero ha de tenerse en cuenta que puede generar confusión al cliente, que no sabe cuándo se ha producido realmente la actualización de datos de contacto. Por otra parte, la inmediatez, en cuanto a la disponibilidad del comprobante pueda ser fundamental en aquellos supuestos en los que cliente tenga que acreditar la modificación realizada frente a terceros o frente a la propia entidad.

Por tanto, el diseño no resultaba idóneo al no sustentarse en un enfoque basado en el cliente, en el enfoque en los riesgos en sus derechos y libertades y su protección efectiva. Resolvía un problema a la entidad bancaria, pero generaba los perjuicios antes expuestos al cliente.

B. En el caso de ***(…):***

(…).

En este caso, se optaba por un diseño que traslada el problema de la entidad bancaria al cliente.

En este supuesto ***(…).***

El inspector en su informe de 18 de enero de 2023 destacaba:

> ***(…).***

Se comparte la opinión del Inspector, con una solución que pone la carga en el cliente, que ***(…)***.

El cliente puede necesitar acreditar de forma fehaciente y urgente haber realizado dicha transferencia. Actualmente no resulta tan sencillo que te atiendan en una oficina de una entidad bancaria.

Al igual que en caso anterior, tampoco se considera un diseño transparente, ***(…).***

4.1.3. ***(…):***

Al primer documento ***(…).***

Cabe apreciar que este diseño es mejor que el anterior desde el punto de vista del cliente.

(…).

En conclusión, la actuación de CaixaBank en este ámbito no es la idónea, partiendo de la perspectiva del artículo 25 del RGPD.

Como consecuencia ***(…).***

Posteriormente, cuando ***(…).***

La adopción de dicha medida era positiva de cara al futuro (…)**,** pero no para una brecha que había tenido lugar en el pasado (***…).***

Prueba de ello es que ***(…).***

En cuanto al diseño, en el momento en el que se produjo la brecha de datos personales no era el idóneo.

En la segunda fase, se observa un diseño que está más enfocado en los riesgos de la organización y sus problemas, que en los riesgos del cliente.

En la tercera fase, se ha mejorado el sistema, ***(…).***

. Análisis de otras alegaciones formuladas por CaixaBank en su escrito de 20 de febrero de 2023:

En su escrito de alegaciones de 20 de febrero de 2023 CaixaBank destaca:

(…)

(…).

En el escrito de 13 de diciembre de 2022, elaborado por CaixaBank en contestación al segundo requerimiento del Inspector, reproducido en el hecho probado vigésimo séptimo, afirma que ***(…)***:

"(…)."

En la ***(…)*** se recogen las siguientes propiedades deseables en una ***(…):***

(…):

- ***(…)***
- ***(…).***
- ***(…).***

- ***(…).***
- ***(…).***
- ***(…).***
- ***(…).***
- ***(…)***

Continuando con el análisis de las alegaciones formuladas al acuerdo de inicio, junto con el escrito de 20 de febrero de 2023 CaixaBank aporta numerosos documentos. Se reproducen dos párrafos que hacen referencia a los mismos:

"(…)."

Resulta necesario aclarar, que, si bien se valora positivamente que CaixaBank disponga de un corpus normativo en materia de seguridad, la existencia del mismo no garantiza de forma automática el cumplimiento por parte de la entidad bancaria de lo dispuesto en el artículo 25 del RGPD, máxime cuando el cumplimiento de este precepto exige medidas técnicas y organizativas de todo tipo y no sólo de seguridad. Es necesario analizar si su organización a diario funciona de una manera adecuada, a la vista de lo dispuesto en dicho artículo. Verificar que los procedimientos internos están bien diseñados y permiten garantizar la protección de los numerosos datos de carácter personal, que son tratados a diario por dicha entidad financiera, con las suficientes garantías.

Continuando con el análisis del escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023, en el mismo CaixaBank destaca que:

"(…)"

No se discute que eso sea así, pero dichos métodos o medios que sean empleados tendrán que ser eficaces y cumplir adecuadamente su labor de protección de los datos de carácter personal que se está llevando a cabo, resultando conformes con lo dispuesto tanto en el RGPD como en la LOPDGDD.

A continuación, el escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2023 afirma:

> *"Es decir, la obligación de cumplimiento del artículo 25.1 del RGPD no es concebida por el EDPB como una obligación de resultado, en el sentido de que pueda considerarse que los resultados derivados de su realización sean conformes con lo establecido en el RGPD, sino como una obligación de análisis, de forma que si un responsable del tratamiento ha llevado adecuadamente a cabo el mismo, aun cuando el resultado pudiera ser erróneo a juicio de la autoridad de control, no existiría una vulneración del principio de Privacidad desde el Diseño, sino, en su caso, de alguno de los principios establecidos en el artículo 5 del RGPD o de las normas en que dichos principios se concretan.*
>
> *Por decirlo gráficamente, y como ya se ha apuntado anteriormente, es posible que de la realización del análisis del tratamiento efectuado por un responsable se derive un alcance del cumplimiento del deber de transparencia que posteriormente no sea considerado suficiente por parte de la autoridad de control, entendiendo ésta que la información facilitada a los interesados no es la sufi-*

ciente. Sin embargo, ello no implicaría que la entidad en cuestión no hubiera cumplido su obligación de adoptar las medidas necesarias para el cumplimiento del principio de transparencia, sino que dicho principio no se consideraría por la AEPD respetado plenamente. Es decir, el resultado de esa apreciación sería una vulneración de los artículos 5.1 a), 13 y 14 del RGPD, pero no una vulneración de su artículo 25. No cabría sancionar la falta de privacidad desde el diseño, sino el supuesto incumplimiento del principio o de la norma en que se concreta.

Y esta circunstancia es la que concurre en el presente caso: mi mandante ha analizado y valorado plenamente todas las medidas que correspondía adoptar para garantizar el cumplimiento de los principios establecidos en el artículo 5 del RGPD.

Cuestión distinta, negada por mi representada, será que la AEPD aprecie que una de las medidas de seguridad adoptadas por mi mandante es insuficiente. En ese caso podrá apreciarse que no se han adoptado las medidas adecuadas, pero en ningún caso esa supuesta insuficiencia podrá considerarse como un incumplimiento de lo preceptuado por el artículo 25.1 del RGPD."

No se comparte la interpretación expuesta por CaixaBank, que minimiza el alcance del artículo 25 del RGPD hasta tal punto, que no resulta compatible con lo dispuesto en el RGPD. Tal y como se ha destacado anteriormente, el Reglamento establece un sistema completo destinado garantizar plenamente los derechos y libertades de los ciudadanos.

A pesar de que en el escrito de alegaciones se ubica en el apartado relativo al artículo 32, al estar más vinculado al diseño, se va a analizar en este apartado la siguiente alegación:

"(…)."

No se comparte que la concurrencia de factores fuera imprevisible tal y como se ha expuesto anteriormente.

Si en una entidad del tamaño de CaixaBank, con un volumen de operaciones que puede alcanzar una media de ***(…),*** se diseña ***(…):***

- ***(…).***
- ***(…).***

(…).

(…), debería estar previsto que pudiera llegar a pasar esta coincidencia de (…), a fin de evitar que en la práctica llegara a producirse una brecha de datos personales.

Afirma ahora CaixaBank en sus alegaciones a la propuesta de resolución que no todas las operaciones bancarias son generadoras de documento, sin aportar si quiera un porcentaje aproximado de las mismas. Como se ha indicado anteriormente, trata de minimizar un problema existente en el afán de salir exonerada de toda responsabilidad.

En el caso analizado, ***(…).***

(…)***.***

No se aprecia previsión. Además, demuestra que CaixaBank está aceptando e intentando corregir las deficiencias detectadas y comunicadas por esta Autoridad de Control. Tampoco una actuación proactiva, tal y como exige el artículo 5.2 del RGPD, sino una actitud fundamentalmente reactiva. Se van resolviendo los problemas a medida que se detectan, se van tapando agujeros a medida que la entidad es consciente de los mismos.

En conclusión, resultaría acreditada una infracción del artículo 25 del RGPD por la falta de privacidad del diseño en el procedimiento establecido por la entidad bancaria.

- En relación con la adecuada y correcta aplicación de la Privacidad desde el diseño prevista en el artículo 25 del RGPD:

    - El enfoque de la entidad bancaria en los riesgos no es el propio de la Privacidad desde el Diseño del artículo 25 del RGPD.

      No enfoca en los riegos en los derechos y libertades de los interesados (clientes o no de la entidad cuyos datos personales traten) sino en los riesgos en la organización.

    - La actuación de CaixaBank en relación con el diseño de los procedimientos objeto de este sancionador y antes descritos no ha sido previa, reflexionada y proactiva en ningún momento tal como mandata el artículo 25 del RGPD, sino fundamentalmente improvisada y reactiva. Además, incluso a lo largo de este expediente CaixaBank no ha pensado en una situación ex ante.

- (…)***.***

  Lo ahora diseñado ***(…).***

- En relación con el ***(…)*** de documentos relativos a la operativa bancaria de CaixaBank.

    - En cuanto al sistema diseñado en el momento de la brecha de datos personales para lograr ***(…):***

        - ***(…).***
        - ***(…).***
        - ***(…).***

          (…).

        - ***(…).***

(…).

- ***(…).***
- ***(…).***

En cuanto al sistema diseñado en el momento posterior a la brecha de datos personales para lograr ***(…)***, indicar que se han realizado modificaciones en el sistema (consecuencia de las incidencias detectadas por la AEPD y puestas de manifiesto en los dos requerimientos de información del Inspector, el acuerdo de inicio y las solicitudes de prueba) parciales, reactivas y sin abarcar una revisión completa del sistema.

En cuanto a la probabilidad de ***(…)*** resulta que dicha probabilidad que es considerablemente más alta que la calculada por CaixaBank ***(…).***

En cuanto ***(…):***

- ***(…).***
- ***(…).***
- ***(…).***

VIII Supuesta vulneración del principio de proporcionalidad

En relación con esta cuestión, en el escrito de alegaciones al acuerdo de inicio de 20 de febrero de 2022 se indica:

> *"De este modo, resulta necesario que por el Órgano Sancionador se proceda a evaluar que en el presente supuesto nos encontramos ante una sola reclamación formulada por un solo cliente de mi mandante, no referida a sus propios datos, sino a los de un tercero y relacionada con un supuesto determinado y concreto, el acceso a un documento ajeno al Reclamante, siendo además así que dos de las infracciones establecidas por el RGPD para la conducta mencionada son de las incluidas en su artículo, el 83.4 del RGPD.*
>
> *Sin embargo, la AEPD no duda en este caso en imponer a mi mandante tres sanciones, subsumibles las unas en las otras, por una cuantía total de cinco millones de euros, acudiendo para la determinación del importe de la sanción a criterios completamente genéricos, que mi mandante rechaza de plano. Al propio tiempo, nuevamente, mi mandante desea poner de manifiesto como los criterios utilizados para la agravación de una de las infracciones son, literalmente, reproducidos respecto de las restantes, lo que no hace sino poner de manifiesto la concurrencia que la propia AEPD aprecia en su Acuerdo respecto de las tres infracciones, en que los argumentos resultan perfectamente intercambiables entre sus fundamentos de derecho VI, IX y XII."*

Ya se ha dado respuesta a las alegaciones relativas a la supuesta vulneración del principio de non bis in idem y al concurso medial.

El escrito de alegaciones a la propuesta de resolución vuelve a insistir en que se trata de una única reclamación:

> *"Mi representada no ha tenido ninguna otra reclamación relacionada con hechos similares a los acaecidos, pese al enorme volumen de reclamaciones que la misma tramita y, del mismo modo, tampoco la AEPD ha tenido conocimiento de otra reclamación de similares características. Todo ello no hace sino poner de manifiesto que ni la probabilidad de concurrencia de las circunstancias del caso es la pretendida por la Agencia ni es posible considerar potenciales perjudicados a todos los clientes de CAIXABANK."*

En cuanto al primer párrafo de la alegación al acuerdo de inicio y el párrafo relativo a la propuesta de resolución que acaban de ser reproducidos, muestran el problema de fondo que se ha producido en este procedimiento. CaixaBank considera que todo el contenido de este expediente se reduce a una sola reclamación, que afecta a un solo cliente.

Amén de que lo reclamado en este caso concreto afecta a dos clientes de la Caixa y a un tercero, y no sólo a un cliente, la operativa establecida por la Caixa como responsable del tratamiento afecta a todos sus clientes. Lo expuesto en los fundamentos de derecho anteriores refleja que, en dicha entidad bancaria, en el momento en el que se produjo la brecha de datos personales, existían importantes deficiencias tanto en las medidas de seguridad como en aspectos relacionados con el diseño. Y todo ello se ha podido determinar a partir de la reclamación formulada, poniéndose de manifiesto importantísimas deficiencias en el procedimiento establecido por la entidad bancaria.

La AEPD ha sido consciente de dichos problemas, que resultan sancionables por sí mismos (aún sin brecha de datos personales), como consecuencia de la investigación de una brecha de datos personales, que los ha sacado a la luz.

Dichas deficiencias son problemas estructurales, que afectan a la entidad financiera en su conjunto. En el momento en el que la entidad financiera ***(…)*** *(hecho probado vigésimo cuarto*), debería haberse parado a pensar sobre las causas últimas del ***(…)*** que se había producido y su alcance. Dicho análisis, le habría permitido determinar las medidas adecuadas que era necesario adoptar para ***(…)***, con el fin de garantizar una adecuada protección de los datos de carácter personal de sus clientes.

Frente a ello, en un primer momento no hizo nada. Consideró que ***(…),*** era suficiente. Posteriormente, al comenzar a indagar la AEPD y a realizar requerimientos de información, fue adoptando medidas, de forma reactiva y muchas veces improvisada, (…).

Por otra parte, cabe recordar que el art. 83 del RGPD que dispone 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 disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual (…)".

Asimismo, cabe destacar que según disponen "*las Directrices 04/2022 sobre el cálculo de las multas bajo el RGPD"* Versión 2.0 Adoptadas el 24 de mayo de 2023:

"139. Por lo tanto, la autoridad de control verificará que el importe de la multa es proporcional tanto a la gravedad de la infracción como al tamaño de la empresa a la que pertenece la entidad que cometió la infracción, y que la multa impuesta no excederá de lo necesario para alcanzar los objetivos perseguidos por el RGPD." (el subrayado es nuestro).

Así, la multa será proporcional en atención a la gravedad de la infracción del caso concreto, examinada en la resolución administrativa, considerando todos los elementos de juicio precisos en el supuesto concreto en relación con las previsiones del art. 83.2 del RGPD, incluyendo el tamaño, el volumen de negocio y la viabilidad de la empresa de que se trate.

Asimismo, la multa debe ser disuasoria, a los efectos de desincentivar la comisión de una nueva infracción y alentar el cumplimento del RGPD.

Sobre este particular, las Directrices 04/2022 establecen que:

"143. Una multa es disuasoria cuando impide que una persona infrinja los objetivos perseguidos y las normas establecidas por el Derecho de la Unión. Lo decisivo a este respecto es no solo la naturaleza y el nivel de la multa, sino también la probabilidad de que se imponga. Cualquier persona que cometa una infracción debe temer que se le imponga la multa de hecho. Aquí existe una superposición entre el criterio de disuasión y el de eficacia." (el subrayado es nuestro).

En relación con la infracción del artículo 5.1 f) del RGPD, dicho Reglamento en su artículo 83.5 dispone:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, en relación con las infracciones de los artículos 25 y 32, que tienen entidad propia, tal y como se ha indicado en el fundamento de derecho III, el artículo 83.4 del RGPD prevé:

"4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;"

Dado lo expuesto hasta el momento, no cabe considerar que ninguna de las tres sanciones (multa de 2.000.000 de euros, como consecuencia de la vulneración del artículo 5.1f) del RGPD, multa de 1.500.000 de euros, como consecuencia de la vulneración del artículo 25 del RGPD y multa de 1.500.000 de euros, como consecuencia de la vulneración del artículo 32 del RGPD) resulten desproporcionadas. Amén del volumen de negocios de la entidad, todas ellas se ajustan a los límites del art. 83.4 y 5 del RGPD.

Respecto a la cuantía de la sanción, en la propia web de CaixaBank:https://www.CaixaBank.com/comunicacion/noticia/CaixaBank-gana-3-145-millones-de-euros-en-2022--un-29-7-mas-en-base-comparable-gracias-a-la-fortaleza-comercial-y-las-sinergias-de-la-integracion_es.html?id=43875#:~:text=Corporativo-,CaixaBank%20gana%203.145%20millones%20de%20euros%20en%202022%2C%20un%2029,las%20sinergias%20de%20la%20integraci%C3%B3n&text=Jos%C3%A9%20Ignacio%20Goirigolzarri%20y%20Gonzalo,consejero%20delegado%20de%20CaixaBank%20respectivamente, se encuentra disponible el documento *"NOTA DE PRENSA – RESULTADOS 2022. Valencia, 3 de febrero de 2023.* En dicho documento puede consultarse la cuantía del margen bruto de la cuenta de resultados, que alcanza los ***(…)*** 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 CaixaBank, y de la proporcionalidad en el cálculo de la cuantía de las tres sanciones conforme a lo dispuesto en el artículo 83.4 del RGPD.

En el escrito de alegaciones a la propuesta de resolución CaixaBank afirma:

"(…) es preciso tener en cuenta que las imputaciones dirigidas contra mi representada parten de una premisa, ***(…)****.*

Teniendo en cuenta esta premisa, si bien, como se ha indicado, CAIXABANK considera que con todo ello queda desvirtuada la imputabilidad a la misma de las sanciones a las que se refiere la Propuesta de Resolución, mi mandante considera que, cuanto menos, su responsabilidad en el presente caso quedaría enormemente minorada."

A la vista del contenido de esta resolución, no cabe afirmar que todas las imputaciones dirigidas contra CaixaBank partan del cálculo efectuado por el Inspector el 18 de julio de 2023.

En el fundamento de derecho VII (Análisis de la vulneración del artículo 25 del RGDPD), se ha puesto de manifiesto la ***(…)***, así como otras deficiencias desde el punto de vista del diseño, circunstancia que en ningún caso justificaría la enorme minoración del importe de dicha sanción pretendida por CaixaBank. En cuanto a las otras dos infracciones (artículo 5.1.f) y artículo 32 del RGPD) las alegaciones formuladas por CaixaBank a la propuesta de resolución no incluyen ningún elemento que lleve a la minoración de las sanciones reflejadas en la propuesta de resolución.

Asimismo, alega al acuerdo de inicio CaixaBank lo siguiente:

> *"• Finalmente, el Acuerdo de Inicio, aprecia, nuevamente reproduciendo literalmente su motivación en los fundamentos de derecho VI, IX y XII que la sanción debe agravarse como consecuencia de la vinculación de la actividad de mi mandante con la realización de tratamientos de datos. Respecto de este punto, es preciso en primer lugar que la AEPD, nuevamente, toma en consideración el giro o tráfico de mi representada en cada una de las agravantes adoptadas. Así, en la primera de ellas esa circunstancia es tomada en consideración para reforzar la potencial afectación de los hechos (sin perjuicio de que, como se ha dicho, una afectación potencial no es sancionable conforme al RGPD, tal y*

como ha declarado la Audiencia nacional); al propio tiempo, respecto de la negligencia, se agrava la conducta de mi mandante al entender que por su sector de actividad se le debe exigir una especial diligencia; finalmente, se considera que el giro o tráfico de mi mandante está vinculado a la realización de tratamientos, lo que debe suponer esa triple agravación derivada de este hecho. Es decir, a juicio de la AEPD cuando una entidad financiera comete una supuesta infracción su conducta ha de verse triplemente afectada por el mero hecho de su pertenencia al sector financiero, lo que difícilmente puede considerarse acorde con el principio de proporcionalidad."

En relación con esta cuestión, el escrito de alegaciones a la propuesta de resolución destaca:

"Respecto de las agravantes apreciadas, mi representada no puede sino reiterar que no es posible establecer el apriorismo consistente en considerar que cualquier infracción de la normativa de protección de datos ha de ser incrementada, cuando no multiplicada en cuanto a la determinación del importe de la sanción en los supuestos en que la encartada pertenezca al sector financiero y sea una gran empresa, por considerar que tal circunstancia, por sí sola, agrava la negligencia en su actuación y determina además, por el solo sector de actividad de la encartada un incremento de la responsabilidad. Mi representada, por el contrario podría igualmente indicar que el incidente acaecido no sólo tenía una mínima probabilidad de producirse, sino que además representa un solo caso entre los ***(…)****, lo que debería redundar en una atenuación, y no en una agravación del reproche sancionador dirigido contra la misma."*

No se comparte la alegación formulada. Tal y como se ha indicado anteriormente, en este expediente se habrían cometido tres infracciones diferenciadas (artículo 5.1 f), artículo 25 y artículo 32 del RGPD).

En cada una de dichas infracciones distintas, cabe la posibilidad de considerar como agravante el hecho de que CaixaBank sea una gran empresa que lleva a cabo el tratamiento diario de un volumen importantísimo de datos de carácter personal. En este sentido el escrito de alegaciones a la propuesta de resolución afirma *"representa un solo caso* ***(…)****"* y en otro apartado añade *"el ingente volumen de reclamaciones dirigidas a CaixaBank, que solo en materia de protección de datos personales en el año 2022 fueron* ***(…)****, a las que hay que añadir un total de* ***(…)*** *ejercicios de derechos*").

A la vista del ingente volumen de datos que tramita dicha entidad bancaria, se recuerda el contenido de la Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (rec. 63/2006) en la que se destaca que: "*cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".*
No es lo mismo que idéntica infracción sea cometida por una gran entidad, como CaixaBank que afirma efectuar "***(…)"*** de tratamientos datos de carácter personal, con la posibilidad afectar a los derechos y libertades de un elevadísimo número de personas físicas, que por un pequeño autónomo. Así, la multa proviene de la individualización de la infracción, tal y como dispone el art. 83 del RGPD.

En el escrito de alegaciones a la propuesta de resolución CaixaBank destaca:

"(…) mi representada considera necesario dar por reproducido lo ya indicado en sus alegaciones al Acuerdo de Inicio: la AEPD en su Propuesta de Resolu-

ción no hace sino aplicar para la determinación de las agravantes concurrentes en el presente caso los elementos que ha tenido en cuenta para la determinación de la aplicación del tipo sancionador, aplicando éstos así tanto como elemento del tipo cuanto como agravante del mismo."

No se aprecia que se hayan considerado como agravantes elementos contenidos en el tipo de las infracciones sancionadas. Lo que sí puede considerarse como tales serían circunstancias que concurren en los hechos probados y que les dotan de una mayor gravedad, como, por ejemplo, la duración de la infracción. Sirva de ejemplo la falta de disponibilidad del comprobante de la actualización de datos de contacto por parte del reclamante, que se prolongó hasta el ***(…)***, tal y como refleja el hecho probado décimo, con la consiguiente falta de disponibilidad de todos los datos personales del reclamante que figuran en el mismo.

Por otra parte, continuando con el análisis de las alegaciones a la propuesta de resolución, a juicio de CaixaBank resulta ilustrativo de la supuesta arbitrariedad en la que, en su opinión, incurre la actuación de la AEPD, que la propuesta de resolución considere que la infracción de mayor cuantía corresponde a la supuesta vulneración del artículo 5.1 f) del RGPD teniendo en cuenta, que dicha propuesta hace referencia única y exclusivamente al supuesto concreto enjuiciado.

Asimismo, considera curioso que la mayor de las sanciones se aplique a la supuesta vulneración el citado artículo (art. 5.1f) del RGPD), cuando el riesgo de brecha de confidencialidad desapareció por completo el día ***FECHA.1, casi dos años antes del inicio del procedimiento sancionador.

CaixaBank entiende que la AEPD toma un caso concreto para extraer una consecuencia que, en su opinión, no ha quedado en modo alguno acreditada y considera que ese caso se extiende a una supuesta situación sistémica.

En contestación a dicha alegación, la conducta de CaixaBank ha supuesto una clara y grave vulneración del principio consagrado en el artículo 5.1f) del RGPD.

El artículo 83.2 del RGPD, prevé la necesidad de descender al caso concreto, considerando las circunstancias concurrentes que están presentes y que determinan, en este supuesto, la mayor gravedad considerada por la AEPD en relación con la vulneración del artículo 5.1.f) del RGPD.

En primer término, resulta necesario destacar que la multa por importe de 2.000.000 de euros no corresponde a única brecha de datos personales, sino a dos: una consistente en una pérdida de confidencialidad y otra por pérdida de disponibilidad.

Además, en cuanto a la brecha de datos personales por pérdida de confidencialidad, resulta de especial gravedad no sólo la exhibición a un tercero (la parte reclamante) de datos personales de dos personas, sino todo el tiempo durante el cual ha tenido a su disposición la parte reclamante el justificante de una transferencia con los datos personales de dos personas (…), lo que incrementa el riesgo de sufrir daños en los derechos y libertades de esas dos personas, entre otros, una eventual suplantación de identidad. Una vez que los datos personales salen del ámbito de control del responsable del tratamiento, quien tiene acceso a los mismos puede, aunque no deba, compartirlos, difundirlos o utilizarlos, incrementándose el riesgo en los derechos y libertades de los interesados por, por ejemplo, la difusión indiscriminada que puede hacerse a través de las nuevas tecnologías.

También, y en cuanto a la brecha de datos personales por pérdida de disponibilidad no es de recibo que la parte reclamante haya estado más de ***(…)*** sin tener acceso a los datos personales que le concernían en relación con la actualización de datos personales. La absoluta pérdida de control y disposición de los datos personales que le concernían a la parte reclamante por dilatadísimo periodo de tiempo es de una gravedad inmensa, máxime cuando a la parte reclamada no se le ha ocurrido en ningún momento, hasta que le fue requerido por la AEPD en la práctica de la prueba I, poner a disposición del reclamante ***(…)*** realizada el 1 de febrero de 2021***.***

Por último, hemos de significar que desde la fase de traslado de la reclamación, pasando por las actuaciones previas de investigación, las alegaciones al acuerdo de inicio, la fase de práctica de pruebas, hasta las alegaciones a la propuesta de resolución se ha mantenido una constante. CaixaBank ha tratado de minimizar lo que ha sucedido, de negar la existencia del riesgo (afirmaba que la probabilidad de reiteración de la brecha era ***(…***); sigue negando que se haya producido una brecha de disponibilidad, durante toda la tramitación del expediente (…) de manera evidente al cliente de la tercera entidad bancaria al que ni siquiera ha considerado, llegando, incluso, a afirmar que los riesgos derivados del tratamiento han quedado reducidos a cero con la simple ***(…)***.

Este enfoque resulta totalmente contrario al artículo 5.1f) del RGPD, que pretende garantizar que el tratamiento de los datos de carácter personal se lleve a cabo de tal manera que se garantice una seguridad adecuada de dichos datos.

Si se parte de una perspectiva caracterizada por tratar de hacer creer que lo que ha sucedido no es grave, cuando sí que lo es, y negar la existencia del riesgo, cuando dicho riesgo sigue existiendo, resulta imposible garantizar que el tratamiento se lleve a cabo de tal manera que se garantice una seguridad adecuada de los datos personales.

IX Cuestiones generales relativas a la protección de datos de carácter personal

El artículo 4.2 del RGPD, define «tratamiento» como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."*

En el presente caso, de acuerdo con lo establecido en dicho artículo, consta la realización de un tratamiento de datos personales, toda vez que CaixaBank, para la prestación de sus servicios como entidad financiera, realiza de forma diaria el tratamiento de numerosos datos de carácter personal. Por tanto, la parte reclamada está obligada a cumplir con las obligaciones que, para el responsable del tratamiento, se disponen en el RGPD y en la LOPDGDD.

El artículo 4 apartado 12) del RGPD define, de un modo amplio, las *"violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen 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."*

En el presente caso, consta una brecha de datos personales de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad.

Hay que señalar que la recepción de una denuncia sobre una brecha de datos personales no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f).

Por su parte, el artículo 32 del RGPD, relativo a la seguridad del tratamiento, prevé la obligación del responsable y del encargado del tratamiento de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Finalmente, cabe destacar el artículo 25 del RGPD, que regula la protección de datos desde el diseño y por defecto. Dicho precepto exige al responsable del tratamiento la obligación de aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, 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 RGPD y proteger los derechos de los interesados.

X Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

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

En este fundamento de derecho, se entiende reproducido el contenido del fundamento de derecho V (Análisis de la vulneración del Artículo 5.1f) del RGPD en su integridad, en el que detallan las causas por las que la AEPD entiende que, en el caso examinado en este expediente sancionador, se ha vulnerado el contenido del artículo 5.1f) del RGPD.

XI Tipificación de la infracción del artículo 5.1.f) del RGPD y calificación a los efectos de la prescripción

La citada infracción del artículo 5.1 f) del RGPD supondría la comisión de una de las infracciones tipificadas en el artículo 83.5 del RGPD, que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas",* dispone:

"5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"*

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 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

XII Sanción por la infracción del artículo 5.1.f) del RGPD

Se considera que la infracción en cuestión es muy grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Se tienen en cuenta las siguientes circunstancias como agravantes:

Artículo 83.2 a) del RGPD:

a) Naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

El fundamento jurídico II (Íter de la reclamación) se refleja el prolongado período de tiempo durante el cual ***(…).***

El hecho de que el reclamante tuviera acceso a dicho comprobante durante ese dilatadísimo período de tiempo aumentaba los riesgos en los derechos y libertades del ordenante y del beneficiario cuyos datos personales figuraban en el mismo (suplantación de identidad, etc.).

Por otra parte, la brecha de datos personales, que tanto tiempo tardó en ser detectada (un año y cuatro meses después de haberse producido y consecuencia del traslado de la reclamación formulado por la AEPD) y resuelta por CaixaBank, tuvo una consecuencia que ha supuesto un perjuicio para el reclamante: **(…)** que había realizado el 1 de febrero de 2021.

En el caso analizado en este expediente sancionador, el reclamante realizó una actualización de datos de contacto, que consistió, tal y como se refleja en el hecho probado segundo, en:

1. ***(…).***

2. ***(…).***

Resulta indudable la importancia que tiene el teléfono móvil actualmente en el ámbito bancario, ya que actúa, entre otras cuestiones, como:

- Medio a través del cual las entidades financieras contactan con sus clientes.
- Dispositivo electrónico que permite realizar tanto consultas como operaciones bancarias de todo tipo. En ocasiones, permite la firma de documentos relativos a operativas bancarias, recibir información de gastos realizados, etc.
- Juega un papel clave como elemento de seguridad a la hora de realizar compras online (doble factor de autenticación). De hecho, la mayoría de los clientes lo utiliza para poder completar con éxitos dicho tipo de compras.

(…).

Tal y como se refleja en el fundamento de derecho II (Íter de la reclamación) ***(…).***

CaixaBank afirma en sus alegaciones que no se ha producido una brecha de disponibilidad:

> ***"****Sin embargo, dicho sea con el debido respeto, la citada brecha de disponibilidad no tuvo lugar en la práctica****: (…).***
>
> ***(…).***
>
> ***(…).***
>
> *Por todo ello, y frente a lo indicado en el Acuerdo de Inicio, la brecha producida responde a lo señalado por mi mandante en las respuestas dadas a los requerimientos efectuados por esa AEPD, no tratándose en ningún caso de una brecha de disponibilidad."*

No se comparte la argumentación defendida por CaixaBank. El reclamante se ha visto afectado por una brecha de disponibilidad, ***(…).***

El Derecho Fundamental a la Protección de Datos de Carácter Personal está conformado por un haz de facultades que el ordenamiento jurídico dota al interesado a los efectos *"garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado",* en palabras del Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre de 2000, rec. 1463/2000.

No sólo la actualización efectiva de los datos de contacto, una suerte de derecho de rectificación realizada directamente por el cliente, tiene que llevarse a cabo, sino que

debe de justificarse su realización a este. Y ello a los efectos de que mantenga un verdadero control sobre sus datos personales tal y como se ha explicado anteriormente, especialmente si tiene que reaccionar frente a la entidad, por ejemplo, ante una eventual falta de actualización de sus datos personales (y los perjuicios que se podrían derivar al respecto). Como se ha explicitado a lo largo de la resolución administrativa en el justificante se contenían todos los datos personales que el cliente tenía que tener disponibles.

No resulta admisible que la entidad bancaria pretenda trasladar las consecuencias derivadas de su falta de actividad en este aspecto al cliente.

En sus alegaciones, CaixaBank parece dar a entender que dicha falta de actividad por su parte ha de ser suplida con comprobaciones que tiene que realizar el cliente o que existe una obligación por parte del mismo de ponerse en contacto con el personal de la entidad bancaria al objeto de que le faciliten el comprobante de la operación bancaria que había realizado.

Sin embargo, dicho comprobante ***(…).***

Artículo 83.2 b) del RGPD:

Intencionalidad o negligencia:

En este caso cabe apreciar una negligencia grave por parte de CaixaBank.

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto. (Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (rec. 63/2006)).

No cabe apreciar rigor ni exquisito cuidado en el hecho de que CaixaBank detectara la brecha de datos personales ***(…).***

Tampoco se observan en el hecho de que ***(…).***

Asimismo, resulta llamativo que ***(…).***

El hecho de que se considere que una brecha no es comunicable, no exime a la entidad de cumplir con las obligaciones relativas al registro de la misma de forma diligente y sin dilaciones excesivas.

Asimismo, tampoco cabe calificar de diligente la gestión ***(…).***

El hecho de que la entidad bancaria obviara ***(…)*** tampoco acreditan un comportamiento diligente por parte de dicha entidad bancaria.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los criterios que establece el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

Artículo 76. 2 b) de la LOPDGDD

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

CaixaBank es una importante entidad bancaria que realiza de forma habitual y continua el tratamiento de numerosos datos de carácter personal, tanto de sus propios clientes, como de los clientes de otras entidades bancarias cuyos datos figuran en el operativa bancaria que se está llevando a cabo, tal y como sucede con las transferencias.

Conoce y aplica la normativa en materia de protección de datos personales.

En consecuencia y a efectos del cumplimiento de los requisitos legalmente establecidos, el ejercicio de dicha actividad implica necesariamente el conocimiento y aplicación de la normativa vigente en materia de protección de datos personales.

A tenor de los hechos expuestos, se considera que corresponde imputar una sanción a la parte reclamada por la vulneración del Artículo 5. 1 f) del RGPD.

La sanción que corresponde imponer es de multa administrativa por un importe de 2.000.000 € (dos millones de euros).

XIII Artículo 25.1 RGPD

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: (el subrayado es nuestro)

“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 res-

ponsable 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 para los derechos y libertades de los interesados, 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 Comité Europeo de Protección de Datos (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 in-*

teresados 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 (protección de datos desde el diseño y por defecto) *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 completo 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, se encuentra íntimamente vinculada a una actitud proactiva y no reactiva. La actuación de CaixaBank en este caso ha sido fundamentalmente reactiva, a golpe de traslado, requerimientos del Inspector, acuerdo de inicio y escritos de práctica de prueba.

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 ten-

dente a visualizar, respecto de un tratamiento de datos personales, los riesgos en los derechos y libertades de las personas físicas.

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.

Por otra parte, en la ya mencionada Guía de Privacidad desde el diseño de la AEPD se establecen diversas orientaciones: (el subrayado es nuestro)

"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".

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. (…)".

En este fundamento de derecho, se entiende reproducido el contenido del fundamento de derecho VII (Análisis de la vulneración del Artículo 25 del RGPD) en su integridad, en el que detallan las causas por las que la AEPD entiende que, en el caso examinado en este expediente sancionador, se ha vulnerado el contenido del artículo 25 del RGPD.

XIV Tipificación de la posible infracción del artículo 25 RGPD y calificación a los efectos de la prescripción

La citada infracción del artículo 25 del RGPD supondría la comisión de una 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."

XV Sanción por la infracción del artículo 25 del RGPD

Se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Se consideran las siguientes circunstancias como agravantes:

Artículo 83.2 a) del RGPD:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

Resulta grave que una entidad bancaria, con la relevancia y volumen de operaciones, diarias de CaixaBank ***(…).***

Asimismo, se considera grave, que a pesar de haber detectado ***(…).***

Artículo 83.2 b) del RGPD:

b) la intencionalidad o negligencia en la infracción;

Si bien la Agencia considera que no hubo intencionalidad por parte de la entidad bancaria, concluye que su negligencia fue grave.

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, acceso a datos sensibles o el riesgo evidente de una pérdida patrimonial para el cliente que sufre las consecuencias.

Vuelve a destacarse el rigor y el exquisito cuidado en el manejo de datos de carácter personal mencionado en la Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (rec. 63/2006).

Dicho esto, no cabe apreciar diligencia ***(…).***

La ejecución de ese esquema, en el caso concreto que estamos analizando, tuvo las siguientes consecuencias:

1.No se detectó que se trataba de una reclamación sobre una brecha de datos personales, tramitándose como una supuesta reclamación por unos recibos indebidamente cargados.

En el escrito de CaixaBank de fecha 10 de noviembre de 2021 (hecho probado decimotercero), se destaca:

"***(…).***"

Examinado el contenido de la documentación presentada por el reclamante junto con su escrito de reclamación, no se acierta a comprender qué comprobaciones pudo haber efectuado la persona que elaboró el contenido de dicho escrito, cuando tramitó una brecha de datos personales como una reclamación por unos recibos indebidamente cargados en una cuenta bancaria.

2. (…)***.***

3. Como tercera consecuencia, una entidad financiera no puede gestionar una brecha de datos personales si no conoce de su existencia (a pesar de haber recibido una reclamación al respecto).

Tampoco cabe apreciar diligencia en el ***(…).***

En este segundo caso, como se ha visto en el fundamento de derecho VII se estableció un sistema poco transparente, que traslada al cliente los problemas de la entidad bancaria.

En el caso de las transferencias, el hecho de que se optara por una solución ***(…),*** da idea de improvisación, es lo opuesto a un enfoque orientado al cliente y no puede ser considerado como un comportamiento diligente.

En este sentido las Directrices 4/2019 del CEPD disponen respecto del principio de lealtad que "*Los responsables del tratamiento no deben transferir los riesgos de la empresa a los interesados".*

Tampoco cabe apreciar rigor y exquisito cuidado cuando ***(…).***

Es decir, determinados factores que contribuyeron a la brecha de datos personales continúan latentes y el ***(…)*** permitiría que volviera a producirse la suma de factores que ocasionó la brecha de datos personales.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los criterios que establece el apartado 2 del artículo 76 "Sanciones y medidas correctivas" de la LOPDGDD:

Artículo 76. 2 b) de la LOPDGDD

Se considera la siguiente circunstancia como agravante:

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

CaixaBank, en su actividad empresarial, lleva a cabo de forma habitual y continua el tratamiento de numerosos datos de carácter personal, tanto de sus propios clientes, como de los clientes de otras entidades bancarias cuyos datos figuran en el operativa bancaria que se está llevando a cabo, tal y como sucede con las transferencias.

En consecuencia y a efectos del cumplimiento de los requisitos legalmente establecidos, el ejercicio de dicha actividad implica necesariamente el conocimiento y aplicación de la normativa vigente en materia de protección de datos personales.

A tenor de los hechos expuestos, se considera que corresponde imputar una sanción a la parte reclamada por la vulneración del Artículo 25 del RGPD.

La sanción que corresponde imponer es de multa administrativa por un importe de 1.500.000 € (un millón quinientos mil euros).

XVI Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece: (el subrayado es nuestro).

"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."

En este fundamento de derecho, se entiende reproducido el contenido del fundamento de derecho VI (Análisis de la vulneración del Artículo 32 del RGPD) en su integridad, en el que detallan las causas por las que la AEPD entiende que, en el caso examinado en este expediente sancionador, se ha vulnerado el contenido del artículo 32 del RGPD.

XVII Tipificación de la infracción del artículo 32 del RGPD y calificación a los efectos de la prescripción

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

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

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

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."

XVIII Sanción por la infracción del artículo 32 del RGPD

Se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Se tienen en cuenta las siguientes circunstancias como agravantes:

Artículo 83. 2 a) del RGPD:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

Tal y como se ha expuesto en el fundamento de derecho VI (Análisis de la vulneración del Artículo 32 del RGPD), CaixaBank no había cumplido adecuadamente con la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en su procedimiento, tal y como prevé el artículo 32 del RGPD.

Resulta grave que el ***(…).***

En un contexto en el que las medidas de seguridad resultaban deficientes, es grave que las brechas de datos personales pudieran producirse, tanto en relación con operaciones
(…) (como fue el caso de la actualización de datos de contacto realizada por el reclamante) ***(…)*** (este fue el caso de la transferencia realizada por D. ***C.C.C.***). Es decir, ***(…).***

Finalmente, resulta grave que ***(…)***, ya que estamos hablando de una entidad financiera con un elevado número de operaciones ***(…).***

Artículo 83. 2 b) del RGPD:

b) la intencionalidad o negligencia en la infracción;

Si bien la AEPD considera que no hubo intencionalidad por parte de la entidad financiera, estima que su actuación muestra una negligencia grave.

La deficiencia de las medidas de seguridad implantadas por CaixaBank provocaba consecuencias en una parte del ***(…).***

Resulta llamativo que al generarse ***(…).***

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los criterios que establece el apartado 2 del artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD:

Se considera la siguiente circunstancia como agravante:

Artículo 76. 2 b) de la LOPDGDD

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

CaixaBank, en su actividad empresarial, lleva a cabo de forma habitual y continua el tratamiento de numerosos datos de carácter personal, tanto de sus propios clientes, como de los clientes de otras entidades bancarias cuyos datos figuran en el operativa bancaria que se está llevando a cabo, tal y como sucede con las transferencias.

En consecuencia y a efectos del cumplimiento de los requisitos legalmente establecidos, el ejercicio de dicha actividad implica necesariamente el conocimiento y aplicación de la normativa vigente en materia de protección de datos personales.

A tenor de los hechos expuestos, se considera que corresponde imputar una sanción a la parte reclamada por la vulneración del Artículo 32 del RGPD.

La sanción que corresponde imponer es de multa administrativa por un importe de 1.500.000 € (un millón quinientos mil euros).

XIX Imposición de medidas

En primer lugar, se dará respuesta a la alegación formulada por CaixaBank a la propuesta de resolución en relación con la imposición de medidas.

Frente a la propuesta de imposición de medidas formulada en la propuesta de resolución, la parte reclamada muestra sorpresa por la exigencia contenida en la fundamentación jurídica de la propuesta de resolución, al no indicar la AEPD por qué es precisa su adopción ajustando sus actividades de tratamiento a las disposiciones del RGPD; reitera la parte reclamada que con la ***(…)*** es suficiente para que se evite el resultado analizado por la AEPD, reduciendo a cero el riesgo en los derechos y libertades para los interesados; asimismo, aduce a que ha ***(…)***. Alega que ***(…)***. En resumen, que no puede deducir cuáles son las medidas correctivas, lo que le genera indefensión.

Sobre este particular se han de indicar una serie de cuestiones.

La primera es que la AEPD ha dispuesto desde el acuerdo de inicio, pasando por la propuesta de resolución, la posibilidad de imponer medidas. Y ello en atención a los hechos recogidos en el acuerdo de inicio y a los hechos probados consignados en la propuesta de resolución que determinaban la necesidad de que la parte reclamada ajustase sus tratamientos a las disposiciones del RGPD.

Y todo ello en virtud de los poderes correctivos otorgados a la AEPD como autoridad de control en el artículo 58.2 del RGPD.

De hecho, en este caso, se han impuesto específicamente las medidas con la propuesta de resolución, momento procedimental en que se han fijado los hechos probados que determinan con claridad meridiana cuáles han sido los incumplimientos del RGPD en los que ha incurrido la parte reclamada, tras una fase de prueba, compuesta por tres prácticas de prueba.

Ninguna sorpresa, por tanto, puede representar para la parte reclamada lo que desde el inicio se le ha advertido e indicado. A lo largo de todo el proceso seguido en la AEPD -desde la entrada de la reclamación, pasando por el traslado, las actuaciones previas de investigación y el procedimiento sancionador- la parte reclamada ha ido solventado algunas cuestiones relacionadas con su incumplimiento a razón del traslado, requerimiento o práctica de prueba por parte de la AEPD, de forma reactiva y no proactiva, mas no todo y ni completamente, a la vista del texto de la resolución.

Segundo que, la resolución administrativa no sólo ha determinado de forma pormenorizada y con precisión los antecedentes y los hechos probados de los que se concluye cuáles son las infracciones imputadas a CaixaBank, sino que ha enervado la presunción de inocencia de la entidad, demostrando y motivando perfectamente cuáles son los incumplimientos que se han producido del RGPD por parte de la reclamada.

Frente a ello, la parte reclamada se limita a negar su incumplimiento, sin aportar elementos suficientes que demuestren que ha cumplido con el RGPD.

Una muestra indubitada de que no están aplicando correctamente, por ejemplo, la privacidad desde el diseño, se pone de manifiesto con las alegaciones ahora examinadas cuando reiteran que la ***(…)***.

Se realiza por la parte reclamada esta afirmación absoluta sin ninguna prueba que la sustente, ***(…)***, amén de lo que tal afirmación implica de desconocimiento de la normativa de protección de datos, que considera que los riesgos están en continua evolución, siendo necesario adoptar las medidas necesarias frente a dichos riesgos cambiantes.

Pero es que, además, no es cierto lo aseverado, puesto que la ***(…)***, sin que riesgo alguno fuera identificado o evaluado. Resultando asimismo que tal afirmación supone una contradicción evidente con sus propias actuaciones posteriores, en atención a los cambios efectuados en su procedimiento cuando la propia AEPD le advierte en el acuerdo de inicio de la ***(…)***. Si el riesgo para los derechos y las libertades de los interesados era cero tras la ***(…)***, tendrán que explicar el porqué de las modificaciones posteriores.

En tercer lugar, que en el texto de la resolución se establecen y prueban cuáles han sido los hechos constitutivos de infracción 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, pues estas medidas han de ser tendentes a solventar los incumplimientos detectados por la AEPD, cumpliendo con el RGPD.

Así, por ejemplo, y sin ningún ánimo de ser exhaustivo, de una simple lectura de la resolución administrativa se observa que, respecto de la concreta brecha de datos personales sufrida por la parte reclamante por falta de disponibilidad de sus datos personales y acreditada por la AEPD, la parte reclamada ha puesto finalmente a disposición del cliente los datos personales que le conciernen completos respecto de la operación efectuada el ***(…).***

Sin embargo, respecto de la implantación de las medidas técnicas y organizativas apropiadas de todo tipo derivadas de la aplicación de la privacidad desde el diseño, entre otras cuestiones, la determinación y establecimiento de las que dicen que tienen implementadas no se ha enfocado desde los riesgos en los derechos y libertades de los interesados (sino desde los riesgos en la organización), ni el sistema se encuentra gestionado de forma proactiva, de tal forma que no se ha cumplido con la privacidad

desde el diseño. No son, por tanto, las medidas que dice la parte reclamada que tiene implementadas estrictamente medidas de protección de datos, debiendo realizar la parte reclamada todas las actuaciones que sean precisas para aplicar correctamente la privacidad desde el diseño el marco de la gestión del cumplimiento normativo previsto por el RGPD conforme a su responsabilidad proactiva.

En resumen, todos y cada uno de los incumplimientos del RGPD de la parte reclamada se encuentran perfectamente explicitados en la propuesta de resolución y en la resolución y de ellos se infieren las medidas a adoptar en su caso.

Y todo ello 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 plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y el enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

En todo caso, la parte reclamada cuenta con un DPD que, en cumplimiento de las funciones atribuidas por el artículo 39 del RGPD, le debe informar y asesorar, así como supervisar el cumplimiento del RGPD, auxiliándole asimismo a implementar las medidas correctivas precisas.

Por lo tanto, no se considera que exista la indefensión alegada de contrario.

En realidad, esta Agencia no considera que nos encontremos ante un problema de indefensión, ante una cuestión de falta de motivación pormenorizada por parte de la AEPD de las infracciones cometidas y de las correlativas medidas correctivas impuestas, ni siquiera una dificultad de comprensión de la propuesta de resolución, sino que tal alegación de indefensión responde más bien a una simple estrategia de defensa de la parte reclamada: pretende justificar la indefensión en base a que ha cumplido con el RGPD y que, por tanto, ya no sabe qué más tiene que hacer.

Mas esto no es así tal y como se acredita y fundamenta a lo largo de esta resolución administrativa.

CaixaBank ha infringido el RGPD, no ha adoptado, a lo largo del procedimiento sancionador, todas las medidas necesarias para cumplir con la legalidad vigente y le corresponde a la Agencia conforme a los poderes que tiene conferidos imponer medidas correctivas para que los tratamientos del responsable del tratamiento se ajusten al RGPD y se protejan los derechos y libertades de todas las personas físicas cuyos datos personales son tratados, con la finalidad de evitar que se vuelvan a materializar los riesgos en el futuro.

Por tanto, partiendo de lo que acaba de exponerse y, en relación con la imposición de medidas a CaixaBank, cabe destacar que:

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 plenamente 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 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.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de 2.000.000,00 € (dos millones de euros).

SEGUNDO: IMPONER CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 25 del RGPD, tipificada en el Artículo 83.4 del RGPD, una multa de 1.500.000 € (un millón quinientos mil euros).

TERCERO: IMPONER CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una multa de 1.500.000 € (un millón quinientos mil euros).

CUARTO: ORDENAR a CAIXABANK, S.A., con NIF A08663619, que en virtud del artículo 58.2.d) del RGPD, en el plazo de nueve meses, notifique a la Agencia la adopción de las medidas a la vista del contenido del fundamento de derecho XIX.

QUINTO: NOTIFICAR la presente resolución a CAIXABANK, S.A..

SEXTO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad.
Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

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

De conformidad con lo establecido en el artículo 76.4 de la LOPDGDD y dado que el importe de la sanción impuesta es superior a un millón de euros, será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción.

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

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

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

938-250923

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