Expediente Nº: E/01583/2011

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante SONY COMPUTER ENTERTAINMENT ESPAÑA, S.A. en virtud de las denuncias presentadas por la organización FACUA-CONSUMIDORES EN ACCIÓN y por 15 personas cuyo nombre se relaciona en anexo, y en base a los siguientes

HECHOS

PRIMERO: Con fecha de 27 de abril de 2011 tiene entrada en la Agencia una denuncia de la organización FACUA-CONSUMIDORES EN ACCIÓN contra la compañía británica SONY COMPUTER ENTERTAINMENT EUROPE LIMITED, "*por el agujero de seguridad en su red de juegos online PlayStation Network por el que un cracker ha accedido a datos confidenciales de sus usuarios*". La organización solicita de la Agencia que, dentro de sus competencias, determine si la compañía ha vulnerado el principio de seguridad de los datos regulado en el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

A la vista de la denuncia y de las noticias aparecidas en distintos medios de comunicación a ese respecto, el Director de la Agencia Española de Protección de Datos ordena la apertura de actuaciones previas de inspección.

En fechas posteriores tienen entrada en esta Agencia escritos de denuncia de 15 personas, que se hacen eco de las noticias de prensa y en algunos casos aportan copia del mensaje electrónico recibido de SONY COMPUTER ENTERTAINMENT EUROPE, informándoles de la intrusión ilegal no autorizada en sus sistemas y de las medidas adoptadas por la entidad. Las respectivas denuncias se incorporan a las actuaciones de inspección iniciadas.

SEGUNDO: Del informe de actuaciones previas de inspección se desprende lo siguiente:

1 Al acceder a la página web URL http://es.playstation.com, desde la que se ofrecen los servicios *PlayStation Network (PSN)* y *Qriocity*, se constata que la entidad que se hace responsable de los datos proporcionados por los usuarios es SONY COMPUTER ENTERTAINMENT EUROPE LIMITED, en adelante SCE EUROPA, con establecimiento principal en el Reino Unido.

Aunque los servicios *PSN* y *Qriocity* son distintos en cuanto a los contenidos, la cuenta necesaria para acceder a ellos es única.

Al acceder a la página de "*política de privacidad*", obtenida del enlace de "*Información Legal*" del sitio web, se indica que "*PlayStation®Network EUROPE Limited recabará su información personal cuando utilice o acceda a PlayStation®Network ("PSN") o a Qriocity…*"

En el capítulo 6 del citado documento se indica que "*Puesto que los servicios de Sony Online Network son de carácter global, su información se procesará, almacenará y transferirá para los fines establecidos en esta Política de privacidad a países que no pertenecen al Espacio Económico EUROPE o (EEE), como Estados Unidos, Japón, Australia y Nueva Zelanda [….] Si no está de acuerdo con esta transferencia, no acceda ni use Sony Online Network.*"

2 De la inspección realizada el 1 de junio de 2011 en el establecimiento de SONY COMPUTER ENTERTAINMENT ESPAÑA, S.A. (en adelante SONY ESPAÑA), filial española de SCE EUROPE, de la documentación remitida a la Agencia por esta última compañía y de la información publicada en el Registro de Protección de Datos del Information Commissioner's Office (ICO), Autoridad británica equivalente a la Agencia Española de Protección de Datos, se desprende lo siguiente:

2.1 SCE EUROPE es responsable del fichero que contiene los datos de los usuarios de los servicios *PSN* y *Qriocity.*

2.2 En el Registro de Protección de Datos del ICO consta inscrito a nombre de SCE EUROPE un fichero entre cuyas finalidades figura la gestión de las cuentas relacionadas con la actividad comercial de la entidad.

2.3 SONY NETWORK ENTERTAINMENT EUROPE LIMITED, sociedad filial propiedad de SCE EUROPE al cien por cien, es quien opera la plataforma de la red PlayStation Network en Europa, Oriente Medio y África.

2.4 En el citado Registro consta inscrito a nombre de SONY NETWORK ENTERTAINMENT EUROPE LIMITED un fichero entre cuyas finalidades figura la gestión de las cuentas relacionadas con la actividad comercial de la entidad.

2.5 SONY NETWORK ENTERTAINMENT INTERNATIONAL LLC presta, en calidad de encargado del tratamiento, servicios de proceso en relación con *los datos personales del fichero de usuarios de PSN.*

2.6 *PlayStation Network* es un servicio que permite a los usuarios de diversos dispositivos comercializados por el grupo SONY acceder a productos y servicios relacionados con éstos (p.e. versiones de demostración de juegos y actualizaciones de juegos). *Qriocity*, por su parte, es un servicio de comercialización de música y video. Ambos servicios requieren la suscripción del usuario.

2.7 Un usuario del servicio puede estar asociado a una cuenta principal o, en el caso de que sea menor de edad, a una subcuenta que siempre está asociada a una cuenta principal.

2.8 Los servicios son accesibles en la URL http://es.playstation.com/....., cuyo dominio está registrado a nombre de SONY COMPUTER ENTERTAINMENT AMERICA LLC, con sede en los Estados Unidos y cuyos servidores también están ubicados en los Estados Unidos.

2.9 Durante el proceso de registro de un usuario en una cuenta principal, éste debe de proporcionar de manera obligatoria la siguiente información: Correo electrónico, Contraseña, Pregunta de seguridad y su respuesta, Identificador del usuario, Nombre y apellido, Dirección postal y país.

2.10 De manera opcional, el usuario puede introducir la siguiente información relativa a una tarjeta de crédito: tipo de tarjeta, nombre del titular, número de tarjeta, fecha de caducidad, código de seguridad y, caso de que sea distinta de la proporcionada anteriormente, dirección de facturación.

2.11 En el mensaje electrónico remitido el 27 de abril de 2011 a los usuarios de

PlayStation Network y *Qriocity* se les informa de lo siguiente: "*Hemos descubierto que entre el 17 y el 19 de abril de 2011, determinada información de usuarios de PlayStation Network y Qriocity fue puesta en compromiso en conexión con una intrusión ilegal no autorizada en nuestro sistema.*" En el mensaje se enumeran las medidas adoptadas:

- Cierre temporal de ambos servicios.
- Iniciar una investigación exhaustiva dirigida por una agencia de seguridad externa de prestigio.
- Tomar medidas rápidamente para fortalecer su infraestructura de red y reconstruir el sistema para ofrecer una mayor protección a la información de los usuarios.

Respecto de los datos que, según manifiestan, pueden haberse visto comprometidos enumeran los siguientes: nombre, dirección postal, país, correo electrónico, fecha de nacimiento, nombre de acceso, contraseña del acceso al servicio, identificador del usuario en el servicio, datos de perfil, historial de compra y dirección de facturación.

En el mensaje se indica asimismo: "*A pesar de no haber evidencia de que los datos de tarjeta de crédito hayan sido obtenidos no pueden negar esa posibilidad*" y si bien excluyen la posibilidad de que el código de seguridad de la tarjeta haya podido obtenerse. Por ese motivo recomiendan a aquellos usuarios que hubiesen facilitado dichos datos que revisen regularmente el saldo y movimientos bancarios de dichas tarjetas.

2.12 En la política de privacidad del servicio *PlayStation Network* se indica que los datos proporcionados por los usuarios que se registren se procesarán, almacenarán y transferirán para los fines establecidos en la política de privacidad a países que no pertenecen al Espacio Económico Europeo, como Estados Unidos, Japón, Australia y Nueva Zelanda.

2.13 SONY ESPAÑA ha declarado que no tiene acceso ni trata los datos de los usuarios del servicio, ya que su ámbito de negocio está limitado a la venta de consolas de la marca SONY y videojuegos desarrollados por empresas contratadas por SONY.

2.14 No se ha hallado constancia en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos de que figure inscrito algún fichero cuyo propósito sea la gestión de los datos de los usuarios de los servicios *PlayStation Network* y *Qriocity*.

2.15 Respecto de los datos del mencionado fichero:

2.15.1 A 20 de abril de 2011 existían 2.940.467 cuentas principales y 41.811 subcuentas.

2.15.2 De las cuentas principales indicadas, 334.453 habían proporcionado datos de tarjetas de crédito.

2.15.3 La clave de usuario no se guarda en claro, sino que se guarda tras procesarla con un algoritmo de resumen o *hash*.

2.15.4 Los datos asociados al código de verificación de la tarjeta no se guardan en la misma base de datos y es por ello que han declarado que no se han visto comprometidos.

2.15.5 Los datos concernientes a las tarjetas de crédito se almacenan cifrados.

2.15.6 Los datos recabados en el sitio web de *PlayStation Network* son almacenados físicamente en un centro de proceso de datos de una empresa del grupo SONY en San Diego, Estados Unidos.

2.16 Respecto del incidente de seguridad, SONY ESPAÑA declaró:

2.16.1 El incidente tuvo lugar en las instalaciones de San Diego donde se almacenaban los datos.

2.16.2 El 17 de abril de 2011 fue detectado un comportamiento anormal de los sistemas.

2.16.3 Un análisis de lo que estaba ocurriendo les llevó a la conclusión el día 19 de abril de 2011 de que se había producido una intrusión por parte de personas no autorizadas en el sistema que gestiona los datos de los usuarios registrados en los servicios *PlayStation Network* y *Qriocity*.

2.16.4 El día 20 de abril de 2011 los sistemas que proporcionaban los servicios *PlayStation Network* y *Qriocity* fueron desconectados de forma que no se pudiese producir una nueva intrusión.

2.16.5 El día 26 de abril de 2011 se remitió el mensaje electrónico antes mencionado a todos los usuarios cuyos datos podían haberse visto comprometidos.

2.17 Respecto de las medidas adoptadas para evitar que se repita un incidente de este tipo, SONY ha mencionado las siguientes:

2.17.1 Acelerar el traspaso de los datos, que estaba planificado con anterioridad, a un nuevo centro de proceso con mayores medidas de seguridad.

2.17.2 Implantación de software automatizado de gestión de control y configuración.

2.17.3 Mejora en los niveles de protección y cifrado de datos.

2.17.4 Mejoras en la detección de intrusiones, accesos no autorizados y patrones de actividad anormales.

2.17.5 Adición de nuevos muros electrónicos.

2.17.6 Creación de la figura del Jefe de Seguridad de la Información, dependiente directamente del Jefe de Seguridad de la Corporación SONY.

2.17.7 Se ha modificado el software de las consolas *PlayStation 3,* de forma que solicite a todos los usuarios que modifiquen sus claves de acceso. Dicho cambio únicamente se puede realizar desde la consola desde la

que se activó la cuenta.

2.18 La investigación de la intrusión se llevó a cabo por un equipo de SONY NETWORK ENTERTAINMENT R.L.C, además de por un equipo de auditores externos de la empresa VERIZON.

2.19 SCE EUROPE no ha facilitado información a la Agencia acerca de la estructura del fichero, para verificar el almacenamiento separado del código de verificación de la tarjeta. Tampoco se ha aportado copia del informe de auditoría, de las comunicaciones intercambiadas con los encargados del tratamiento o información justificativa del retraso en el envío de la comunicación dirigida a los usuarios.

2.20 Por la Agencia no se ha logrado obtener información adicional de SONY NETWORK ENTERTAINMENT EUROPE LIMITED.

2.21 En fecha 17 de junio de 2011 por la Inspección se solicitó la colaboración del ICO, sin que hasta la fecha se haya tenido conocimiento de la finalización de las actuaciones iniciadas por esa Autoridad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la LOPD.

II

El apartado 1 del artículo 2 de la LOPD establece:

"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito."

No se ha obtenido constancia por esta Agencia de que al tratamiento de los datos de carácter personal de los usuarios de los servicios prestados en España por SONY NETWORK ENTERTAINMENT EUROPE LIMITED le resulte de aplicación la LOPD.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a SONY COMPUTER ENTERTAINMENT ESPAÑA S.A., a la organización FACUA-CONSUMIDORES EN ACCIÓN y a cada una de las personas relacionadas en el Anexo.

3. **DAR TRASLADO** de la presente Resolución al INFORMATION COMMISSIONER'S OFFICE, de acuerdo a lo previsto en los artículos 4 y 28 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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 del referido texto legal.

Madrid, 19 de abril de 2012
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Rodríguez Álvarez