IX

NUEVAS TECNOLOGÍAS Y PROPIEDAD INTELECTUAL

La Agencia de Protección de Datos Británica notifica propuesta de sanción a British Airways por importe de 204,6 millones de euros como consecuencia de las violaciones de la seguridad de los datos personales sufridas en 2018

La multa que ha propuesto la Agencia británica de protección de datos equivale al 1,5% de la cifra de negocio global que obtuvo British Airways en el ejercicio 2017.
La sanción sería la mayor en la historia impuesta por el ente regulador.

8 de julio 2019

1.- Introducción.-

La Agencia de Protección de Datos de Reino Unido ("*ICO*", por sus siglas en inglés) ha notificado propuesta de sanción por importe de 183,39 millones de Libras (204,6 millones de Euros) a la aerolínea British Airways por las brechas de seguridad sufridas en 2018 y que comprometieron los datos personales de aproximadamente 500.000 interesados.

La aerolínea British Airways, parte del grupo aéreo IAG, sufrió varios ciberataques en 2018 con el consecuente robo y acceso ilícito a los datos personales de sus clientes. La ICO, en su notificación, ha manifestado que las escasas medidas de seguridad impuestas por la entidad comprometieron los datos personales y facilitaron el acceso ilícito a los mismos por parte de terceros.

De formalizarse dicha sanción, estaríamos ante la mayor sanción de la historia impuesta por la ICO, superando las 500.000 Libras impuestas a Facebook en el caso *Cambridge Analytica*. Con esta notificación, la ICO deja entrever las consecuencias negativas que asumirán todas aquellas entidades que no traten los datos personales conforme a la normativa europea en materia de protección de datos.

La violación de la seguridad de los datos personales afecta a clientes localizados en distintos Estados Miembros de la UE. A tal efecto, se ha designado a la ICO como la Autoridad de Control Principal en lo que respecta al presente caso, de acuerdo con el régimen de Ventanilla Única que prevé la normativa europea en

materia de protección de datos.

2. Análisis del caso y alcance de la violación de la seguridad de los datos personales.

El 6 de Septiembre de 2018, British Airways anunció que su página web oficial y aplicación móvil habían sido objetivo de un ciberataque entre las 22:58 del 21 de agosto de 2018 y las 21:45 del 5 de septiembre de 2018.

En un primer momento, la compañía afirmó que la brecha de seguridad había afectado a 380.000 clientes, corrigiendo más tarde la cifra de afectados y rebajándola a 244.000. No obstante, la ICO, en su notificación, indica que la cantidad total de afectados asciende a 500.000 personas

El acceso ilícito a los datos personales por parte de los autores del ciberataque se llevó a cabo mediante la redirección del tráfico de usuarios a una URL fraudulenta. A tal efecto, todos los usuarios que accedían a la página web y/o aplicación móvil de la compañía, reservaban vuelos y pagaban mediante tarjeta de crédito eran automáticamente redirigidos a un sitio web fraudulento en el que los responsables del ciberataque obtenían datos de identificación, contacto, 'logins', itinerarios e información relativa a las tarjetas de crédito de los usuarios, inclusive el código CVV de las mismas, permitiendo a dichos responsables realizar compras a través de las tarjetas de los clientes de British Airways.

3. Criterio de la Agencia Británica de Protección de Datos.

La ICO, en su propuesta de sanción deja entrever que los requisitos por los que impone una multa de tan elevada cuantía son los siguientes:

- *La demora en la identificación de la brecha*. La ICO en su notificación revela que el incidente de seguridad tuvo lugar en junio de 2018, contradiciendo lo expuesto por British Airways en su declaración;
- *La falta de medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales*. La Agencia británica a su vez concluye en que la gravedad del incidente se origina en parte por la falta de medidas de seguridad que contenían tanto la página web como la aplicación móvil de British Airways. A tal efecto, entiende la ICO que la falta de medidas de seguridad, en particular, en lo que se refiere a los inicios de sesión, la gestión de los pagos y los formularios de reserva, han favorecido la gravedad del incidente de seguridad.

Por el contrario, la ICO ha hecho mención en su notificación a la predisposición de British Airways a cooperar durante el transcurso de la investigación, así como la implementación de medidas reforzadas de seguridad con el fin de mitigar futuras amenazas de similares características.

4. Propuesta de sanción y futuro desarrollo del procedimiento.

A tal efecto, y en base a los criterios manifestados anteriormente, la ICO ha notificado a British Airways con propuesta de sanción por una cuantía de 183 millones de libras (204 millones de euros) por la violación de seguridad de los datos personales sufrida en su página web y aplicación móvil.

La multa que ha propuesto la autoridad británica de protección de datos es equivalente al 1,5% de los ingresos globales de British Airways en el ejercicio 2017.

British Airways dispone de 28 días para apelar la sanción. A tal efecto, Álex Cruz, CEO de British Airways, ha manifestado la intención de la compañía en realizar las pertinentes alegaciones ante la ICO con el fin de rebajar el importe de la sanción.

Adicionalmente, y conforme al Régimen de Ventanilla Única, la ICO, como Autoridad de Control Principal ha sido y será la interlocutora con British Airways, si bien cooperará y deberá tener en cuenta los puntos de vista de todas las autoridades de control de los Estados Miembros en los que sus residentes también se vieron afectados por la violación de la seguridad de los datos personales.

5. El RGPD y las violaciones de la seguridad de los datos personales.

El RGPD define las violaciones de la seguridad de los 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*."

El Comité Europeo de Protección de Datos (Ex. Grupo de Trabajo del Artículo 29), indica que la "*violación*" a la que se refiere el RGPD solamente se aplica en la medida en que afecte a datos de carácter personal y, en consecuencia, dicho incidente pueda comprometer al responsable del tratamiento en el cumplimiento de los principios del RPGD.

5.1. Notificación de las Brechas de Seguridad.

5.1.1 Notificación a la Autoridad de Control.

La normativa aplicable en materia de protección de datos obliga a notificar a la autoridad de control competente, y en ocasiones, al afectado, aquellas violaciones o brechas de seguridad que ocasionen la destrucción, pérdida, o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado de terceros.

Asimismo, la normativa exige la notificación a la autoridad de control competente en un plazo máximo de 72 horas desde que tuvieran constancia de la misma, aunque es posible hacerlo más tarde si se acreditan los motivos de la dilación. La notificación debe contemplar, al menos, cuestiones como (i) la descripción de la naturaleza de la violación, (ii) el grado de sensibilidad de los datos y el número de interesados afectados, (iii) la identificación del delegado de protección de datos o persona que vaya a gestionar la incidencia con la autoridad de control, (iv) la descripción de las posibles consecuencias de la violación y (v) las medidas que se proponen para mitigar o remediar los efectos de la violación de seguridad.

En caso de que en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información exigida, ésta será facilitada de manera gradual, a la mayor brevedad posible y sin dilación alguna.

Es conveniente recordar que no todas las violaciones de seguridad de los datos personales son susceptibles de notificación ante la Autoridad de Control. A tal efecto, aquellas violaciones de seguridad en las que el riesgo para los derechos y las libertades de las personas físicas sea improbable no estarán sujetas a notificación.

En el presente caso, British Airways consideró que la violación de la seguridad de los datos personales tenía la capacidad de producir riesgos significantes en los derechos y libertades de las personas físicas, tomándose la decisión de notificar la violación de la seguridad de los datos personales ante la ICO en fecha 6 de septiembre de 2018, si bien entiende la agencia británica que el incidente se remonta a junio de 2018.

Adicionalmente, y en cualquier caso, será necesaria la documentación de todas las violaciones de seguridad de los datos personales con el fin de que se pueda poner a disposición de la autoridad de control a efectos de verificar el cumplimiento de la normativa.

5.1.2 Notificación a los interesados afectados.

Por otro lado, la normativa aplicable contempla la notificación de la violación de seguridad de los datos personales a los propios interesados afectados, sin dilación, cuando sea probable que la misma suponga un riesgo alto para sus derechos, de forma que puedan llevar a cabo con la máxima rapidez las medidas oportunas para proteger sus intereses.

A tal efecto, British Airways, consciente de las implicaciones del incidente, notificó a sus clientes de la violación de la seguridad de los datos personales sufrida y les instó a ponerse en contacto con sus respectivas entidades bancarias.

6. Régimen sancionador.

La normativa aplicable en materia de protección de datos contempla la imposición de multas administrativas de 20.000.000 Euros o de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

A tal efecto, la ICO, en la determinación de la sanción a British Airways tomó como referencia el segundo criterio del párrafo anterior, tomando como referencia las características particulares del caso y determinando una multa sobre el 1.5% del volumen de negocio total anual global del ejercicio financiero anterior.

7. Conclusiones aplicables a las empresas que traten datos de carácter personal.

La propuesta de sanción a British Airways por parte de la autoridad de control británica obliga a las empresas a adecuarse a la nueva normativa de protección de datos y refleja la adopción por parte de las autoridades de control de la tendencia a penalizar de forma severa a cualesquiera entidades que no tratan los datos de sus interesados con suficiente diligencia.

Las empresas, independientemente de su tamaño y complejidad, tanto si son responsables o encargados de tratamientos de datos personales, deben tener establecido, en sus políticas de seguridad de la información y protección de datos, cómo van a proceder ante una brecha de seguridad. En algunos casos, toda la gestión del incidente será interna y en muchos casos de forma externa.

Asimismo, es necesario un proceso previo en el que se acuerdan las medidas técnicas y organizativas para afrontar un incidente, consistente en: la identificación de los agentes implicados en la gestión de la brecha, el análisis de riesgos y/o evaluación de impacto en caso de que sean necesarias y la definición de los “planes de respuesta a incidentes” o “plan de contingencia”.

Por último, se ha de implementar un proceso constante de revisión y actualización de las políticas y procedimientos con el fin de que los mismos garanticen en todo momento un adecuado nivel de protección. Las empresas deberán idear mecanismos de control de la seguridad de los datos personales así como concienciar a sus empleados, directivos, colaboradores, etc. del principio de responsabilidad proactiva a fin de tratar los datos personales de los interesados conforme a las obligaciones que precisa la normativa y evitar la imposición de sanciones por parte de las autoridades de control.

ONTIER

Global IP, Innovation & Entertainment Team
Author: Álvaro Vidal – Avidal@ontier.net
Contact: Joaquín Muñoz - Jmunoz@ontier.net