- **Expediente N.º: EXP202306253**

Actuaciones Investigación AI/00085/2023.

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas de 27/02/23, 28/02/23 y 01/03/23 se notifica ante la División de Innovación Tecnológica de esta Agencia Española de Protección de Datos por parte del BANCO DE ESPAÑA, con NIF Q2802472G (en adelante, BDE), IBERCAJA BANCO, S.A, con NIF A99319030 (en adelante, IBERCAJA), y UBS EUROPE SE, SUCURSAL EN ESPAÑA**,** con NIF W2760881I (en adelante, UBS EUROPE), la posible concurrencia de una brecha de datos personales acontecida el 21/02/2023.

Resumidamente, de las referidas notificaciones se desprende el siguiente contenido:

- Se pone en conocimiento de esta Agencia que el informe preceptivo que debe emitir el BDE el día 21 del mes siguiente con los datos referentes a riesgos de crédito que mantienen con sus clientes las entidades financieras declarantes, ha sido inexacto debido a que la información que debían facilitar dos de las entidades obligadas, no fue remitida en el plazo establecido al efecto.

- En particular, los desajustes comunicados tienen relación con los datos de riesgos de clientes correspondientes (…) de dos de las entidades financieras, IBERCAJA y UBS EUROPE. Estos informes incompletos contenían datos de un máximo de (…) afectados que fueron remitidos a (…) entidades financieras ((…) informes automáticos remitidos a las entidades declarantes y (…) informes ad hoc remitidos a las entidades solicitantes) y, a los (…) afectados que solicitaron acceder a sus informes de riesgo crediticio entre los días 21 y 24 de febrero de 2023.

SEGUNDO: Teniendo en cuenta la sensibilidad de la información, de acuerdo con lo señalado y de conformidad con el artículo 67.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), con fecha de 17/03/2023 se acuerda por la directora de la Agencia Española de Protección de Datos abrir una investigación de oficio y se insta a la Subdirección General de Inspección de Datos a que inicie actuaciones previas de investigación tendentes a verificar lo sucedido y evaluar las implicaciones en materia de protección de datos personales de esta conducta, y, en su caso, la adecuada observancia de la normativa.

TERCERO: Como consecuencia de dicho acuerdo, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, tramitadas con el número

AI/00085/2023, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD.

En el marco de esta investigación se realizaron una serie de requerimientos a las principales entidades afectadas recibiéndose respuesta puntual y exhaustiva a las cuestiones planteadas a todas ella.

En virtud del análisis de la información recopilada en el marco de la investigación, se puede concluir lo siguiente:

1. Sobre las circunstancias y origen del incidente:

La remisión del informe de riesgos de crédito a las entidades declarantes a las que se refiere el artículo 60 de la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, fue realizada por el BDE el 21 de febrero de 2023 en virtud de lo dispuesto en la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero. Dicho informe, contenía datos inexactos al no reflejar debidamente los riesgos de crédito del mes de enero de 2023 correspondientes a dos de las entidades declarantes.

El incidente declarado como “brecha de datos personales” tuvo su origen en la declaración incompleta formulada por IBERCAJA y UBS EUROPE, incumpliendo los plazos de remisión previstos en la normativa, por incidencias tecnológicas en sus sistemas que les impidieron remitir la información en plazo. No obstante, una vez solucionadas dichas incidencias, procedieron a remitir la información correctamente.

En consecuencia, la Central de Información de Riesgos del Banco de España (CIRBE) no recibió los datos omitidos por ambas declarantes antes del 16/02/2023 a las 15:00 horas, última fecha en la que los sistemas del BDE podrían haber asimilado la información que se remitiese fuera del plazo inicial de 10 días, que había sido superado por ambas entidades. Recibiendo estas declaraciones posteriormente al 16 de febrero a las 15 horas, los sistemas de la CIRBE no pudieron procesar la información completa hasta los días 22 y 24 de febrero, por lo que el BDE no pudo incluirlas en los informes que se debían remitir forzosamente el 21 de febrero.

2. Respecto al alcance del incidente:

La tipología de datos que no aparecían en la información remitida a fecha de 21 de febrero de 2023 fueron los siguientes datos económicos y financieros:

- Datos sobre los riesgos crediticios de algunos clientes de IBERCAJA que aparecían como titulares de riesgos crediticios, cuya cantidad adeudada figuraba como cero euros.

- Los importes de los créditos de XX empleados UBS ESE no eran exactos, al no incluir los pagos mensuales efectuados por estos empleados desde el último envío remitido a la CIRBE.

El informe de crédito de riesgo realizado por el BDE el 21 de febrero de 2023 en el que figuraban datos inexactos fue remitido a las (…) entidades declarantes a las que se refiere el artículo 60 de la Ley 44/2002.

Asimismo, se remitió informe ad hoc a (…) entidades que contenían información incompleta respecto a (…) afectados, potenciales clientes de dichas entidades, en aplicación del artículo 61 de la Ley 44/2002 y a 254 afectados titulares de riesgos que solicitaron acceder a sus informes al amparo del artículo 65 de Ley 44/2022.

Una vez recibidas las declaraciones completas por parte de IBERCAJA (24-2) y UBS EUROPE (22-2), el día 24/02/23 el BANCO DE ESPAÑA remite los listados completos a todas las entidades y afectados que habían recibido los listados del día 21 de febrero, comunicándoles por correo electrónico el mismo día 24 que los listados anteriores eran incompletos, por faltar los datos de estas dos entidades a los que se ha hecho referencia.

1. Respecto a los motivos por los que el BDE remitió la información de riesgo el 21 de febrero de 2023:

El BDE señala que debido a la modificación operada por la Orden ECO 699/2020, desde enero de 2021, el artículo 4.3 de la Orden ECO/697/2004 exige al Banco de España la distribución a las entidades declarantes de los informes de riesgos el día 21 de cada mes siguiente al que se generan, habiéndose eliminado la posibilidad de que el BDE pudiera determinar el plazo y alargarlo hasta disponer de toda la información completa.

El BDE se acogió a la posibilidad de remitir declaraciones complementarias antes de transcurrir 5 días desde dicho plazo (antes del día 25), que está prevista en la norma cuarta de la Circular 1/2013 del Banco de España, y en base a ella, remitió los informes actualizados el día 24, advirtiendo del error a todas las entidades receptoras, que solo estuvieron en posesión de información incompleta durante 3 días (Entre el 21 y el 24 de febrero).

En cumplimiento de la normativa aplicable, no existiendo previsión legal que habilite para prorrogar el plazo de remisión del día 21, el BDE se vio obligado a remitir los datos de que disponía a fecha de 21-02, con las omisiones de créditos de estas dos entidades, y a remitir las actualizaciones y correcciones de los mismos tan pronto como pudo procesar los datos completos, y dentro del plazo fijado en la normativa para remitir actualizaciones, que finalizaba el día 25-02.

Se alega y acredita asimismo que el BDE realizó las pertinentes actuaciones para requerir la información completa dentro de los plazos establecidos, y que tenía previstas medidas por defecto en sus sistemas que le advirtieron de que IBERCAJA y UBS EUROPE habían realizado informes incompletos, por lo que actuaron diligentemente, advirtiendo del error a las mismas, y dándoles soporte para solucionar los problemas técnicos que motivaron los errores producidos.

Y por último, se argumenta la falta de concurrencia de perjuicios producidos por la omisión de esta información, manteniendo que: "*Al consistir los errores cometidos en informar de riesgo cero de algunos créditos y no incluir parte de los créditos de otros, se trataba de "datos financieros no sensibles", por cuanto no son susceptibles de ser utilizados para cometer fraude ni determinan la situación financiera global de los Afectados.*

Además, en el Informe aportado por BDE el 12 de abril de 2023 se hace referencia a que los datos inexactos contenidos en los informes que fueron remitidos el 21/02/23, a los que denomina "datos incompletos", no han generado perjuicios a los afectados, en los siguientes términos:

> "*Un eventual tratamiento de los datos incompletos por parte de las entidades financieras receptoras de los mismos comportaría un daño o perjuicio limitado para los afectados, dado que no implicaría una falta de acceso a servicios, una afectación a su reputación, ni riesgo alguno de fraude, usurpación de identidad o pérdidas financieras. De hecho, el principal perjuicio que podría derivarse no sería imputable a los Afectados sino a las entidades financieras receptoras de los datos incompletos si, en atención a éstos, hubiesen adoptado decisiones que comportasen una selección adversa de potenciales clientes. En todo caso y en atención al escaso tiempo transcurrido entre la fecha del incidente (21/02/2023) y la fecha en que se informó de la misma a las entidades financieras receptoras de la información y se les remitió la información completa (24/02/2023), es escasamente probable que estas entidades hayan adoptado decisiones vinculadas con dicha información.*"

2. Respecto de las medidas de seguridad adoptadas para prevenir remisiones incompletas o incorrectas:

A lo largo del informe se describen las medidas preventivas que ya estaban previstas para asegurar la integridad de la información remitida, así como las correctivas que fueron adoptadas para la resolución del incidente, y las medidas correctivas que se hallan en proceso de implantación para evitar que incidentes similares vuelvan a materializarse.

En concreto, el inspector destaca la relevancia de dos de las medidas de nueva implantación que el BDE ha trasladado a esta Agencia, manifestando que con fechas de 1 y 17 de marzo de 2023, han lanzado una consulta interna al Departamento Jurídico y, en su caso, a la Delegada de Protección de Datos, y la Dirección competente, cuya decisión estaba prevista para el 15 de noviembre de 2023, en la que se proponen diversas medidas, cuya implantación sería recomendable, cuales son:

> *"-Establecimiento de un protocolo para determinar si es factible retrasar la puesta a disposición de informes de riesgos, como consecuencia de la falta de declaración de información de riesgos por alguna entidad declarante en el plazo establecido.*
> *-Análisis de la viabilidad de incluir una leyenda de no disponibilidad de informes de riesgos en caso de falta de declaración de alguna entidad."*

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del RGPD confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la LOPDGDD) es competente para resolver estas actuaciones de investigación 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
Cuestiones previas

El RGPD tiene por objeto garantizar el derecho a la protección de los datos de las personas físicas. El artículo 4.1 del RGPD entiende por "*datos personales*" "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".*

El artículo 4.2 del RGPD define el "*tratamiento*" como "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;".*

El artículo 4.7. del RGPD entiende por responsable del tratamiento "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros determine los fines y medios del tratamiento;".*

Así pues, los informes de créditos de riesgo que se deben declarar y remitir mensualmente por el BANCO DE ESPAÑA, contienen datos personales sobre las personas titulares de estos riesgos, que están siendo objeto de varias operaciones de

tratamiento (recogida de datos, procesamiento, transmisión a otras entidades, conservación…etc) de las que el BANCO DE ESPAÑA es responsable, por lo que cabe examinar los hechos declarados al objeto de determinar si este pudiera ser responsable de haber cometido alguna infracción administrativa por incumplir la normativa de protección de datos, que es plenamente aplicable a estas operaciones.

El presente procedimiento se deriva de que tanto el BDE como las dos entidades que formularon las declaraciones incompletas de informes de riesgos a las que les obliga la normativa sectorial aplicable a estas operaciones de riesgo gestionadas por la CIRBE, han notificado a esta Agencia la concurrencia de una brecha de datos personales, por considerar que no se había remitido la información completa que era legalmente exigible.

De acuerdo con lo previsto en el artículo 4.12 del RGPD, la brecha de seguridad (violación de seguridad) se define como: "*toda violación de la seguridad que ocasione 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*", lo que se entiende no concurre en el supuesto presente, toda vez que no existe destrucción, pérdida, alteración, o comunicación o acceso no autorizado de los datos que fueron recabados por el BDE y remitidos el 21 de febrero.

Descartada la concurrencia de brecha, el objeto de la investigación practicada se ha centrado en asegurar que el BDE contaba con una base de licitud adecuada para realizar su tratamiento, y a que ha realizado el mismo cumpliendo con los principios y obligaciones establecidos en la normativa de protección de datos.

III
Sobre la licitud del tratamiento realizado

El artículo 6 del RGPD relativo a la "*Licitud del tratamiento*" determina en su apartado 1 qué condiciones deben de concurrir para que un tratamiento sea considerado lícito:

> *"1. El tratamiento sólo será lícito si cumple al menos una de las siguientes condiciones:*
>
> *a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
> *b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
> *c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
> *d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.*
> *e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
> *f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que*

sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

Al respecto, el BDE alega estar actuando bajo el título legitimador previsto en el artículo 6.1.c) del RGPD, al estar obrando en cumplimiento de una obligación legal atribuida al Central de Información de Riesgos (CIRBE), servicio público gestionado por el BDE, al que se atribuye una obligación de recabar y suministrar información sobre riesgos crediticios a ciertas entidades y afectados del sector financiero.

La obligación de declarar, recabar y suministrar tal información de riesgos crediticios a la que se refiere el presente procedimiento se deriva de lo preceptuado en las siguientes normas:

En primer lugar, la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, crea la Central de Información de Riesgos y el deber de recabar mensualmente los datos riesgos de crédito que se hayan contraído hasta el mes anterior por las entidades obligadas a declarar esos riesgos que se establecen en el artículo 60.2 (entidades declarantes), encargándose de procesar la información para remitirla a todas las declarantes los informes de riesgo recopilados con periodicidad mensual. Información que solo podrá ser usada por las entidades declarantes en relación con la concesión y gestión de créditos.

"*Artículo 60. Entidades declarantes y contenido de las declaraciones.*

Primero. Tendrán la consideración de entidades declarantes, a los efectos de esta Ley, las siguientes: el Banco de España, las entidades de crédito españolas, las sucursales en España de las entidades de crédito extranjeras, las entidades de crédito que operen en régimen de libre prestación de servicios, […]

Segundo. Las entidades declarantes estarán obligadas a proporcionar a la CIRBE los datos necesarios para identificar a las personas con quienes se mantengan, directa o indirectamente, riesgos de crédito, así como las características de dichas personas y riesgos, […]

Los datos referentes a las personas mencionadas no incluirán en ningún caso, los regulados en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Los datos declarados a la CIRBE por las entidades obligadas serán exactos y puestos al día, de forma que respondan con veracidad a la situación actual de los riesgos y de sus titulares en la fecha de la declaración.

Tercero. A efectos de esta Ley se considera riesgo de crédito la eventualidad de que la entidad declarante pueda sufrir una pérdida como consecuencia del incumplimiento de alguna de las obligaciones de sus contrapartes o de los garantes de éstas en contratos tales como préstamos, créditos, descuentos, emisiones de valores, contratos de garantía, compromisos relativos a instrumentos financieros, o cualquier otro tipo de negocio jurídico propio de su actividad financiera. También se incluirán como riesgo de crédito, en todo caso,

las situaciones en las que haya tenido lugar el incumplimiento de las mencionadas obligaciones.

Cuarto. El Ministro de Economía y competitividad y, con su habilitación expresa, el Banco de España, determinará las clases de riesgos a declarar, las declaraciones periódicas o complementarias a remitir de modo que se asegure que los datos están suficientemente actualizados, las fechas a las que habrán de referirse, el procedimiento, la forma y el plazo de remisión de las mismas, el alcance de los datos a declarar a la CIRBE respecto a las características y Circunstancias de las diferentes clases de riesgo y de sus titulares".

La obligación general recogida en la Ley, se ha visto desarrollada a través de la Orden ECO/697/2004, de 11 de marzo, sobre la Central de Información de Riesgos, modificada por la Orden ECO/699/2020, de 24 de julio. Asimismo, en el ejercicio de las potestades normativas que le atribuye su estatuto, el BDE emite la Circular 1/2013, de 24 de mayo, del Banco de España, sobre la Central de Información de Riesgos.

Quedando la normativa sectorial aplicable fuera del ámbito competencial de esta Agencia.

IV

Conclusión

De todo lo expuesto se concluye que no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a BANCO DE ESPAÑA, IBERCAJA BANCO, S.A. y UBS EUROPE SE, SUCURSAL EN ESPAÑA.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la 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.

940-301023

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