- Procedimiento Nº: E/03889/2021

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 FACUA - ASOCIACIÓN DE CONSUMIDORES Y USUARIOS EN ACCIÓN (en adelante, la parte reclamante) tiene entrada con fecha 18 de enero de 2019 en la Agencia Española de Protección de Datos.

La reclamación se dirige contra EPIC GAMES INTERNATIONAL, S.à.r.L., (en adelante, el reclamado).

Los motivos en que basa la reclamación son que la prensa se ha referido a una brecha de seguridad en el juego FORTNITE, con lo que se ha podido tener acceso a datos de los jugadores. Acompañan la dirección del diario en e que se hacen eco de la brecha ***URL.1**.

SEGUNDO: Teniendo en cuenta el carácter transfronterizo de la reclamación y dado que el reclamado tiene su establecimiento principal o único en ***PAÍS.1**, correspondería a la autoridad de protección de datos de ese Estado actuar como autoridad de control principal, a tenor de lo dispuesto en el artículo 56.1 del RGPD.

A través del "Sistema de Información del Mercado Interior" (en lo sucesivo IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, la Agencia Española de Protección de Datos (AEPD), con fecha 29 de agosto de 2019, preguntó a la autoridad de ***PAÍS.1** si habían revisado el caso y si podían confirmar que son la autoridad competente para tratar con el caso.

Contestan, el mismo día, diciendo que aún están deliberando si es ***PAÍS.1** o ***PAÍS.2** la autoridad líder (LSA) que asumirá la reclamación.

Con fecha 25 de febrero de 2020, se vuelve a solicitad información a la autoridad de protección de datos de ***PAÍS.1**, respondiendo, el día 4 de marzo de 2020, que continúan debatiendo si le corresponde actuar a esa autoridad o a la de ***PAÍS.2**.

De conformidad con el artículo 66 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), la Directora de la Agencia Española de Protección de Datos acordó remitir la reclamación presentada por FACUA a la autoridad de control de ***PAÍS.1**, a fin de que por la misma se le diera el curso oportuno, así como proceder al archivo provisional del procedimiento, quedando automáticamente suspendidos los plazos de admisión a trámite regulados en el artículo 65.5 de la LOPDGDD, de acuerdo con lo dis-

puesto en su artículo 64.4.

Sin embargo, con fecha 13 de octubre de 2020, la autoridad alemana comunicó a las demás autoridades de control que, como resultado de una serie de investigaciones e inspecciones llevadas a cabo en el proceso de tramitación de diversos casos, habían llegado a la conclusión de que el responsable no tiene un establecimiento principal en la UE según el art. 4.16.a del RGPD y por tanto el mecanismo de ventanilla única no aplicaría. La autoridad luxemburguesa ha informado de que se encuentra en proceso de analizar si este establecimiento es realmente el principal, ya que consiste en un apartado de correos, gestionado, según corrobora la autoridad berlinesa, por empleados en un centro de la empresa en Suiza. En consecuencia, por el momento, el responsable del tratamiento sería el establecimiento de la empresa en ******PAÍS.3*** (EPIC GAMES INC.), siendo cada autoridad competente para gestionar las reclamaciones recibidas contra este responsable.

Con fecha 22 de diciembre de 2020, se inició un procedimiento de asistencia mutua, de conformidad con lo establecido en el artículo 61 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 (en lo sucesivo Reglamento General de Protección de Datos o RGPD). La autoridad de ******PAÍS.1*** considera que no se cumplen las condiciones de la guía WP244 para determinar que el establecimiento principal en Europa esta en ese estado, ya que solo hay un apartado de correos allí. La autoridad luxemburguesa necesita aclarar las cuestiones con los abogados de la reclamada, y discutir la necesidad de corregir la política de privacidad. Sugieren, en la línea de lo que ya ha dicho ******PAÍS.2*** y Epic Games, que cada autoridad contacte con Epic Games individualmente, para seguir adelante con las reclamaciones.

TERCERO**:** Con fecha 29 de marzo de 2021, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

CUARTO: A la vista de los hechos expuestos, la Subdirección General de Inspección de Datos procedió a realizar actuaciones para su esclarecimiento de los hechos objeto de reclamación, al amparo de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del RGPD, teniendo conocimiento de los siguientes extremos:

Consideraciones previas

En primer lugar, es necesario aclarar que el suceso al que hace referencia el artículo ******URL.1*** no fue una brecha de seguridad sino una vulnerabilidad de seguridad reportada externamente.

Check Point Software Technologies Ltd. ("Check Point") es una XXXXXXXXXX-XX.

Registro de actividades en el que figure el fichero de datos comprometido

Ningún fichero quedó comprometido por la vulnerabilidad detectada ***por Check Point.***

El reclamado cuenta con un registro XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Análisis de riesgo del tratamiento que ha sufrido la brecha de seguridad realizado con anterioridad al incidente de seguridad

Con anterioridad a la vulnerabilidad, el reclamado había llevado a cabo numerosas ***XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

El reclamado no realizó un análisis XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Descripción detallada y cronológica de los hechos ocurridos que incluya información sobre la detección de la incidencia y su resolución. Indicar fechas

El suceso al que hace referencia el artículo ******URL.1*** no fue una brecha de seguridad; fue una vulnerabilidad de seguridad reportada externamente.

Empleados de Check Point desarrollaron un XXXXXXXXXXXXXXXXXXXXX.

La vulnerabilidad fue subsanada de forma independiente XXXXXXXXXXXXXXXX.

El equipo de Seguridad de la Información del reclamado XXXXXXXXXXXXXXXXX.

Desde entonces, el reclamado ha establecido una página pública para notificar vulnerabilidades y una dirección de correo electrónico específica, y ha adoptado nuevas medidas para mejorar la identificación de las notificaciones de vulnerabilidades a través de los tickets de Soporte al Jugador.

Especificación detallada de las causas que han hecho posible la incidencia incluyendo información respecto de las condiciones que se dieron para que se hayan producido los hechos relatados.

El ataque hipotético desarrollado por Check Point consistía XXXXXXXXXXXXXX.

Si un hipotético atacante lograra obtener XXXXXXXXXXXXXXXXXXXXXXXXXXX.

Es importante destacar que esta vulnerabilidad se limitaba a los usuarios XXXX-XXXXXXX.

Detalle de las medidas de seguridad implementadas con anterioridad a la brecha de seguridad.

Antes de que se informara de esta vulnerabilidad, ***el reclamado había realizado evaluaciones internas XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.***

Tipología de los datos afectados.

Dado que el problema de Check Point no fue una brecha de seguridad, sino una vulnerabilidad de seguridad XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Los investigadores de Check Point únicamente comprobaron XXXXXXXXXXXXX.

Número de afectados**.**

Dado que el problema que encontró ***XXXXXXXXX*** no fue una brecha de seguridad, sino una vulnerabilidad de seguridad reportada externamente, ninguna persona se vio afectada.

Posibles consecuencias para los afectados.

Dado que el problema que detectó ***XXXXXXXXX*** no fue una brecha de seguridad, sino una vulnerabilidad de seguridad reportada externamente, no hay afectados ni consecuencias para ningún usuario.

No obstante, cabe destacar que, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Descripción detallada de las acciones tomadas con objeto de minimizar los efectos adversos indicando fecha y hora de las medidas adoptadas.

Desde que se notificó el problema, el reclamado XXXXXXXXXXXXXXXXXXXX-XX.

El reclamado no informó a los usuarios ni a las autoridades de protección de datos porque XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XX.

Descripción detallada de las acciones realizadas para la resolución final de la incidencia, incluyendo fecha y hora de las medidas.

Después de que Check Point notificara el problema al reclamado XXXXXXXXXX.

Al finalizar la investigación, el reclamado adoptó medidas XXXXXXXXXXXXXX.

Tras recibir la notificación del problema, el reclamado implementó medidas XXX-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Para garantizar que los problemas de seguridad XXXXXXXXXXXXXXXXXXXX-XX.

Además, el reclamado ha formado a los integrantes del Servicio XXXXXXXXXX-XX.

El reclamado ha incluido el programa XXXXXXXXXXXXXXXXXXXXXXXXXXXXX-XX.

Aparte de eso, el reclamado ha continuado dando prioridad a la identificación y prevención de problemas de ciberseguridad XXXXXXXXXXXXXXXXXXXXXXX-XX.

Si se tiene conocimiento de la utilización por terceros de los datos personales obtenidos a través del ataque, en cuyo caso, documentación que obre en su entidad al res-

pecto, incluyendo información en relación con posible indexación por los buscadores.

Dado que no ha habido un ataque ***XXXX***, no se han obtenido datos personales por parte de ningún tercero.

La información recogida en los artículos de prensa no es exacta ya que la investigación del reclamado indicó que la vulnerabilidad no fue explotada. Además, la información de las tarjetas de crédito nunca estuvo en riesgo, ya que, como señalamos anteriormente, el reclamado oculta parcialmente la información de las tarjetas de pago por defecto y cualquier hipotético atacante no habría podido acceder a esa información.

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

En este caso, la Agencia Española de Protección de Datos ha tramitado la reclamación presentada relativa a la brecha de seguridad de datos personales en el juego FORTNITE, con lo que se ha podido tener acceso a datos de los jugadores, produciéndose una presunta vulneración del artículo 32 RGPD.

El resultado de las actuaciones ha sido reflejado en el Hecho Cuarto.

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 vulnerabilidad de seguridad reportada externamente, a través de una empresa de software que vende productos y servicios de ciberseguridad a empresas y otras entidades. Como parte de sus actividades de marketing, algunos empleados buscan vulnerabilidades en internet y publican los hallazgos en sus blogs para promocionar los productos y servicios de la compañía.

El artículo 32 del RGPD señala lo siguiente:

“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 citado artículo contempla que "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".* En consecuencia, no adopta una relación cerrada de medidas técnicas y organizativas, sino que éstas deberán ser las apropiadas en función del nivel de riesgo previamente analizado.

En el supuesto objeto de reclamación, se trata de determinar si las medidas técnicas y organizativas eran las adecuadas al nivel de riesgo predeterminado, así como la diligencia en la reacción ante el problema de seguridad detectado por un tercero, y, en su caso, las medidas adoptadas para evitar que en el futuro pueda repetirse una incidencia de similares características que pudieran comprometer los derechos y libertades de los interesados.

De las actuaciones de investigación se desprende que la entidad investigada, en calidad de responsable del tratamiento, disponía de medidas técnicas y organizativas preventivas a fin de evitar este tipo de incidencia, pero, sin embargo, de forma excepcional se produjo la incidencia ahora analizada**.**

Antes de que se informara de esta vulnerabilidad, el reclamado había realizado ***XXXX-XXXXXXXXXXXXXXXXXXXX.***

Desde que se notificó el problema, el reclamado ha introducido cambios XXXXX.

Al finalizar la investigación, el reclamado adoptó medidas adicionales XXXXXXX.

Tras recibir la notificación del problema, el reclamado implementó medidas XXX.

Por último, dado que el problema que encontró Check Point no fue una brecha XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

En consecuencia, se debe concluir que la entidad investigada disponía de medidas técnicas y organizativas razonables y proporcionales al nivel del riesgo para evitar este tipo de vulnerabilidades y que al resultar insuficientes ha afrontado de forma diligente la identificación y corrección de la vulnerabilidad de seguridad de datos personales así como la diligente reacción ante la misma al objeto de implementar nuevas medidas razonables y proporcionales para evitar que se repita la supuesta incidencia en el futuro.

No constan reclamaciones ante esta AEPD por parte de los clientes afectados.

En consecuencia, por todo lo expuesto, se considera que la actuación del reclamado, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales y que no procede el inicio de un procedimiento sancionador al haber implantado nuevas medidas de seguridad proporcionales al riesgo evaluado para evitar la repetición de incidentes similares en el futuro, por lo que se procede a acordar el archivo de las actuaciones realizadas.

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