- Procedimiento Nº: E/02871/2019

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: La reclamación interpuesta por Don ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 17 de diciembre de 2018, reiterada en fechas 15 de febrero y 4 de marzo de 2019, en la Agencia Española de Protección de Datos.

La reclamación se dirige contra FERROCARRILS DE LA GENERALITAT VALENCIANA (FGV), con CIF Q9650001B (en adelante, el reclamado).

Los motivos en que basa la reclamación son los siguientes:

"Por medio de la presente formulo reclamación por escrito por presunta violación del derecho a la protección de datos de carácter personal por parte de Ferrocarrils de la Generalitat Valenciana, con CIF Q9650001B, y/o las empresas adjudicatarias de su software que correspondan, por los hechos que se exponen a continuación.

La empresa dispone de una aplicación para dispositivos móviles que se comunica con sus sistemas a través de una API (interfaz de programación de aplicaciones, por sus siglas en inglés) disponible públicamente en internet a través del protocolo HTTP en la siguiente dirección base: ******URL.1****.*

Se adjunta un documento que argumenta, amplía y prueba los hechos expuestos"

Junto a la reclamación aporta la auditoría se seguridad realizada por el reclamante.

SEGUNDO: Con fecha 20 de diciembre de 2018, el Delegado de Protección de Datos del reclamado presenta la notificación de la brecha de seguridad sufrida.

Con fecha 7 de enero de 2019, el Delegado de Protección de Datos del reclamado presenta notificación complementaria de la brecha de seguridad sufrida. En esta ampliación, señalan los siguientes aspectos:

Fecha de detección de la brecha

20 de diciembre de 2018

Medidas preventivas aplicadas antes de la brecha

Número de registros afectados

Número de personas afectadas

Medidas para minimizar la brecha:

Justificación para no informar a los interesados:

Acompaña informe de auditoría y el informe de la brecha de seguridad.

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), con número de referencia E/00645/2019, se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El reclamado contestó a esta Agencia indicando que ya habían contestado al reclamante sobre las causas de la incidencia. Asimismo, se informó del problema detectado a la Delegación de Protección de Datos, Subdelegación del Sector Público. Por último, añaden que han interpuesto una demanda contra el reclamante por vulneración del artículo 197 bis, 1 del Código Penal, ya que siendo secreta la clave de acceso a la aplicación figura varias veces en el documento que acompañaba su denuncia. Esto no hubiera sido posible si el reclamante no tuviese conocimientos informáticos avanzados y hubiese hecho hacking; conoce de la denuncia el Juzgado de Instrucción número 6 de Valencia.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra de seguridad) como “*todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”*

En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas.

El reclamado manifiesta que el posible origen de la quiebra, notificada en el plazo establecido legalmente, pudo ser consecuencia de una acción deliberada maliciosa del reclamante, que en todo caso superaron las medidas de seguridad implantadas.

No obstante, se significa que el reclamado disponía de medidas de seguridad razonables en función de los posibles riesgos estimados.

Por último, señalar que la actuación del reclamado, tras detectar la quiebra de seguridad debe considerarse razonablemente diligente al iniciar sin dilación una investigación interna de los hechos y tomar las medidas indicadas para minimizar los riesgos de acceso a los datos por terceros ajenos, denunciar ante el Juzgado la actuación de la persona reclamante e implantar nuevas medidas de seguridad para evitar la repetición en el futuro de hechos similares.

En cuanto al impacto del mismo, cabe señalar que no ha supuesto un alto riesgo para los derechos y libertades de los titulares de los datos y no se ha detectado una exfiltración masiva de los mismos sino únicamente el acceso a unos pocos registros, como parte de la prueba de concepto, a cargo de la persona que ha detectado y denunciado la vulnerabilidad. No hay evidencias de extracción de datos personales.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia y que al resultar insuficientes han sido actualizadas de forma diligente.

Por lo tanto, 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 al reclamante y reclamado.

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.

940-0419

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