- **Expediente N.º: EXP202213126**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: A.A.A. (en adelante, la parte reclamante) con fecha 13 de octubre de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra CAIXABANK, S.A. con NIF A08663619 (en adelante, CAIXA). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 28 de marzo de 2022, la CAIXA, sin su consentimiento, facilitó a su exmarido "*la información fiscal del 2021 de todos mis productos de Caixabank, de los cuales soy titular*".

Manifiesta que tuvo conocimiento de lo ocurrido porque, con posterioridad, su exmarido le entregó dicha documentación a la hija de ambos.

A raíz de lo ocurrido, en fecha 19 de abril de 2022, presenta reclamación ante la CAIXA, recibiendo confirmación de la recepción en fecha 22 de abril de 2022.
En fecha 13 de mayo de 2022, recibe respuesta indicando que están realizando las investigaciones internas oportunas para esclarecer los hechos ocurridos y, en su caso, adoptar las medidas pertinentes y que recibirá la correspondiente contestación a su reclamación.
No obstante, y ante la falta de respuesta, en fecha 9 de junio de 2022, presenta reclamación ante el delegado de protección de datos de la CAIXA (mediante la cumplimentación del formulario habilitado al efecto en la web de dicha entidad) recibiendo respuesta, en fecha 10 de junio de 2022.
En dicha respuesta se le indica que la reclamación ha de ser realizada por la titular de los datos o por persona con poderes suficientes para ello (debiendo presentar su letrado poder notarial).
Manifiesta que, en fecha 11 de julio de 2022, se entrega en mano, en una oficina de la parte reclamada, copia de los poderes referidos a la atención del delegado de protección de datos.
Puesto que, no recibe ningún tipo de respuesta en relación con el resultado de las investigaciones sobre una posible vulneración del deber de confidencialidad, presenta reclamación ante esta Agencia.

Junto a la reclamación aporta:
- Copia del poder general para pleitos y especial para otras facultades, de fecha 8 de julio de 2022.
- Copia de la documentación relativa a la información fiscal controvertida.
- Copia de la respuesta de la parte reclamada, de fecha 13 de mayo de 2022, comunicando el inicio de las actuaciones de investigación interna pertinentes.

- Copia de la respuesta del delegado de protección de datos, de fecha 10 de junio de 2022.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la CAIXA, 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 13 de diciembre de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 16 de enero se recibe en esta Agencia escrito de respuesta indicando "… *Que, en relación con el mencionado escrito y, en lo relativo a la reclamación interpuesta por Dª* ***A.A.A.*** *(la "Reclamante"), en la que manifiesta que, en fecha 28 de marzo de 2022, la parte reclamada, sin su consentimiento, facilitó a su exmarido "la información fiscal del 2021 de todos mis productos de Caixabank, de los cuales soy titular", cúmplenos informarles de lo siguiente:*

*(i) Según consta en nuestros sistemas, la Reclamante y Sr. B.B.B. (exmarido) resultaban ser ambos titulares solidarios del depósito ***REFERENCIA.1, hasta el 25 de agosto de 2022, siendo el señor* ***B.B.B.*** *el que figuraba como interlocutor del producto.*

(ii) Se ha procedido a efectuar una investigación interna sobre lo manifestado por la Reclamante, y se ha determinado que el 8 de abril de 2022 acontecieron los siguientes hechos:

> ➢ *El Sr.* ***B.B.B.*** *acudió a la oficina para recabar la información fiscal correspondiente al año anterior (que CaixaBank pone a disposición de sus clientes mediante el "Comunicado Fiscal Único").*
> ➢ *Desde la oficina se accedió por el NIF del cliente a los comunicados del Sr.* ***B.B.B.****, y, concretamente, al Comunicado Fiscal Único de las posiciones del cliente en CaixaBank correspondiente al año 2021.*
> ➢ *Seguidamente, consultó los movimientos del depósito ***REFERENCIA.1, titularidad indistinta del Sr.* ***B.B.B.*** *y de la Reclamante, Sra.* ***A.A.A.****, accediendo a continuación al Comunicado Fiscal Único del año 2021 correspondiente a la Reclamante.*

Como es de ver, en el contexto de la gestión indistinta del producto compartido por el matrimonio formado por la Reclamante y el señor ***B.B.B.****, que actuaba como interlocutor ante la oficina (y que ahora, según manifiesta la Reclamante, resulta ser su excónyuge), la oficina accedió a toda la información fiscal de ambos titulares. incurriendo en un error humano e involuntario en la entrega del Certificado Fiscal Único al exmarido de la Reclamante…".*

TERCERO: Con fecha 13 de enero de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 21 de agosto 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 y Artículo 32 del RGPD, tipificadas en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD, respectivamente.

QUINTO: 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), la parte reclamada presentó escrito de alegaciones en el que solicita se acuerde el archivo de las actuaciones, al no constituir la conducta de CAIXABANK infracción ninguna del artículo 5.1 f) RGPD ni del artículo 32 RGPD.

SEXTO: Con fecha 20 de diciembre de 2023 se dictó propuesta de resolución proponiendo se sancione a CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD, con una multa de:

> - Por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) de dicha norma, multa administrativa de cuantía 50.000€ (CINCUENTA MIL EUROS)
> - Por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) de dicha norma, multa administrativa de cuantía 20.000€ (VEINTE MIL EUROS).

SÉPTIMO: Notificada la propuesta de resolución 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), la parte reclamada presentó escrito de alegaciones en el que, solicita se acuerde el archivo de actuaciones del presente procedimiento, al no constituir la conducta de CAIXABANK infracción ninguna del artículo 5.1.f RGPD ni del artículo 32 RGPD.

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

HECHOS PROBADOS

ÚNICO: Consta acreditado en el expediente que la CAIXA, sin el consentimiento de la parte reclamante, facilitó a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679

(Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II
Alegaciones al acuerdo de inicio

ALEGACIONES

PREVIA. – "UNA RECLAMACIÓN SOBRE UNA BRECHA DE SEGURIDAD NO IMPLICA LA IMPOSICIÓN DE UNA SANCIÓN DE FORMA DIRECTA"

Estimamos oportuno iniciar las presentes alegaciones con la citación literal del propio escrito del Acuerdo de inicio (Apartado II, Cuestiones Previas):

> En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse facilitado a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante.
>
> Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad 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.

Como la misma Agencia indica, si existe diligencia del responsable y las medidas de seguridad adecuadas y proporcionadas, un eventual y accidental suceso como el que nos ocupa no resulta susceptible de devengar sanción ninguna.

En contestación a dicha alegación, esta Agencia Española de Protección de datos debe resaltar que, tal y como se cita en el Acuerdo de inicio (Apartado II, Cuestiones Previas):

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."

Efectivamente, la recepción de una reclamación sobre una brecha de seguridad, entendida como una violación de seguridad de datos personales, no implica la imposición de una sanción; debe procederse al análisis de las circunstancias concurrentes a efectos de imposición de una sanción.

PRIMERA. – EL SUCESO ACONTECIDO NO CONSTITUYE UNA BRECHA DE SEGURIDAD COMUNICABLE

Nos encontramos ante una incidencia causada por una persona, empleada de una oficina de la Entidad, en relación a determinada información titularidad de la reclamante (el Certificado Fiscal correspondiente al año 2021, que recoge el resumen de los rendimientos del capital mobiliario), que fue puesta a disposición de su excónyuge, manifestando la reclamante no haber autorizado dicha puesta a disposición.

Esta es una incidencia aislada, con una persona concernida y con un único receptor identificado, afectando a un volumen muy exiguo de datos, que, en ningún caso, constituyen datos de carácter sensible.

Si bien la reclamante no nos ha trasladado los perjuicios de la actuación del personal de la oficina, resultarían estimables unas eventuales consecuencias con un nivel de severidad bajo.

De acuerdo con la anterior evaluación de los oportunos factores de riesgo, realizada de la mano de la "Guía para la notificación de brechas de datos personales" publicada por esta Agencia, únicamente cabe concluir que el suceso acontecido no constituye una brecha de seguridad comunicable, ni a la Autoridad de Control, ni al titular de los datos.

En contestación a dicha alegación, esta Agencia debe hacer referencia a lo preceptuado en el 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 el presente caso, consta que los datos personales de la parte reclamante, obrantes en la base de datos de CAIXA, fueron indebidamente difundidos a terceros, vulnerándose el principio de confidencialidad; al haberse facilitado a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante, teniendo conocimiento de lo ocurrido porque, con posterioridad, su exmarido le entregó dicha documentación a la hija de ambos.

El RGPD define, de un modo amplio, las “brechas de datos personales” 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”.

Es evidente que estamos ante una brecha de datos personales; puesto que, se ha producido un acceso no autorizado a la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante.

Resaltar que dicha definición se encuentra recogida en la “Guía para la notificación de brechas de datos personales” publicada por esta Agencia.

Aclarado el concepto de brecha de datos personales conviene subrayar que; en ningún momento, se ha imputado a la parte reclamada ni la vulneración del artículo 33 del RGPD ni la vulneración del artículo 34 del RGPD, que es donde se regula la comunicación de las brechas de seguridad a la autoridad de control y a los interesados respectivamente.

SEGUNDA. – SOBRE LAS MEDIDAS ADOPTADAS PARA EVITAR QUE SE PRODUZCAN SUCESOS SIMILARES y SOBRE LAS MEDIDAS ADOPTADAS PARA EVITAR QUE SE PRODUZCAN SUCESOS SIMILARES

2.1. MEDIDAS ADOPTADAS PARA EVITAR QUE SE PRODUZCAN SUCESOS SIMILARES

El suceso objeto de la presente reclamación se ha producido por la actuación contraria a las normas internas, por parte de un empleado de la Entidad en una actuación individual y aislada.

CaixaBank ha adoptado las oportunas medidas preventivas técnicas y organizativas con el objetivo de evitar incidencias como la acontecida, A este efecto, la Entidad tiene implementado un cuerpo normativo y un programa de formación y concienciación de sus empleados, que contempla, entre otras actuaciones y documentos, los siguientes:

• Un Código Ético (Código Ético y Principios de Actuación de CaixaBank), que resulta de aplicación a todos los empleados de la Entidad, que deben conocer y cumplir, en el que se contemplan específicamente las obligaciones de los empleados en relación con el acceso a los datos e información de los clientes de la Entidad que contempla, entre otras, las siguientes previsiones:

“1. El presente Código es de aplicación a CaixaBank y a todos los/las empleados/as, directivos/as y miembros de los Órganos de Gobierno de CaixaBank (en lo sucesivo, las “Personas Sujetas”). Todos ellos deberán conocer y cumplir el presente Código.”

“3.6 Confidencialidad Preservamos la confidencialidad de la información que nos confían nuestros accionistas y clientes.

1. La confidencialidad de la información relativa a nuestros clientes, empleados, miembros de los órganos de gobierno y dirección, proveedores y accionistas constituye el pilar fundamental sobre el que asienta la relación de confianza que constituye la esencia de nuestra actividad.
2. Deberá respetarse la normativa vigente y las normas internas sobre tratamiento y confidencialidad de los datos personales y sobre privacidad.
3. CaixaBank protege al máximo la información personal de sus clientes, accionistas, personas empleadas, miembros de sus Órganos de Gobierno o de cualquier persona física o jurídica con la que se relaciona. CaixaBank exige, asimismo, a terceras empresas proveedoras o con las que tenga relación, que preserven la confidencialidad de la información a la que puedan acceder con ocasión de la relación contractual que mantengan con CaixaBank.
4. Las personas sujetas sólo harán uso de la información recibida de los accionistas, clientes, proveedores, Órganos de Gobierno y personas empleadas para la finalidad para la que fue transmitida, todo ello de conformidad con la normativa vigente en esta materia. Nunca se accederá a información que no sea estrictamente exigida para el desempeño de nuestro trabajo. Antes de transmitir información a terceros, las personas sujetas deberán asegurarse de que están autorizados y que existe una una razón legítima para dicha transmisión. Incluso en el caso de estar autorizados, es preciso limitar a lo estrictamente necesario el volumen de información a revelar. En caso de cualquier duda, deberán consultar con el superior jerárquico o, atendiendo a la identidad de la misma, con el Departamento de Seguridad de la Información de CaixaBank.”

• Una Norma Interna sobre tratamiento y confidencialidad de los datos de los clientes (Norma 47: Confidencialidad y tratamiento de datos de carácter personal), que trata específicamente el aspecto del acceso a datos por parte de los empleados, que contempla, entre otras, las siguientes previsiones:

“ 2.9. Obligaciones generales de los empleados de CaixaBank Los empleados de CaixaBank están obligados a: • Custodiar y mantener el secreto profesional y la confidencialidad de los datos personales que tratan lo que implica: o NO revelar a terceros aquella información a la que tienen acceso en su condición de empleados y para el desempeño de las funciones que tiene atribuidas. o PROHIBICIÓN de cualquier consulta que no sea necesaria para el desempeño de las mencionadas funciones y esté justificada por la operativa que se está realizando. • Usar en su día a día únicamente las herramientas y aplicaciones corporativas que pone a su disposición la Entidad.”

• Un protocolo de formación continua y obligatoria en materia de privacidad y protección de datos para apoyar este cuerpo normativo. Se adjunta como Documento nº 1 el contenido de la formación realizada por el empleado.

• Una implementación de indicadores, por parte de Auditoria de la Red de Oficinas que, en base a indicadores de actividad ordinaria y de alertas de actividades no relacionadas a los roles de los empleados, tales como consultas a clientes no asignados a la cartera de la oficina o gestor, personas relevantes, horarios de consulta o similares, promueve investigaciones recurrentes sobre operativas sospechosas de no ser adecuadas al puesto de trabajo desempeñado. En el caso que nos ocupa en esta reclamación, el hecho de que la oficina y persona empleada involucrados en la incidencia fueran los habituales de la reclamante, impidió que el sistema de alertas de actividades anómalas detectara la incidencia antes de la reclamación de la clienta.

• Un programa continuo de concienciación mediante la publicación de notas y noticias en la intranet corporativa de la Entidad, para recordar a los empleados sus obligaciones en materia de confidencialidad. Se adjuntan un ejemplo de los contenidos periódicos que se publican.

2.2. MEDIDAS ADOPTADAS PARA EVITAR QUE SE PRODUZCAN SUCESOS SIMILARES

Por parte de esta Entidad, y a la vista de los hechos acontecidos, se procedió a adoptar dos tipos de medidas:

- se ha procedido a reiterar a los empleados de la oficina la relevancia de los contenidos indicados en el anterior apartado 2.1. en la interlocución con los clientes.
- respecto la persona empleada de la oficina involucrada en el suceso, se ha procedido a la incoación del correspondiente expediente por esta falta confidencialidad.

De acuerdo con lo anterior, resulta probado que CaixaBank aplica diligentemente medidas técnicas y organizativas apropiadas que garantizan la seguridad adecuada de los datos de sus clientes; si bien, obviamente, la adopción de dichas medidas no puede eliminar un suceso singular causado por un empleado de la entidad, por lo que no existe infracción ninguna del artículo 5.1.f RGPD.

En contestación a dicha alegación, debemos insistir en que, efectivamente, los hechos ocurridos constituyen una infracción del artículo 5.1.f 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 el presente caso, consta que los datos personales de la parte reclamante, obrantes en la base de datos de CAIXA, fueron indebidamente difundidos a terceros, vulnerándose el principio de confidencialidad; al haberse facilitado a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante, teniendo conocimiento de lo ocurrido porque, con posterioridad, su exmarido le entregó dicha documentación a la hija de ambos.

Cuestión distinta es que, la CAIXA, como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

Dichas medidas no solo son medidas de los sistemas informáticos sino también medidas de organizativas de factor humano.

La formación de los empleados que tienen acceso o disponibilidad a datos personales disponibles en sus bases de datos es un control esencial que toda organización diligente debe asegurar y acreditar.

Por otro lado, debe resaltarse que el reconocimiento por parte de CaixaBank de que ha adoptado las oportunas medidas preventivas técnicas y organizativas con el objetivo de evitar incidencias como la acontecida, denota que las medidas de seguridad implantadas eran insuficientes o no lo suficientemente robustas.

Por último, alegar que “El suceso objeto de la presente reclamación se ha producido por la actuación contraria a las normas internas, por parte de un empleado de la Entidad en una actuación individual y aislada” no exime de responsabilidad a la organización ni justifica el incumplimiento de la normativa vigente en materia de protección de datos como responsable del tratamiento de datos.

TERCERA. – SOBRE LA PRESUNTA INFRACCIÓN DEL ARTÍCULO 32 RGPD

Esta Entidad está en absoluto desacuerdo con esta imputación realizada por la Agencia en el Acuerdo de inicio.

En primer lugar, cúmplenos señalar que parecería que esta Agencia está imputando doblemente a CaixaBank por la misma presunta infracción: presunta falta de medidas de seguridad adecuadas o apropiadas, por lo que podía estar incurriendo en una vulneración de los principios del procedimiento sancionador (en concreto, el principio non bis in idem), y, por ende, vulnerando los derechos de mi representada.

En segundo lugar, traemos a colación todos los aspectos ya indicados en la anterior alegación SEGUNDA, para reiterar que CaixaBank aplica

medidas técnicas y organizativas apropiadas para garantizar la seguridad adecuados de los datos que trata.

A este efecto, debemos incidir en el hecho que los protocolos, procedimientos, sistemas y medidas establecidas por CaixaBank están encaminados a evitar que nadie acceda a información de la que no tiene derecho a conocer, evitando así quiebras de confidencialidad. Una única actuación singular ignorando dichos protocolos, procedimientos, sistemas y medidas, en el contexto del volumen de datos e información que diariamente es gestionado todos los empleados de CaixaBank, es la prueba que los protocolos, procedimientos, sistemas y medidas funcionan apropiadamente porque son conocidos y aplicados por los empleados de la Entidad.

Además, nos encontramos que esta Agencia realiza una extrapolación de una situación estrictamente singular para, sin realizar ninguna actividad probatoria al respecto, imputar a mi representada el incumplimiento de las obligaciones de responsabilidad proactiva a las que está sometida por la normativa de protección de datos.

Efectivamente, el Acuerdo de Inicio incurre en el maximalismo de entender que acontecido un suceso estrictamente singular, dicha circunstancia determina, a ojos de la Agencia, pero sin prueba que lo refute, que mi mandante no ha adoptado medidas de seguridad suficientes para preservar los derechos de los interesados y garantizar la confidencialidad e integridad de los datos.

De este modo, la Agencia en el Acuerdo de inicio, vincula el supuesto incumplimiento de lo dispuesto en el artículo 32 RGPD con la producción del resultado que aconteció como consecuencia de un mero y fortuito error humano.

Esta imputación ni se ajusta ni se corresponde a los hechos objetivos acontecidos, y resulta, aparte de desmesurada, totalmente contraria al ordenamiento jurídico, puesto que supone inseguridad jurídica y nula predictibilidad de las normas jurídicas de aplicación.

En este sentido, se considera necesario traer a colación una sentencia del Tribunal Supremo de 15 de febrero de 2022 (recurso de casación 7359/2020), donde el Alto Tribunal señala de forma clara que la obligación impuesta por el artículo 32 RGPD 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, como tradicionalmente venía considerando la Agencia y respaldando la doctrina de la Audiencia Nacional.

> “En las obligaciones de medios el compromiso que se adquiere es el de adoptar los medios técnicos y organizativos, así como desplegar una actividad diligente en su implantación y utilización que tienda a conseguir el resultado esperado con medios que

razonablemente puedan calificarse de idóneos y suficientes para su consecución, por ello se las denomina obligaciones "de diligencia " o "de comportamiento".
La diferencia radica en la responsabilidad en uno y otro caso, pues mientras que en la obligación de resultado se responde ante un resultado lesivo por el fallo del sistema de seguridad, cualquiera que sea su causa y la diligencia utilizada. En la obligación de medios basta con establecer medidas técnicamente adecuadas e implantarlas y utilizarlas con una diligencia razonable. En estas últimas, la suficiencia de las medidas de seguridad que el responsable ha de establecer ha de ponerse en relación con el estado de la tecnología en cada momento y el nivel de protección requerido en relación con los datos personales tratados, pero no se garantiza un resultado."

Consecuencia de todo lo anterior es que, en opinión de esta parte, las premisas que sientan el juicio de valoración de las circunstancias del caso y que conducen a la Agencia a la imposición de la infracción por la supuesta vulneración del artículo 32 RGPD, decaen ante la realidad del hecho singular acontecido y la jurisprudencia del Tribunal Supremo, circunstancias que necesariamente deberían conducir al archivo del presente expediente sancionador.

En contestación a esta alegación, es evidente que la CAIXA no disponía de medidas de seguridad razonables en función de los posibles riesgos estimados, vulnerándose lo previsto en el artículo 32 "Seguridad del tratamiento" del RGPD que establece:

"*1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento

para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

Insistimos en lo argumentado en la contestación a la anterior alegación, CaixaBank, como responsable del tratamiento de datos, está obligado a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de datos.

Dichas medidas no solo son medidas de los sistemas informáticos sino también medidas de organizativas de factor humano.

En relación al principio non bis in idem alegado, la Sentencia de la Audiencia Nacional de 23 de julio de 2021 (rec. 1/2017) dispone que,

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

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

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

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

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

En consecuencia, 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, mientras que la infracción del art. 32 del RGPD se reduce a la ausencia y 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 CAIXA se hubieran detectado por la AEPD sin que se hubiera producido la pérdida de confidencialidad y de disponibilidad, únicamente hubiera sido sancionada por el art. 32 del RGPD.

CAIXA considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada. No es cierto, puesto que el art. 5.1.f) del RGPD no se constriñe a la garantía de la seguridad adecuada al riesgo, sino a la garantía de la integridad y disponibilidad. Y no sólo mediante medidas de seguridad, sino mediante todo tipo de medidas técnicas u organizativas apropiadas.

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

En cuanto a la duda sobre si el art. 5.1.f) del RGPD impone al igual que el art. 32 del RGPD una obligación de medios, o si se trata de una obligación de resultado, mencionar que el art. 5.1.f) del RGPD recoge el principio de integridad y confidencialidad y determina que los datos personales serán 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. Establece una obligación de resultado.

Por otra parte, el art. 32 del RGPD reglamenta cómo ha de articularse la seguridad del tratamiento en relación con las medidas de seguridad concretas que hay que implementar, de tal forma que 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 incluya entre otras cuestiones, la capacidad de garantizar la confidencialidad de los datos.

Puede ocurrir que las medidas no sean adecuadas sin que por ello se haya producido una pérdida de integridad y/o confidencialidad. Se trata de una obligación de medios.

El artículo 32 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

A fin de mantener la seguridad de los tratamientos se exige al responsable evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. En dicha evaluación del riesgo deben tenerse en cuenta los riesgos que atenten contra los derechos y libertades de los interesados, especialmente sus derechos y libertades fundamentales.

CUARTA. - DE LA APLICACIÓN DE LAS AGRAVANTES

Los apartados PRIMERO, y CUARTO de la parte dispositiva del Acuerdo de Inicio del presente Procedimiento Sancionador señalan (transcribimos textualmente) que la Directora de la AEPD, acuerda lo siguiente:
"PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a CAIXABANK, S.A., con NIF A08663619, por las presuntas infracciones de los artículos 5.1.f) y 32 del RGPD, tipificadas, respectivamente, en los artículos 83.5.a) y 83.4.a) del RGPD. (…)

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) de dicha norma, multa administrativa de cuantía 50.000€ (CINCUENTA MIL EUROS).
- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) de dicha norma, multa administrativa de cuantía 20.000€ (VEINTE MIL EUROS)."

La AEPD refiere en su FUNDAMENTO DE HECHO V y VIII, determinadas circunstancias concurrentes en la actuación de Caixabank, determinando que deben ser consideradas como factores agravantes de su responsabilidad. Todo ello, unilateralmente y sin haber escuchado previamente la defensa de mi mandante sobre los hechos imputados.

En el presente Procedimiento Sancionador, esta Agencia considera que concurren las siguientes circunstancias agravantes:

Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, 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:
Como agravantes:
- b) la intencionalidad o negligencia en la infracción;

> Sanción por la infracción del artículo 32 del RGPD A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, 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: Como agravantes:
> - b) la intencionalidad o negligencia en la infracción; Mi mandante considera que en el presente caso no existe infracción ninguna del artículo 5.1.f RGPD ni del artículo 32 RGPD, por lo que menos resultarían aplicables las agravantes que, indebida e improcedentemente, considera concurrentes esta Agencia.

En contestación a dicha alegación y, en relación al agravante aplicado a las sanciones por las infracciones cometidas, esta Agencia Española de Protección de Datos reproduce el criterio adoptado por el Tribunal Supremo por falta de la diligencia exigible.

> **QUINTA. – CAMBIO DE CRITERIO EN EL EJERCICIO DE LA POTESTAD SANCIONADORA**
>
> Finalmente, esta Agencia en un expediente anterior (EXP 202300974) con idéntico objeto, resolvió el archivo de actuaciones, en fecha 9 de mayo del presente.
>
> Es decir, en un suceso similar al que nos ocupa, donde se constata un error humano e involuntario, esta Agencia procedió al archivo de actuaciones. señalando que Caixabank tiene implementadas aquellas medidas necesarias, proporcionadas y adecuadas, requeridas por la normativa de protección de datos.
>
> El hecho que el organismo administrativo cambie el criterio de su interpretación, sin actividad probatoria ninguna, y por lo mismo, adopte medidas opuestas a las que venía realizando con anterioridad, supone la vulneración de los principios del Derecho Administrativo sancionador, así como las garantías constitucionales de mi representada, circunstancia que implica la nulidad plena y radical del procedimiento administrativo que nos ocupa, en el supuesto que esta Agencia pretenda persistir en el mismo.

En contestación a dicha alegación, hay que subrayar que el citado expediente no tiene idéntico objeto; por tanto, no procede el archivo del expediente que nos ocupa.

En aquel momento ya manifestó CAIXABANK que tenía implementado un cuerpo normativo y un programa de formación y concienciación que contempla, entre otras actuaciones y documentos, los siguientes:

- Un Código Ético (Código Ético y Principios de Actuación), que resulta de aplicación a todos los empleados de la Entidad, que deben conocer y cumplir, en el que se contemplan específicamente las obligaciones de los empleados en relación con el acceso a los datos e información de los clientes, la confidencialidad de la información y no acceder nunca a información que no sea estrictamente exigida para el desempeño de nuestro trabajo.

- Una Norma Interna sobre tratamiento y confidencialidad de los datos de los clientes, que trata específicamente el aspecto del acceso a datos por parte de los empleados, que contempla, entre otras, obligaciones el custodiar y mantener el secreto profesional y la confidencialidad de los datos personales que tratan lo que implica, no revelar a terceros aquella información a la que tienen acceso en su condición de empleados y para el desempeño de las funciones que tiene atribuidas, prohibición de cualquier consulta que no sea necesaria para el desempeño de las mencionadas funciones y esté justificada por la operativa que se está realizando, y usar en su día a día únicamente las herramientas y aplicaciones corporativas que pone a su disposición la Entidad."

- Un protocolo de formación continua y obligatoria en materia de privacidad y protección de datos para apoyar este cuerpo normativo

- Una implementación de indicadores, por parte de Auditoria de la Red de Oficinas que, en base a indicadores de actividad ordinaria y de alertas de actividades no relacionadas a los roles de los empleados, tales como consultas a clientes no asignados a la cartera de la oficina o gestor, personas relevantes, horarios de consulta o similares, promueve investigaciones recurrentes sobre operativas sospechosas de no ser adecuadas al puesto de trabajo desempeñado.

Curiosamente, las mismas medidas alegadas en el presente expediente como medidas adoptadas para evitar que se produzcan sucesos similares.

En consecuencia, es evidente la insuficiencia y debilidad de las medidas de seguridad técnicas y organizativas de CAIXABANK apropiadas para garantizar el nivel de seguridad adecuado al riesgo en el tratamiento de los datos de carácter personal de sus clientes.

Por todo lo expuesto, SE DESESTIMARON las alegaciones presentadas.

III
Alegaciones a la propuesta de resolución

En respuesta a las alegaciones presentadas, según el orden expuesto por la entidad reclamada, se debe señalar lo siguiente:

ALEGACIONES

PRIMERA. - LA AEPD NO PUEDE DEDUCIR, POR EL ACONTECIMIENTO DE UN HECHO SINGULAR, QUE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS POR EL RESPONSABLE NO ERAN APROPIADAS

Indica la CAIXA lo siguiente:

En el anterior escrito de alegaciones, mi representada abrió el mismo con la siguiente citación literal de las palabras de la misma AEPD, recogidas en el Acuerdo de inicio (Apartado II, Cuestiones Previas):

> En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haberse facilitado a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante.
>
> Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad 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.

De acuerdo con tal premisa, en el escrito de alegaciones al Acuerdo de Inicio, remitido a la AEPD en fecha 11 de septiembre de 2023, CaixaBank procedió a describir todas las medidas, técnicas y organizativas, implementadas por CaixaBank que acreditan y prueban que se trata de medidas apropiadas para que no se produzca una comunicación no autorizada como la acontecida en el procedimiento que nos ocupa, y que enunciamos nuevamente, si bien ya ampliamente detalladas en nuestro anterior escrito, al que oportunamente nos remitimos:

(i) Medidas técnicas

- Acceso de las personas gestoras únicamente a los datos de los clientes de la cartera de clientes de su oficina.

- Implementación de indicadores y alertas por parte de Auditoría Interna destinados a detectar actividades de las personas gestoras no relacionadas con sus roles y/o con sus clientes gestionados.

(ii) Medidas organizativas

***-** Cuerpo normativo de obligado cumplimiento para todas las personas empleadas en Caixabank, integrado por (i) un Código Ético y Principios de Actuación de CaixaBank, y también (ii) la Norma 47 (Confidencialidad y Tratamiento de datos de carácter personal).*

- La eventual infracción de las disposiciones del cuerpo normativa anterior son objeto de incoación de expediente disciplinario, que puede conllevar la imposición de sanciones que van desde la suspensión de empleo y sueldo hasta el despido del empleado o empleada.

- Programa de formación en materia de protección de datos de carácter personal

con afectación a Bonus (es decir, que aquellos empleados o empleadas que no llevan a cabo o no superan el curso no cobran este concepto de retribución variable).

- Programa continuo de concienciación sobre el tratamiento de los datos de carácter personal de nuestros clientes.

Como es de ver, CaixaBank, en su condición de responsable diligente del tratamiento, ha demostrado que tiene implementadas múltiples y diversas medidas técnicas y organizativas apropiadas, destinadas a:
(i) prevenir y evitar que sus empleados y empleadas realicen operaciones de tratamiento que no resulten conformes con el RGPD, y
(ii) garantizar que el tratamiento de datos de sus clientes se realiza de conformidad con los principios del artículo 5 del RGPD,

En cambio, esta Agencia, en su propuesta de resolución, no realiza examen ni valoración ninguna en cuanto al fondo de las medidas (ni en relación con la naturaleza de las mismas, ni en lo que concierne a su contenido, ni tampoco a su forma de aplicación), limitándose a "insistir en los hechos recurridos" (página 11/23) o la simple manifestación "es evidente que la CAIXA no disponía de medidas de seguridad razonables" (página 12/23).

Esta necesidad de examen o valoración objetiva no es un requerimiento de mi representada, sino que se encuentra expresamente exigido por la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea, que en su Sentencia en el Asunto C-340/21 (Natsionalna agentsia za prihodite, dictada en fecha 14 de diciembre de 2023). Esta Sentencia resulta totalmente extrapolable al procedimiento que nos ocupa, y en ella, el Tribunal Europeo señale expresamente lo siguiente:

> ***"****45 Por consiguiente, para controlar el carácter apropiado de las medidas técnicas y organizativas adaptadas con arreglo al artículo 32 del RGPD, un órgano jurisdiccional nacional no debe limitarse a comprobar de qué manera el responsable del tratamiento ha procurado cumplir con las obligaciones que le incumben en virtud de dicho artículo, sino que debe llevar a cabo un examen en cuanto al fondo de estas medidas, a la luz de todos los criterios a que hace referencia el mencionado artículo, así como de las circunstancias propias del caso y de los elementos de prueba de que dispone el órgano jurisdiccional.*
>
> *46 Un examen de este tipo requiere que se proceda a un análisis concreto tanto de la naturaleza como del contenido de las medidas que han sido adoptadas por el responsable del tratamiento, de la forma en la que se han aplicado dichas medidas y de sus efectos prácticos en el nivel de seguridad que este estaba obligado a garantizar, habida cuenta de los riesgos inherentes a ese tratamiento."*

Es decir, que la Agencia no puede limitarse a manifestar, sin más (página 8/23 del escrito de Propuesta de Resolución), que "debemos insistir en que efectivamente los hechos ocurridos constituyen una infracción del artículo 5.1.f RGPD", o que "la CAIXA no disponía de medidas de seguridad razonables" (página 11/23), sin realizar ninguna valoración ni argumentación objetiva de las múltiples y diversas medidas implementadas por mi representada.

Este hecho constituye una vulneración flagrante del derecho fundamental a la tutela judicial efectiva, y, en consecuencia, vicia al presente procedimiento administrativo de nulidad absoluta.

Por todo lo anterior, mi representada únicamente puede concluir en el mismo sentido de la Sentencia del TJUE anteriormente citada:

1. Que no se ha producido infracción ninguna del artículo 5.1.f, RGPD porque el RGPD no exige infalibilidad, sino la adopción de medidas apropiadas para garantizar la protección adecuada de los datos personales tratados por el responsable. La previsión de adopción de medidas regulada por el RGPD carecería de todo sentido si la exigencia al responsable por parte del RGPD consistiera, simple y llanamente, en impedir toda infracción:

> *"50 En particular, el responsable del tratamiento debe, de conformidad con los principios de integridad y de confidencialidad de los datos personales establecidos en el artículo 5, apartado 1, letra f, de dicho Reglamento, garantizar que estos datos son 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 y debe ser capaz de demostrar la conformidad con los referidos principios"*

2. Que la AEPD no puede pretender que las medidas técnicas y organizativas implementadas por el responsable no son apropiadas porque se ha producido el hecho denunciado, sin valoración probatoria ninguna de las citadas medidas:

"39 (…) los artículos 24 y 32 del RGPD deben interpretarse en el sentido de que una comunicación de autorizada de datos personales o un acceso no autorizado a tales datos por parte de "terceros" a los efectos del artículo 4, punto 10, del mencionado Reglamento, no bastan por sí solos, para considerar que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento no eran "apropiadas" con arreglo a los citados artículos 24 y 32".

En contestación a dicha alegación, esta Agencia debe recordar que las medidas técnicas y organizativas hay que adoptarlas, implantarlas por el responsable del tratamiento y seguirlas por el personal que presta servicios en la organización.

En el presente caso, no sólo consta que las medidas técnicas y organizativas impuestas por el responsable del tratamiento se pudieron quebrantar por un empleado de la organización que actuó negligentemente, sino que también se ha puesto de manifiesto una falta de medidas apropiadas, pues las medidas que se adopten deben ser eficaces para garantizar el cumplimiento del RGPD, lo que habrá de valorarse caso por caso.

Se han de adoptar las medidas apropiadas teniendo en cuenta los riesgos para los derechos y libertades de los interesados lo que incluirá la aprobación de protocolos, políticas y la toma de decisiones, pero también será necesaria la adopción de medidas técnicas que mitiguen el riesgo.

Tal y como razona el TJUE en la sentencia que se cita: "*27. Todo el Reglamento se basa en la prevención del riesgo y la responsabilidad proactiva del responsable del tratamiento y, por tanto, en un enfoque teleológico que persigue el mejor resultado posible en términos de eficacia, es decir, muy lejos de la lógica formalista vinculada a la mera obligación de cumplir procedimientos específicos que eximan de responsabilidad. (11)*"

En este sentido el Considerando 74 del RGPD declara que "*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas*"

Y añade el Considerando 76 que "*La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto*".

En el caso que nos ocupa, CaixaBank es responsable del tratamiento de los datos financieros de la reclamante y le incumbe adoptar las medidas apropiadas para garantizar su confidencialidad, teniendo en cuenta para ello el mayor riesgo que supone para la confidencialidad la titularidad solidaria de los productos financieros. Sin embargo, no consta en el procedimiento que CaixaBank identificara este riesgo y adoptara medidas específicas para su mitigación, tanto técnicas como organizativas. CaixaBank se centra en atribuir los hechos a un error humano del empleado, pero el resultado, la materialización del riesgo, era fácilmente previsible, y CaixaBank no ha puesto de manifiesto la existencia de ninguna medida técnica u organizativa, alerta o control, que tuviera como finalidad evitar que en supuestos de titularidad solidaria los empleados accedieran y facilitaran los datos específicos de unos cotitulares a otros cotitulares que carecían de representación. La garantía de la confidencialidad exige la aplicación de aquellos recursos, procedimientos y controles que pudieran ser necesarios, lo que no consta que en este caso se haya realizado.

CaixaBank ha de asegurarse de que las medidas que adopta sean eficaces y una medida básica es la de garantizar que la información financiera de un determinado cliente sólo pueda facilitarse a un tercero si el cliente ha dado su consentimiento y éste se encuentra actualizado y referido a la concreta operación de tratamiento que se pretende realizar.

Es más, CaixaBank debe responder por las actuaciones realizadas por su cuenta, la actuación del empleado no exime de responsabilidad a la empresa. La responsabilidad de la empresa en el ámbito sancionador por la actuación de un empleado que suponga el incumplimiento de la normativa de protección de datos ha sido confirmada por la Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de diciembre de 2023, dictada en el asunto C-807/21 (Deutsche Wohnen), que indica

"*24 En efecto, según el mencionado órgano jurisdiccional, esta jurisprudencia, al igual que la mayoría de la doctrina nacional, concede especial importancia al concepto de «empresa», en el sentido de los artículos 101 TFUE y 102 TFUE, y, por tanto, a la idea de que la responsabilidad se imputa a la entidad económica en la que se ha adoptado el comportamiento indeseable, por ejemplo, un comportamiento contrario a la competencia. A su entender, conforme a esta concepción «funcional», todos los actos de todos los empleados autorizados a actuar en nombre de una empresa son imputables a la empresa, también en el marco de un procedimiento administrativo.*

(…)

44 Por lo que respecta a las personas jurídicas, esto implica, por una parte, como ha señalado, en esencia, el Abogado General en los puntos 57 a 59 de sus conclusiones, que estas son responsables no solo de las infracciones cometidas por sus representantes, directores o gestores, sino también por cualquier otra persona que actúe en el ámbito de la actividad empresarial de esas personas jurídicas y en su nombre. Por otra parte, las multas administrativas previstas en el artículo 83 del RGPD en caso de que se produzcan tales infracciones deben poder imponerse directamente a personas jurídicas cuando estas puedan ser calificadas de responsables del tratamiento en cuestión."

También por la jurisprudencia del Tribunal Supremo. A este respecto, cabe indicar que la Sentencia del Tribunal Supremo núm. 188/2022 (Sala de lo Contencioso, Sección 3ª), de 15 de febrero de 2022 (rec. 7359/2020), mencionada por BBVA en su escrito de alegaciones al acuerdo de inicio; señala en su Fundamento de Derecho Cuarto: *"El hecho de que fuese la actuación negligente de una empleada no le exime de su responsabilidad en cuanto encargado de la correcta utilización de las medidas de seguridad que deberían haber garantizado la adecuada utilización del sistema de registro de datos diseñado. Como ya sostuvimos en la STS nº 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros*."

Continúa la sentencia argumentando acerca de la de la responsabilidad de las personas jurídicas: *"…Sencillamente sucede que, estando admitida en nuestro Derecho Administrativo la responsabilidad directa de las personas jurídicas, a las que se reconoce, por tanto, capacidad infractora, el elemento subjetivo de la infracción se plasma en estos casos de manera distinta a como sucede respecto de las personas físicas, de manera que, como señala la doctrina constitucional que antes hemos reseñado -SsTC STC 246/1991, de19 de diciembre (F.J. 2) y 129/2003, de 30 de junio (F.J. 8)- la reprochabilidad directa deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma."*.

Dicho lo anterior, de lo expuesto por la CAIXA se deduce claramente que es necesario no sólo contar con un cuerpo normativo y un programa de formación y concienciación de sus empleados, tal y como declara la parte reclamada, sino también reiterar que resultan necesarias otras medidas que coadyuven a reducir los riesgos específicos que se derivan de las características concretas del tratamiento. Además, es necesario adaptar en el tiempo la aplicación y vigencia de ese cuerpo normativo e implantar una formación continua en materia de protección de datos, que asegure la concienciación de los empleados en la confidencialidad de la información personal y financiera de sus clientes.

Por todo ello y dado lo ocurrido, resulta fácil valorar que las medidas técnicas y organizativas adoptadas no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo que presenta el tratamiento de datos, es más, debemos insistir en el hecho de que si se han adoptado las oportunas medidas preventivas técnicas y organizativas con el objetivo de evitar incidencias como la acontecida, es porque las medidas de seguridad implantadas eran insuficientes o no lo suficientemente robustas.

Por último y en referencia a lo expuesto, es necesario hacer constar la sentencia de la AN de 9 de febrero de 2023 (rec. 770/2022) que dice:

"(…) Las medidas de seguridad implementadas con posterioridad, no afectan a la comisión de la infracción (…)".

SEGUNDA. - APLICACIÓN DEL PRINCIPIO "NO BIS IN IDEM": LA AGENCIA ESTÁ SANCIONANDO DOS VECES EL MISMO HECHO PUNIBLE.

Señala la entidad lo siguiente:

Nos remitimos a la Propuesta de Resolución de esta Agencia, en la que indica lo siguiente:

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

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

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

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

En consecuencia, 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 seguridad, la infracción del art. 5.1.f) del RGPD se concreta en una clara pérdida de confidencialidad y disponibilidad, mientras que la infracción del art. 32 del RGPD se reduce a la ausencia y 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 CAIXA se hubieran detectado por la AEPD sin que se hubiera producido la pérdida de confidencialidad y de disponibilidad, únicamente hubiera sido sancionada por el art. 32 del RGPD.

Como se puede observar, la AEPD manifiesta que, "entendido grosso modo", no existe vulneración del principio NON BIS IN IDEM, evitando mencionar e incidir en lo que resulta evidente: que la supuesta falta de medidas técnicas y organizativas destinadas a garantizar la seguridad de los datos para evitar que se produzca un hecho como el acontecido es la conducta objeto de doble sanción, sin que podamos entender las divagaciones al respecto de la Agencia, puesto que, tal como indica la Sentencia del Alto Tribunal que ella misma trae a colación, resulta obvio que concurre la triple identidad entre los términos comparados:

(i) El responsable del tratamiento de los datos es Caixabank en ambas presuntas
infracciones
(ii) La conducta es la misma: supuesta falta de medidas técnicas u organizativas,
presuntamente no apropiadas para evitar situaciones como la acontecida
(iii) La misma conducta es objecto de una doble sanción punitiva por parte de esta Agencia

Por lo que es de ver, de un sencillo análisis y no de un entendimiento "grosso modo", resulta que sí concurre la identidad de términos que conducen a la flagrante vulneración del principio NON BIS IN IDEM, en la presente actividad sancionadora administrativa.

Y de nuevo el Tribunal Europeo, en la reciente Sentencia ya citada, respalda la argumentación de esta parte, puesto que ciñe el principio de responsabilidad del responsable del tratamiento al carácter apropiado de las medidas técnicas u organizativas adoptadas por él, destinadas a garantizar que los datos se tratan con la seguridad adecuada, y por lo tanto, que el tratamiento se realiza de conformidad con el RGPD:

“49 A este respecto, procede recordar, en primer lugar, que el artículo 5, apartado 2, del RGPD establece un principio de responsabilidad en virtud del cual el responsable del tratamiento es responsable del respeto de los principios relativos al tratamiento de datos personales enunciados en apartado 1 de este artículo y estipula que este responsable debe ser capaz de demostrar la conformidad del tratamiento con dichos principios.

50 En particular, el responsable del tratamiento debe, de conformidad con los principios de integridad y de confidencialidad de los datos personales establecidos en el artículo 5, apartado 1, letra f), de dicho Reglamento, garantizar que estos datos son 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 y debe ser capaz de demostrar la conformidad con los referidos principios.

51 Asimismo, procede señalar que tanto el artículo 24, apartado 1, del RGPD, en relación con el considerando 74 de este, como el artículo 32, apartado 1, del mismo Reglamento obligan al responsable del tratamiento, para todo tratamiento de datos personales realizado por él mismo o por su cuenta, a aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.”

En contestación a dicha alegación y sin ánimo de reiterar lo ya ha contestado a lo alegado al acuerdo de inicio, esta Agencia debe insistir en que no existe vulneración del principio non bis in idem.

El hecho de haber facilitado al exmarido de la parte reclamante información fiscal del año 2021 de todos los productos de Caixabank, de los cuales era titular ésta, sin su previo consentimiento evidencia una infracción del artículo 5.1.f) del RGPD. Al no haberse acreditado que adoptara medidas técnicas y organizativas, de todo tipo, adecuadas para garantizar la confidencialidad en productos de titularidad solidaria.

Pero, además es evidente que las medidas de seguridad, sólo de seguridad, implantadas por la CAIXA no resultaron ser efectivas al no impedir o reducir la probabilidad de que se materializara el riesgo ante una actuación negligente de un empleado y por ello ha de concluirse que no disponía de medidas de seguridad apropiadas en función de los posibles riesgos estimados, vulnerándose lo previsto en el artículo 32 “Seguridad del tratamiento” del RGPD.

Pues bien, hemos de traer a colación lo explicitado en el apartado anterior sobre la diferencia entre la vulneración del art. 5.1.f) y el 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.

Asimismo, tal y como indicábamos, el art. 5.1.f) del RGPD se vulnera cuando se produce una pérdida de confidencialidad, de integridad o de disponibilidad 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, integridad o disponibilidad cuando explicita "mediante la aplicación de medidas técnicas y organizativas apropiadas", que no son estrictamente de seguridad.

La CAIXA expone que las medidas técnicas y organizativas apropiadas a las que hace mención este precepto son las medidas de seguridad del art. 32 del RGPD. Esto sería simplificar la esencia del RGPD cuyo cumplimiento no se limita a la implantación de medidas técnicas y organizativas de seguridad; significaría, en nuestro caso, reducir la garantía exigida mediante el principio de integridad y confidencialidad a su logro únicamente con medidas de seguridad.

Como hemos señalado anteriormente, cuando el art. 5.1.f) del RGPD se refiere a medidas técnicas u organizativas apropiadas para garantizar los derechos y libertades de los interesados en el marco de la gestión del cumplimiento normativo del RGPD, lo hace en el sentido previsto en el art. 25 del RGPD relativo a la privacidad desde el diseño.

Este precepto determina que,

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

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

Sin embargo, el art. 32 del RGPD comprende la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo. 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 se puede observar los dos artículos persiguen fines distintos, aunque puedan estar relacionados.

Es evidente que, si las medidas de seguridad implantadas por la CAIXA no fueran razonables en función de los posibles riesgos estimados y se hubiera detectado por la

AEPD, sin que se hubiera producido la pérdida de confidencialidad y de disponibilidad, únicamente hubiera sido sancionada por el art. 32 del RGPD.

CAIXA considera que en ambos preceptos se exige una única conducta que es implantar la seguridad adecuada; si bien, es evidente que, son conductas distintas y con distinto fundamento.

TERCERA. - INTERPRETACIÓN PROPIA DE LA AGENCIA SOBRE LAS OBLIGACIONES DE MEDIOS Y LAS OBLIGACIONES DE RESULTADO

Continúa diciendo la CAIXA:

En su escrito de alegaciones, la Agencia conviene parcialmente con mi representada que las obligaciones en relación a las medidas técnicas y organizativas adoptadas constituyen una obligación de medios y no de resultado, que el responsable del tratamiento debe procurar mediante el desarrollo de una conducta diligente, consistente en el despliegue e implementación de las medidas adecuadas. Tal como declara el Tribunal de Justicia Europeo en su ya reiterada Sentencia (en el apartado declarativo final):

"una comunicación no autorizada de datos personales o un acceso no autorizado a tales datos por parte de terceros (…) no bastan, por sí solos, para considerar que las medidas técnicas y organizativas adoptadas por el responsable del tratamiento de que se trate no eran "apropiadas" con arreglo a los citados artículos 24 y 32"

El hecho sorprendente es que la obligación de medios se desprende, según esta Agencia, del artículo 32 RGPD pero no del artículo 5.1.f) RGPD. Muy sorprendentemente, teniendo en cuenta que el principio invocado y presuntamente infringido se vincula a la "aplicación de medidas técnicas u organizativas adecuadas".

Es por ello que, no podemos entender como esta particular (y peculiar) interpretación de esta Agencia casa con la interpretación del TJUE, en la Sentencia que reiteradamente hemos mencionado y transcrito, ni con el propio RGPD: el responsable del tratamiento está sujeto a una obligación de protección de datos, y el cumplimiento de esa obligación pasa por la adopción de medidas técnicas u organizativas apropiadas, destinadas a garantizar dicho cumplimiento. Y esta adopción de medidas idóneas en relación con los eventuales riesgos del tratamiento es, en todos los supuestos, una obligación de medios, nunca de resultado, ya que una comunicación no autorizada en ningún caso constituye infracción por si misma, sino que la posible infracción dimana de la valoración de la idoneidad de las medidas adoptadas por el responsable, una vez evaluados los riesgos de acuerdo con la naturaleza, el alcance, el contexto y los fines del tratamiento. Insistimos que, claramente, se trata jurídicamente de una obligación de medios y no de resultado:
"38 (…) el considerando 83 del RGPD, que establece, en su primera frase, que "a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos". De este

modo, el legislador de la Unión manifestó su intención de "mitigar" los riesgos de violación de la seguridad de los datos personales, sin pretender llegar a eliminarlos".

En contestación a lo alegado, esta Agencia se remite a lo ya argumentado en relación con la diferencia de obligación de medios y de resultado.

Caixabank en su argumentación parece buscar la confusión entre lo que es la imputación del artículo 5.1.f) y la imputación del 32 del RGPD; no obstante, como ya se ha dejado claro con anterioridad, son infracciones distintas, preceptos distintos con distinta tipificación en el RGPD y distinta calificación a efectos de prescripción en la LOPDGDD.

CUARTA. - DE LA APLICACIÓN DE LAS AGRAVANTES

La CAIXA indica:

En el presente Procedimiento Sancionador, esta Agencia considera que concurren las siguientes circunstancias agravantes:
"Sanción por la infracción del artículo 5.1.f) del RGPD
A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, 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:
Como agravantes:
- b) la intencionalidad o negligencia en la infracción;"
"Sanción por la infracción del artículo 32 del RGPD
A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, 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:
Como agravantes:
- b) la intencionalidad o negligencia en la infracción;"

Cúmplenos reiterar que mi mandante considera que en el presente caso no existe infracción ninguna del artículo 5.1.f) RGPD ni del artículo 32 RGPD, y, a la luz de las medidas técnicas y organizativas que CaixaBank tiene implementadas (detalladas en nuestro anterior escrito de alegaciones y enunciadas de nuevo en el presente), para que no se lleven a cabo operaciones de tratamiento de datos contrarias al RGPD, tachar el hecho acontecido de "infracción intencionada o negligente" por parte de la Agencia, resulta, de manera evidente, subjetivamente desproporcionado y en ningún caso ajustado a derecho.

En contestación a lo alegado y puesto que, esta Agencia considera que sí existe una infracción del artículo 5.1.f) RGPD y una infracción del artículo 32 RGPD, a tal efecto,

se hace necesario referirnos a lo invocado por la Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de diciembre de 2023, recaída en el asunto C-807/21 (Deutsche Wohnen), que indica:

"76 A este respecto, debe precisarse además, por lo que atañe a la cuestión de si una infracción se ha cometido de forma intencionada o negligente y, por ello, puede sancionarse con una multa administrativa con arreglo al artículo 83 del RGPD, que un responsable del tratamiento puede ser sancionado por un comportamiento comprendido en el ámbito de aplicación del RGPD cuando no podía ignorar el carácter infractor de su conducta, tuviera o no conciencia de infringir las disposiciones del RGPD (véanse, por analogía, las sentencias de 18 de junio de 2013, Schenker & Co. y otros, C-681/11, EU:C:2013:404, apartado 37 y jurisprudencia citada; de 25 de marzo de 2021, Lundbeck/Comisión, C-591/16 P, EU:C:2021:243, apartado 156, y de 25 de marzo de 2021, Arrow Group y Arrow Generics/Comisión, C-601/16 P, EU:C:2021:244, apartado 97)." (el subrayado es nuestro).

En la misma línea se expresan los órganos jurisdiccionales de nuestro país. Así, la Sentencia de la Audiencia Nacional, de 21 de enero de 2010, expone:

"La recurrente también mantiene que no concurre culpabilidad alguna en su actuación. Es cierto que el principio de culpabilidad impide la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, también es cierto, que la ausencia de intencionalidad resulta secundaria ya que este tipo de infracciones normalmente se cometen por una actuación culposa o negligente, lo que es suficiente para integrar el elemento subjetivo de la culpa. La actuación de XXX es claramente negligente pues… debe conocer… las obligaciones que impone la LOPD a todos aquellos que manejan datos personales de terceros. XXX viene obligada a garantizar el derecho fundamental a la protección de datos personales de sus clientes e hipotéticos clientes con la intensidad que requiere el contenido del propio derecho".

El Tribunal Supremo (Sentencias de 16 y 22 de abril de 1991) considera que del elemento culpabilista se desprende *"...que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable"*. El mismo Tribunal razona que *"no basta... para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia"* (STS 23 de enero de 1998).

Conectada también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (Rec. 63/2006), que precisó: *"(...) 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".*

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del*

tratamiento de datos de extremar la diligencia..." (Sentencia de la Audiencia Nacional de 29 de junio de 2001).

Por todo lo expuesto, SE DESESTIMAN las alegaciones presentadas.

III
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 el presente caso, consta que los datos personales de la parte reclamante, obrantes en la base de datos de CAIXA, fueron indebidamente difundidos a terceros, vulnerándose el principio de confidencialidad; al haberse facilitado a su exmarido la información fiscal del 2021 de todos los productos de Caixabank, de los cuales era titular la parte reclamante, teniendo conocimiento de lo ocurrido porque, con posterioridad, su exmarido le entregó dicha documentación a la hija de ambos.

La CAIXA admite que los hechos acontecidos, la entrega del Certificado Fiscal Único al exmarido de la parte reclamante, fueron consecuencia de un error humano e involuntario del personal que presta servicios en la oficina.

Se considera que los hechos conocidos son constitutivos de una infracción, imputable al CAIXA, por vulneración del artículo 5.1.f) del RGPD.

IV
Tipificación de la infracción del artículo 5.1.f) del RGPD

La citada infracción del artículo 5.1.f) del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.5 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 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. (…)"*

V

Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, 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:

Como agravantes:

- *b) la intencionalidad o negligencia en la infracción;*

La CAIXA informa a esta Agencia respecto a los hechos relatados que se ha incurrido "*… en un error humano e involuntario en la entrega del Certificado Fiscal Único al exmarido de la Reclamante…"*

Sin embargo, los hechos puestos de manifiesto en este caso evidencian una clara falta de diligencia en la actuación de su empleado.

En este mismo sentido, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la 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 17/10/2007 (rec. 63/2006)]**

Como agravantes:
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

La CAIXA, en ejercicio de su actividad financiera, debe facilitar, personalmente o por medio de representación acreditada, a todos sus clientes la información fiscal que requieran en el ejercicio de sus obligaciones tributarias.

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.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar una sanción de 50.000 € (CINCUENTA MIL EUROS).

VI

Artículo 32 del RGPD

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

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, en el momento de producirse la brecha de datos personales, no consta que la CAIXA dispusiese de medidas de seguridad razonables en función de los posibles riesgos estimados.

La CAIXA manifiesta que *"…en el contexto de la gestión indistinta del producto compartido por el matrimonio formado por la Reclamante y el señor* ***B.B.B.****, que actuaba como interlocutor ante la oficina (y que ahora, según manifiesta la Reclamante, resulta ser su excónyuge), la oficina accedió a toda la información fiscal de ambos titulares. incurriendo en un error humano e involuntario en la entrega del Certificado Fiscal Único al exmarido de la Reclamante…".*

Sin embargo, el incidente pone de manifiesto una falta clara de diligencia del empleado y la ausencia de medidas adecuadas para evitar actuaciones de los empleados de esta naturaleza.

Por lo demás, la existencia de titularidad solidaria en productos financieros de la CAIXA comporta un cierto riesgo de que errores como este puedan producirse.

La entrega de la documentación personal correspondiente a la información fiscal de los productos de Caixabank a persona distinta de su titular, sin la autorización y el consentimiento de éste, evidencia una deficiencia en la implantación de medidas adecuadas al riesgo o un quebrantamiento de las existentes.

Se considera que los hechos conocidos son constitutivos de una infracción, imputable a la CAIXA, por vulneración del artículo 32 del RGPD.

VII
Tipificación de la infracción del artículo 32 del RGPD

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

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

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

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

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

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

(…)

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

VIII
Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, 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:

Como agravantes:

- *b) la intencionalidad o negligencia en la infracción;*

La CAIXA informa a esta Agencia respecto a los hechos relatados que se ha incurrido "… *en un error humano e involuntario en la entrega del Certificado Fiscal Único al exmarido de la Reclamante…"*

En este mismo sentido, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la 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 17/10/2007 (rec. 63/2006)]**

Como agravantes:
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

La CAIXA, en ejercicio de su actividad financiera, debe facilitar a todos sus clientes la información fiscal que requieran en el ejercicio de sus obligaciones tributarias.

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.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y el artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar una sanción de 20.000 € (VEINTE MIL EUROS).

IV
Adopción de medidas

En el texto de la resolución se establecen cuáles han sido las infracciones cometidas y los hechos que han dado lugar a la vulneración de 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.

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

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a CAIXABANK, S.A., con NIF A08663619, por una infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificadas en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD, respectivamente, con una multa de:

- Por la infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) de dicha norma, multa administrativa de cuantía 50.000€ (CINCUENTA MIL EUROS)
- Por la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4.a) de dicha norma, multa administrativa de cuantía 20.000€ (VEINTE MIL EUROS).

SEGUNDO: NOTIFICAR la presente resolución a CAIXABANK, S.A.

TERCERO: 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 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.

938-16012024

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