- Procedimiento nº: PS/00179/2020

Recurso de reposición Nº RR/00245/2021

Examinado el recurso de reposición interpuesto por AIR EUROPA LINEAS AÉREAS S.A. contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00179/2020, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 15 de marzo de 2021, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00179/2020, en virtud de la cual se imponía a dos sanciones: primera, por vulneración de lo dispuesto en el artículo 32.1 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo RGPD), infracción tipificada en el artículo 83.4.a) del RGPD y calificada como grave en el artículo 73.g) de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDPGDD)., una multa de 500.000 € (quinientos mil euros) y, segunda, por vulneración del artículo 33 del RGPD, tipificada en el artículo 83.4.a) del RGPD y calificada como grave en el artículo 73.r) de la LOPDPGDD), una multa de 100.000 € (cien mil euros).

Dicha resolución, que fue notificada al recurrente en fecha 16/03/2021, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la LOPDPGDD, y supletoriamente en la LPACAP, en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00179/2020, quedó constancia de los siguientes:

PRIMERO: El 29/11/2018 se recibe en la AEPD escrito del reclamado señalando que el 16/10/2018 había recibido notificación del Banco Popular relativa a un incidente de seguridad provocando la activación del plan de respuestas ante incidentes el 17/10/1018.

SEGUNDO: El 18/01/2019 el reclamado aporto notificación completa a través del formulario habilitado en la sede electrónica de la AEPD, aportando documentos anexos relativos a Medidas preventivas aplicadas con anterioridad al incidente; Medidas de contención e información adicional y Justificación para no informar a los interesados afectados por el incidente.

TERCERO: El reclamado en fecha 01/04/2019 ha aportado: Informe técnico forense elaborado por IBM GLOBAL SERVICES ESPAÑA, S.A. en relación con la incidencia comunicada a la AEPD en el que se analiza la incidencia producida y recomendaciones; señalando que ***(…).***

CUARTO: El reclamado en fecha 14/11/2019 ha aportado Informe forense de FOREGENIX PFI de enero de 2019 basado en investigaciones realizadas y el análisis

de las posibles causas, señalando entre otras que "La investigación realizada por FOREGENIX identificó pruebas concluyentes de violación en AIR EUROPA"; copia del contrato de asistencia y gestión de sistemas de información y comunicaciones de 31/10/2009 entre GLOBALIA SISTEMAS Y COMUNICACIONES, S.L.U. y el reclamado en el que ostentan la condición de responsable y encargado del tratamiento respectivamente; copia el Plan de Respuesta ante Incidentes de Ciberseguridad de GLOBALIA de 05/07/2019 y Manual de Seguridad de la Información de fecha 31/10/2013

QUINTO: El 04/06/2020 el reclamado ha aportado Evaluación de impacto del tratamiento de "Venta a clientes por canales alternativos".

SEXTO: El reclamado ha aportado en periodo de pruebas documentos relativos a medidas que tenía implantadas con anterioridad al incidente de seguridad declarado.

TERCERO: AIR EUROPA LINEAS AÉREAS S.A. (en lo sucesivo el recurrente) ha presentado en fecha 16/04/2021, en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo básicamente en los siguientes hechos: que en la parte dispositiva de la resolución no se concreta la consideración de las infracciones impuestas a efectos de la LOPDGDD, siendo esta concreción necesaria a efectos del cálculo de la prescripción; que la tipificación de la infracción del artículo 33 del RGPD, tipificada en el artículo 83.4.a) de la misma norma, debería ser corregida; que teniendo en cuenta la fecha del ciberataque no existiría infracción por incumplimiento del RGPD, al no ser éste de aplicación en aquella fecha; la desproporción de las sanciones impuestas teniendo en cuenta el resultado económico del reclamado y que para la graduación de las sanciones en el caso de que no se tuvieran en cuenta los argumentos del recurrente debería tenerse en cuenta las cuentas anuales del ejercicio 2020.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 48.1 de la LOPDPGDD.

II

Debido a razones de funcionamiento del órgano administrativo, por ende, no atribuibles a la parte recurrente, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de esta Agencia respecto a la pretensión de la parte recurrente.

De acuerdo con lo establecido en el artículo 24 de la LPACAP, el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio. Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el art. 21.1 de la citada Ley. Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

III

En relación con las manifestaciones efectuadas por el recurrente, reiterándose básicamente en las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II a X ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

II

El artículo 58 del RGPD, Poderes, señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:
(…)
i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;
(…)"

El RGPD establece en el artículo 5 de los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de "integridad y confidencialidad".

El artículo señala que:

"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»)".
(…)
Por otra parte, el artículo 4 del RGPD, Definiciones, establece en sus apartados 7, 8 y 12:
"(…)
7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;
(…)
12) «violación de la seguridad de los datos personales»: 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;

(…)"

Asimismo, el artículo 24, Responsabilidad del responsable del tratamiento, establece que:

"1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

Y el artículo 25, Protección de datos desde el diseño y por defecto, señala que;

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

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

Por tanto, para subsanar una violación de seguridad el responsable del tratamiento debe ser capaz de reconocerla y la consecuencia de tal violación es que el

responsable del tratamiento no puede garantizar el cumplimiento de los principios relativos al tratamiento de los datos personales, tal como se establece en el artículo 5 del RGPD.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD.

III

El RGPD define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control.

En este mismo sentido se señala en los Considerandos 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos,

materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

IV

En primer lugar, se imputa al reclamado la vulneración del artículo 32.1 del RGPD, que señala:

"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".

El Considerando (83) señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

De las actuaciones practicadas y documentación aportada al expediente se ha verificado que las medidas de seguridad que contaba la entidad investigada en relación con los datos que sometía a tratamiento, no eran las más adecuadas para garantizar la seguridad y confidencialidad de los datos personales en el momento de producirse el incidente o quiebra.

Como señala igualmente el Considerando 39:

"…Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

Hay que señalar que las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos ya que no es posible

asegurar el derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad son necesarias medidas tanto de índole técnica como de índole organizativo.

Por tanto, los análisis de riesgos de seguridad en la información deben centrarse en la capacidad de garantizar la confidencialidad, integridad, disponibilidad de los sistemas y servicios de tratamiento, tal como lo contempla también dicho artículo.

Uno de los requerimientos que establece el RGPD para responsables y encargados del tratamiento que realizan actividades de tratamiento con datos personales es la necesidad de llevar a cabo un análisis de riesgos de la seguridad de la información con el fin de establecer las medidas de seguridad y control orientadas a cumplir los principios de protección desde el diseño y por defecto que garanticen los derechos y libertades de las personas.

Se hace necesario señalar que en el presente caso a la luz de los informes emitidos por las empresas IBM y FOREGENIX PFI acreditan vulnerabilidades graves de los sistemas del reclamado, comprometiendo la confidencialidad e integridad de la seguridad de la información provocando un acceso no autorizado que desemboco y provoco una transmisión ilícita de datos.

Como consta en el Informe de IBM de 20/12/2018, ***(…)***

Por tanto, se desprende de lo que antecede que las medidas de seguridad técnicas y organizativas implantadas por la entidad reclamada no eran apropiadas para garantizar un nivel de seguridad adecuado al riesgo e impedir un acceso no autorizado a los datos de los clientes.

Hay que señalar que dada la evolución tecnológica y digital que sufren las actividades de tratamiento de los datos personales, hay que afrontarlos desde el punto de vista de una gestión continuada del riesgo, definiendo desde el diseño las medidas de control y de seguridad necesarias para que el tratamiento se produzca respetando los requerimientos de privacidad asociados a los niveles de riesgo al que puedan estar expuestos y evaluando de manera periódica y continua la efectividad de las medidas de control implantadas.

Esto implica igualmente la protección de los datos personales desde el diseño y por defecto, es decir que el responsable debe aplicar, tanto en el momento de establecer los medios de tratamiento como en el momento del tratamiento mismo, todas aquellas medidas técnicas y organizativas adecuadas y concebidas para aplicar, de manera efectiva, los principios de protección de datos e integrar, en el tratamiento, las garantías necesarias para cumplir los requerimientos que nos señala el RGPD; además, el responsable debe aplicar las citadas medidas para garantizar que, por defecto, sólo se tratan los datos personales necesarios para cada finalidad específica del tratamiento.

El reclamado ha manifestado que la interpretación de la AEPD por el hecho de sufrir una brecha de seguridad implicaría automáticamente el incumplimiento del

artículo 32.1 del RGPD sin proporcionar motivación alguna respecto al motivo por el cual las medidas de seguridad son insuficientes.

(…)

Así, consta en los antecedentes de la presente propuesta y extractado del citado informe: ***(…)***

Esa mera posibilidad supone un riesgo que se ha de analizar y valorar a la hora de tratar los datos personales y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de los mismos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento y en función del mismo establecer las medidas que posiblemente hubieran impedido la pérdida de control de los datos y, por tanto, por parte de los titulares de los datos que le fueron proporcionados a éste como ha sido acreditado.

De acuerdo con lo señalado la actuación del reclamado supone la vulneración del artículo 32.1 del RGPD, infracción tipificada en su artículo 83.4.a).

V

El reclamado ha alegado la no aplicabilidad del RGPD puesto que al producirse el primer acceso el 12/05/2018, se cumplía en esa fecha los requisitos de seguridad exigidos por la legislación aplicable en el momento del incidente la LOPD y su Reglamento.

No obstante, tal alegato no puede ser aceptado; los hechos objeto de la presente reclamación quedan sometidos a las disposiciones del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, cuya fecha de plena aplicación fue el 25/05/2018.

El acceso a los datos personales de los afectados por la quiebra se inició antes de la fecha de plena aplicación del Reglamento (UE) 2016/679 -lo que acontece el 25/05/2018- y cuando estaba aún vigente la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, LOPD. No obstante, la conducta del reclamado en la que se concreta la infracción, quiebra de seguridad motivada por la adopción de medidas técnicas y organizativas inadecuadas, se ha mantenido en el tiempo, al menos, hasta la adopción de medidas consecuencia de la comunicación de Banco Popular al reclamado y la contratación de las empresas forenses que provoco la implementación de medidas a fin de atajar el incidente de seguridad.

(…)

La infracción de la que se responsabiliza al reclamado participa de la naturaleza de las denominadas infracciones permanentes, en las que la consumación se proyecta en el tiempo más allá del hecho inicial y se extiende, vulnerando la

normativa de protección de datos, durante todo el periodo de tiempo en el que los datos son objeto de tratamiento. En el presente caso, pese a que en la fecha en la que se inició la conducta infractora la norma aplicable era la LOPD, la normativa que resulta de aplicación es la que estaba vigente cuando la infracción deja de consumarse con la aplicación de aquellas medidas adecuadas y pertinentes a fin de que los accesos a los datos de carácter personal no se pudieran producir.

El Tribunal Supremo se ha pronunciado sobre la norma que ha de aplicarse en aquellos supuestos en los que las infracciones se prolongan en el tiempo y ha habido un cambio normativo mientras se cometía la infracción. La STS de 17/04/2002 (Rec. 466/2000) aplicó una disposición que no estaba vigente en el momento inicial de comisión de la infracción, pero sí en los posteriores, en los que continuaba la conducta infractora. La Sentencia examinó un supuesto que versaba sobre la sanción impuesta a una Jueza por incumplimiento de su deber de abstención en unas Diligencias Previas. La sancionada alegaba la no vigencia del artículo 417.8 de la LOPJ cuando ocurrieron los hechos. La STS consideró que la infracción se había venido cometiendo desde la fecha de la incoación de las Diligencias Previas hasta el momento en que la Jueza fue suspendida en el ejercicio de sus funciones por lo que esa norma sí era de aplicación. En idéntico sentido se pronuncia la SAN de 16/09/2008 (Rec.488/2006)

VI

El reclamado ha alegado que le produce indefensión la ausencia de respuesta a las pruebas presentadas a requerimiento de la AEPD de fecha 23/11/2020 y no haberse valorado las mismas, señalando, además, que le resulta muy perjudicial que la AEPD no haya tomado en consideración ni una sola de las alegaciones formuladas ni haya tenido en cuenta ni uno solo de los documentos aportados en la contestación al requerimiento cursado por la AEPD durante esa fase probatoria.

Sorprende la causa de indefensión alegada; hay que señalar que si no se hizo referencia a las mismas fue debido a que la respuesta ofrecida no hacía sino consolidar y reforzar los informes aportados por IBM y Foregenix acerca de que las medias implantadas al tiempo y momento de la quiebra producida no eran las más adecuadas para la seguridad de los datos.

Medidas que deben ser establecidas por el responsable del tratamiento teniendo en cuenta el análisis del riesgo llevado a cabo y en función del mismo aplicar aquellas medidas técnicas y organizativas más adecuadas.

(…)

VII

(…)

VIII

En segundo lugar, se imputa al reclamado la vulneración del artículo 33 del RGPD, Notificación de una violación de la seguridad de los datos personales a la autoridad de control, que establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo sucesivo RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

En este sentido el considerando 87 estable que:

"Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento".

Independientemente de las actuaciones de índole interno que se llevaron a cabo por el reclamado para gestionar la brecha o incidente de seguridad una vez que se tuvo conocimiento de la misma, el RGPD establece que en caso de brecha de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

El RGPD también establece los casos en los que una brecha de seguridad se debe comunicar al afectado, en concreto cuando sea probable que la brecha de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Tanto la notificación a la autoridad de control competente como la comunicación al afectado son obligaciones del responsable del tratamiento, aunque puede delegar la ejecución de las mismas en otras figuras.

Por tanto, lo que subyace a dicha obligación es un deber más amplio y que insta al responsable a implantar un procedimiento de gestión de incidentes de seguridad que afecten a datos de carácter personal adaptado a las características del tratamiento.

Por consiguiente, un elemento clave de cualquier política en materia de seguridad de los datos es poder, en la medida de lo posible, prevenir una violación y, cuando a pesar de todo se produzca, reaccionar de forma rápida.

Señala el RGPD que son brechas aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

En el caso examinado, de la documentación aportada en el expediente se ofrecen ***(…)***

Es cierto, como manifiesta la representación del reclamado que hubo notificación de la quiebra, si bien esta se realizó de manera extemporánea 41 días después de que fuera conocida infringiendo claramente lo dispuesto en el artículo 33 del RGPD que establece la obligación de notificar a la autoridad de control sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella.

El reclamado justifica la notificación tardía realizada porque no se tenía conocimiento suficiente de la naturaleza o alcance sufrido y que hubiera afectado a datos personales.

Sin embargo, tal alegato no puede ser admitido puesto que el responsable del tratamiento tenía pruebas claras de que se había producido tal violación y no cabían dudas de que tenía constancia de ello como consecuencia de la notificación del Banco Popular el 16/10/2018 que provoco como anteriormente se ha señalado la activación del plan de respuestas ante incidentes el día siguiente. Así figura en el informe de IBM ***(…)****.*

Además, si fuera cierto lo que el propio reclamado señala en su escrito de fecha 22/01/2019 donde manifiesta que la quiebra estaba solucionada el 17/11/2018, ¿Porque no lo notificó antes?

A más, en el análisis de riesgos efectuado respecto de la necesidad o no de notificación a la Agencia, en conclusiones, se señala que "Aplicando la metodología de análisis de la AEPD al incidente actual (Anexo 1), tanto el resultado cuantitativo como el cualitativo superan el umbral de notificación a la AEPD…"

(…)

De conformidad con lo párrafos precedentes, la actuación del reclamado supone la vulneración del 33.1 del RGPD, infracción tipificada en su artículo 83.4.a) del mismo texto legal.

IX

La vulneración de los artículos 32.1 y 33 del RGPD se encuentran tipificadas en el artículo 83.4.a) del citado RGPD en los siguientes términos:

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

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

(…)

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala 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".

Y en su artículo 73, a efectos de prescripción, califica de "Infracciones consideradas graves":

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una

vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

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

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

Los hechos acreditados evidencian la existencia de una brecha de seguridad en los sistemas del reclamado permitiendo su vulnerabilidad provocando el acceso no autorizado e ilícito a información relativa a clientes en relación con sus tarjetas bancarias, numeración, fecha de caducidad y CVV que se podría haber utilizado para la comisión de operaciones fraudulentas, lo que unido a la notificación extemporánea de la citada brecha o incidente de seguridad supone la infracción de los artículos 32.1 y 33 del RGPD.

X

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

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

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

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

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

"2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

De conformidad con los preceptos transcritos a efectos de fijar el importe de la sanción a imponer en el presente caso por las infracciones tipificadas en el artículo 83.4.a) del RGPD de la que se responsabiliza a AIR EUROPA, se estiman concurrentes los siguientes factores:

- En relación con la infracción del artículo 32.1 del RGPD tipificada en el artículo 83.4 del citado Reglamento:

La naturaleza y gravedad de la infracción dado su alcance no meramente local de la brecha de seguridad declarada, sino todo lo contrario puesto que se han podido ver comprometidos datos de carácter personal no solo de nacionales sino extranjeros, sin olvidar el elevado número de personas, clientes, al que potencialmente afecto la misma (489.000) y el número de registros afectados (1.500.000); en el informe de IBM de 20/12/2018 se señalaba que "GLOBALIA fue informada por las compañías de las tarjetas de crédito de que un gran número de tarjetas de crédito, unas 4000, habían sido utilizadas para cometer fraude" ,"Aunque IRIS no ha logrado confirmar cómo logró el atacante exfiltrar información de la red de GLOBALIA o qué fue exfiltrado, habida cuenta de la limitación de registros, lo que sí ha confirmado IRIS es que el atacante había recopilado al menos 488847 tarjetas de crédito únicas" y en el informe de FOREGENIX aportado por el reclamado el 14/11/2019 se señalaba que "La investigación de FOREGENIX identificó más de 2,7 millones de números de tarjeta únicos que habían sido extraídos de los sistemas de bases de datos por el atacante";

la categoría de datos afectados por la infracción, sin olvidar los daños y perjuicios sufridos por algunos de los clientes.

El grado de responsabilidad del responsable del tratamiento, habida cuenta de las medidas técnicas u organizativas aplicadas y que fueron vulneradas. Así, IBM señala que ***(…).***

FOREGENIX en su informe señala que ***(…).***

Pero la propia entidad reclamada ha señalado que ***(…).***

Las categorías de los datos de carácter personal que se han visto afectados como consecuencia de la infracción pues a los datos identificativos hay que unir los bancarios y financieros, consecuencia del acceso a las tarjetas, con una finalidad claramente fraudulenta. En el informe de auditoría realizado por IBM de 20/12/2018 se manifiesta que ***(…).***

La forma en que se ha tenido conocimiento de infracción pues ello se debió a una comunicación de BANCO POPULAR, y como se señala en el párrafo anterior por compañías de tarjetas de crédito, sin que la reclamada hubiera tenido constancia de la intrusión y accesos cometidos que comenzaron el 12/05/2018.

El carácter continuado de la infracción en el sentido interpretado por la Audiencia Nacional como infracción permanente, pues desde que se produjo el incidente de seguridad hasta que la brecha fue detectada transcurrió un periodo de tiempo de varios meses.

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros; es conocida la citada vinculación ya que la entidad por su actividad está en permanente contacto con clientes y terceros tratando un gran volumen de datos, lo que le impone un mayor deber de diligencia.

El volumen de negocio de la reclamada pues se trata de una de la compañía líder dentro del mercado español, en su objeto de negocio transporte aéreo; el reclamado forma parte del holding empresarial Globalia Corporación Empresarial S.A. y del que forman parte un gran número de empresas, habiendo tenido unos ingresos anuales de 2.367.061.000 € (2018) y 2.130.517.000 € (2019) y un resultado de explotación de 82.921.000 € (2018 y 93.984.000 (2019) según consta en la página web del grupo corporativo y según la última publicación del BORME el 30/12/2020 un capital social de 17.923.050 €.

Por todo ello, se establece una cuantía de la sanción por vulneración del artículo 32.1 del RGPD de 500.000 euros.

En relación con las circunstancias de la responsabilidad el reclamado ha alegado que no se han tenido en cuenta en la ponderación de la sanción la aplicación de circunstancias atenuantes, considerando que de entenderse cometida la infracción del artículo 32.1 habrían de aplicarse las siguientes circunstancias atenuantes: la escasa gravedad del incidente y el bajo nivel de perjuicios causados; las medidas

tomadas por el responsable para paliar los daños y perjuicios sufridos; la cooperación con la autoridad de control y la falta de beneficios obtenidos.

Sin embargo, tal pretensión no puede ser aceptada; las circunstancias agravantes que han sido tenidas en cuenta son las que concurren en el presente caso.

En cuanto a la gravedad de la infracción ya concurre como agravante en la gradación de la sanción por infracción del artículo 32.1: "La naturaleza y gravedad de la infracción dado su alcance no meramente local de la brecha de seguridad declarada, sino todo lo contrario puesto que se han podido ver comprometidos datos de carácter personal no solo de nacionales sino extranjeros, sin olvidar el elevado número de personas, clientes, al que potencialmente afecto la misma (489.000) y el número de registros afectados (1.500.000); en el informe de IBM de 20/12/2018 se señalaba que…"

Además, resulta llamativo que se califique de escasa gravedad a la infracción cometida cuando la propia LOPDGDD en su artículo 73 la considera a efectos de prescripción como infracción grave y cuando resulta evidente y palpable la falta de diligencia en la aplicación de las medidas adecuadas de carácter técnicas y organizativas, prolongándose desde el 12/05/2018 fecha del primer acceso hasta que se implantaron medidas apropiadas a instancias de las empresas contratadas.

En cuanto al bajo nivel de los perjuicios causados como consecuencia de la infracción, ***(…)***

Aun es más llamativo es la petición de que se considere como atenuantes la adopción de medidas tomadas por el responsable para paliar los daños y perjuicios y la cooperación con la autoridad de control, cuando no son sino obligaciones legales que se les ha de exigir a cualquier responsable y encargado del tratamiento y, más cuando como se señalaba anteriormente se ha evidenciado la falta de diligencia en la aplicación de las mismas para evitar accesos no autorizados, aunque es cierto que sus incumplimientos podrían suponer su aplicación como agravantes.

Y en cuanto a la ausencia de beneficios resulta improcedente; el RGPD se refiere a los beneficios obtenidos como consecuencia de la comisión de la infracción, no que la ausencia de beneficios deba ser considerada como atenuante.

Por tanto, valorando las circunstancias concurrentes y tomando en consideración especialmente las que operan como agravantes y que se han analizado anteriormente, se considera ponderada y proporcionada la sanción impuesta por infracción del artículo 32.1 del RGPD, dada la gravedad de los hechos producidos.

- En relación con la infracción del artículo 33 del RGPD tipificada en el artículo 83.4 del citado Reglamento:

La grave falta de diligencia en el cumplimiento de las obligaciones impuestas por la normativa de protección de datos, realizando una notificación extemporánea de la quiebra de seguridad a que estaba obligado.

La forma en que se ha tenido conocimiento de infracción pues ello se debió a una notificación de BANCO POPULAR y por compañías de tarjetas de crédito, sin que la reclamada hubiera tenido constancia de la intrusión y accesos cometidos que comenzaron el 12/05/2018.

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros; es conocido la citada vinculación ya que la entidad por su actividad está en permanente contacto y trata un gran volumen de datos, lo que le impone un mayor deber de diligencia.

El volumen de negocio de la reclamada pues se trata de una de la compañía líder dentro del mercado español, en su objeto de negocio.

Por todo ello, se establece una cuantía de la sanción por vulneración del artículo 33 del RGPD de 100.000 euros.

IV

El recurrente en su escrito de recurso ha mostrado su disconformidad con la resolución recurrida alegando la falta de concreción de las infracciones a efectos del cálculo de la prescripción; que la tipificación de la infracción del artículo 33 del RGPD, debería ser corregida; que teniendo en cuenta la fecha del ciberataque no existiría infracción por incumplimiento del RGPD y que para la graduación de las sanciones en debería tenerse en cuenta las cuentas anuales del ejercicio 2020.

En primer lugar, alega el recurrente que en la resolución recurrida se imponen dos sanciones por infracción de los artículos 32.1 y 33 del RGPD, estando tipificadas en el artículo 83.4.a) de la misma norma, si bien no concreta en su parte dispositiva, cuál es su consideración a efectos de la LOPDGDD, siendo esto necesario a efectos del cálculo de la prescripción.

Sin embargo, tal alegato debe ser rechazado.

Es cierto que, en la parte dispositiva de la resolución, en sus dispositivos Primero y Segundo se señala:

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

PRIMERO: IMPONER a AIR EUROPA LINEAS AÉREAS S.A., con NIF A07129430, por una infracción del artículo 32.1 del RGPD, tipificada en el Artículo 83.4.a) del RGPD, una multa de 500.000 € (quinientos mil euros).
SEGUNDO: IMPONER a AIR EUROPA LINEAS AÉREAS S.A., con NIF A07129430, por una infracción del artículo 33 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una multa de 100.000 € (cien mil euros).
(…)",

habiéndose omitido toda referencia a los artículos de la LOPDGDD a efectos de prescripción.

Y también lo es que la regulación de las infracciones que se hace en la LOPDGDD es más precisa en cuanto a las situaciones que dan lugar a una infracción

y su consideración, de modo que es mucho más sencillo conocer el plazo de prescripción de esa infracción (es decir, si es considerada leve, grave o muy grave) y de cara a la sanción administrativa a imponer por su incumplimiento.

No obstante, el mismo recurrente señala que ya desde el acuerdo de inicio, la Agencia ha venido señalando que el recurrente había incumplido el artículo 33 del RGPD y que esto estaba tipificado en el art. 83.4.a) de la misma norma y en el artículo 73.r) de la LOPDGDD y que la mención a este último precepto se ha mantenido inalterable a lo largo del procedimiento, incluyendo la Propuesta de Resolución y, finalmente, la Resolución.

Y en la propia Resolución recurrida, en su Fundamente IX se hace referencia al artículo 73.r) de la LOPDGDD a efectos de prescripción, estableciendo:

"(…)

Y en su artículo 73, a efectos de prescripción, califica de "Infracciones consideradas graves:

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

(…)

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

Los hechos acreditados evidencian la existencia de una brecha de seguridad en los sistemas del reclamado permitiendo su vulnerabilidad provocando el acceso no autorizado e ilícito a información relativa a clientes en relación con sus tarjetas bancarias, numeración, fecha de caducidad y CVV que se podría haber utilizado para la comisión de operaciones fraudulentas, lo que unido a la notificación extemporánea de la citada brecha o incidente de seguridad supone la infracción de los artículos 32.1 y 33 del RGPD".

En segundo lugar, considera el recurrente que la tipificación de la infracción del artículo 33 del RGPD, tipificada en el artículo 83.4.a) de la misma norma, debería ser corregida para ubicarla en el artículo 74.m) de la LOPDGDD, infracciones leves, en lugar de en el artículo 73.r) de dicho cuerpo legal, ya que de esta manera la sanción de 100.000 € debería ser igualmente revocada en la medida en que la infracción estaría prescrita.

El artículo 74 relativo a las infracciones leves señala que:

"Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

(…)

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

(…)"

En el presente caso, no nos encontramos con una notificación incompleta, tardía o defectuosa de la información relacionada con la brecha de seguridad puesta a disposición de la autoridad de control, sino de una ausencia e incumplimiento de la notificación a la autoridad de protección de datos de la incidencia de seguridad en los datos de carácter personal producida de conformidad con lo previsto en el artículo 33 del RGPD que señala que el responsable del tratamiento debe notificar la brecha sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella.

Pues bien, como ya se señalaba en la Resolución y a pesar de la gravedad de los hechos puestos de manifiesto en la misma, la brecha fue notificada 41 días después de que fuera conocida por su responsable infringiendo claramente lo señalado en el artículo 33 del RGPD.

Además, en el presente caso el responsable del tratamiento tenía pruebas claras de que se había producido tal violación no cabiendo dudas de su constancia como consecuencia de la notificación que le había realizado el Banco Popular y que provoco la activación del plan de respuestas ante incidentes el día siguiente. Así figura en el informe de IBM ***(…).***

A más, como también se señala en la resolución si fuera cierto lo que el propio reclamado señala en su escrito de fecha 22/01/2019 manifestando en el mismo que la quiebra estaba solucionada el 17/11/2018, ¿Porque no lo notificó antes?

Por último, es el propio reclamado quien señala en el análisis de riesgos efectuado y en relación con la necesidad o no de notificación a la Agencia que *"Aplicando la metodología de análisis de la AEPD al incidente actual (Anexo 1), tanto el resultado cuantitativo como el cualitativo superan el umbral de notificación a la AEPD…"*

Por lo tanto, tal argumentación debe igualmente ser rechazada.

En tercer lugar, alega el recurrente que teniendo en cuenta la fecha del ciberataque no existiría infracción por incumplimiento del RGPD, al no ser éste de aplicación en aquella fecha; que no puede entenderse que se haya cometido una infracción continuada, puesto que la infracción no pudo nacer el 12/05/2018 (considerando que las medidas implementadas por Air Europa en ese momento eran las correctas de conformidad con la legislación aplicable) y, que de entenderse que la infracción surgió el 25/05/2018 (momento en el que Air Europa debería haber implementado mayores medidas de seguridad a juicio de esta Agencia), ésta debería tramitarse como una infracción independiente de la violación de la seguridad de los datos sufrida por Air Europa, por lo que no cabría enmarcarla en el presente procedimiento sancionador.

Sin embargo, nuevamente hay que rechazar los argumentos esgrimidos por la recurrente.

Esta cuestión ya fue sometida a consideración de la AEPD a lo largo del procedimiento dando respuesta a la misma; como ya se señalaba en aquella ocasión es cierto que el acceso a los datos personales como consecuencia de la quiebra de seguridad se inició antes de la fecha de plena aplicación del Reglamento (UE)

2016/679 -lo que acontece el 25/05/2018- y cuando estaba aún vigente la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, LOPD. Sin embargo, no es menos cierto que la infracción, se proyecta en el tiempo, al menos hasta la implantación de las nuevas medidas provocadas por la comunicación de Banco Popular al reclamado y las recomendaciones de las empresas forenses participantes y que provoco la implementación de medidas a fin de atajar el incidente de la quiebra de seguridad.

El primer acceso se produce, como señala el reclamado, el 12/05/2018 fecha en la que estaba en vigor la anterior LOPD y que el RGPD no es de plena aplicación hasta el 25/05/2018; sin embargo, la infracción continuó produciendo sus efectos prolongándose en el tiempo hasta la adopción de aquellas medidas a fin de poner remedio a la quiebra en los sistemas de la reclamada.

No hay que olvidar que los accesos a los datos continuaron produciéndose hasta agosto de 2018, cesando a partir de esta fecha si bien las medidas implantadas continuaron siendo inadecuadas hasta que no se implementaron las nuevas con motivo de la comunicación y alerta provocada por el incidente.

Gravedad de la quiebra y de su consecuencia, la violación de los datos de carácter personal provocada por los accesos realizados por el hacker, que fueron confirmados no solo por las empresas actuantes que señalan entre otras la existencia de pruebas de violación de datos de titulares de tarjeta, sino por el propio reclamado indicando que tuvo que ser notificado por Banco Popular (VISA) al comprobar accesos a las tarjetas de clientes, en información aportada el 01/04/2019*: **(...)*** o cuando manifiesta en el análisis de riesgo tras el incidente que ***(...).***

Esta falta de medidas de seguridad adecuadas provoco el acceso a datos personales no autorizados, **(...).**

Por último, alega el recurrente la desproporción en las sanciones impuestas y que se debería haber tenido en cuenta para la graduación de las sanciones las cuentas anuales del ejercicio 2020.

Hay que señalar que, de conformidad con la gravedad de las circunstancias concurrentes en el presente caso, la resolución sancionadora no ha infringido el principio de proporcionalidad para la determinación de las sanciones impuestas, que resulta ponderada y proporcionada a la gravedad de las infracciones cometidas y la entidad de los hechos puestos de manifiesto y acreditados en el procedimiento, sin que se aprecien razones que deban justificar su minoración.

Además, hay que tener en cuenta la cuantía a la que puede ascender dichas sanciones de conformidad con el art. 83.4.a) del RGPD, que prevé para la infracción del artículo 32.1 y 33 del RGDP: *"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

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

Por tanto, la sanción impuesta se considera respetuosa con el principio de proporcionalidad.

V

En consecuencia, en el presente recurso de reposición, el recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos RESUELVE:
PRIMERO: DESESTIMAR el recurso de reposición interpuesto por AIR EUROPA LINEAS AÉREAS S.A. contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 15 de marzo de 2021, en el procedimiento sancionador PS/00179/2020.

SEGUNDO: NOTIFICAR la presente resolución a la entidad AIR EUROPA LINEAS AÉREAS S.A.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 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 en la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o 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 LOPDPGDD, 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 LOPDPGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional,

con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) 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 LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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