Informe 0156/2009

Se consulta como debe considerarse, a efectos de la normativa de protección de datos, la circunstancia de que determinados datos de los participantes en un juego en el servidor de la consultante quedasen a la vista como consecuencia de una manipulación fraudulenta. Se indica que la base de datos de los participantes se encontraba en un servidor diferente en el extranjero, impidiéndose así que los que hicieron un uso fraudulento accedieran a ella. Los datos que quedaron a la vista (teléfono y correo electrónico) fueron facilitados por los participantes tratándose de datos que no se exigían para la participación en el concurso.

La primera cuestión que ha de analizarse en el supuesto planteado es la de si los datos relativos al teléfono y correo electrónico constituyen datos personales, lo que determinaría la aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

A tal efecto, el artículo 2.1 de la citada Ley establece en su párrafo primero que "*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",* siendo datos de carácter personal, conforme al artículo 3 a), "*cualquier información concerniente a personas físicas identificadas o identificables*".

El artículo 5. 1 f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre considera datos de carácter personal a "*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*." Añade a su vez el artículo 5.1.o) que será persona identificable "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".*

Por consiguiente, el número de teléfono constituirá un dato de carácter personal cuanto resulte adscrito al concreto titular del mismo, o se asocie a datos que permitan identificar a su propietario, de acuerdo con la definición de datos personales contenida en la normativa examinada.

Este criterio ha sido ratificado por la Audiencia Nacional en sentencia de 8 de marzo de 2002. Según se cita en la misma "*para que exista un dato de carácter personal (en contraposición con dato disociado) no es imprescindible una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados*". Señala también que "*para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona".*

Asimismo, en sentencia de 17 de septiembre de 2008, la Audiencia Nacional ha declarado en particular respecto de los números de teléfono que "*Es claro que un número telefónico asociado a un nombre y apellidos es un dato de carácter personal pues nos proporciona información sobre una persona identificada. Es más, el propio número de teléfono, sin aparecer directamente asociado a una persona, puede tener la consideración de dato personal si a través de él se puede identificar a su titular*."

En lo que se refiere a la consideración del correo electrónico como dato personal debe hacerse referencia a lo señalado en informe de 15 de noviembre de 2005 que a continuación se reproduce:

"*La primera de las cuestiones a resolver en este caso estriba en determinar si la dirección de correo electrónico es un dato de carácter personal.*

La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular.

De lo antedicho se desprende que podemos referirnos a dos supuestos esenciales de dirección de correo electrónico, atendiendo al grado de identificación que la misma realiza con el titular de la cuenta de correo:

El primero de ellos se refiere a aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado. En este supuesto, a nuestro juicio, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que

en todo caso dicha dirección ha de ser considerada como dato de carácter personal. Ejemplos característicos de este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del estado en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso delimitarse el centro de trabajo en que se realiza la prestación).

Un segundo supuesto sería aquel en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (por referirse, por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno). En este caso, un primer examen de este dato podría hacernos concluir que no nos encontramos ante un dato de carácter personal. Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello se considera que también en este caso, y en aras de asegurar, en los términos establecidos por la Jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18.4 de la Constitución, será necesario que la dirección de correo electrónico se encuentre amparada por el régimen establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Junto con estos dos supuestos, debe añadirse, evidentemente, que si en un fichero junto con la dirección de correo electrónico aparecieran otros datos que permitieran la identificación del sujeto (tales como su nombre y apellidos, su número de teléfono o su domicilio, conjunta o separadamente), la identificación sería absoluta y no se plantearía duda de que nos encontramos ante datos de carácter personal."

En consecuencia, tanto el número de teléfono del usuario del juego como de su correo electrónico, si permiten, como en el presente caso parece deducirse de la consulta, la identificación del titular constituyen datos personales, siendo su recogida por parte de la consultante, un tratamiento de datos al que resultan de aplicación las previsiones contenidas en la Ley Orgánica 15/1999. A este respecto debe recordarse que dicha Ley al configurar el concepto de tratamiento de datos en su artículo 3 c) lo describe como las "operaciones y procedimientos técnicos de carácter automatizado o

no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

La Ley Orgánica 15/1999 impone al responsable del fichero o tratamiento la adopción de las correspondientes medidas de seguridad, disponiendo su artículo 9 en lo que a ellas se refiere lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."

El Reglamento de desarrollo de la Ley Orgánica 15/1999, al que antes se ha hecho referencia, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

Estas medidas consisten, de conformidad con lo dispuesto en el mismo Reglamento, en la elaboración de un documento de seguridad que recoja las medidas de índole técnica y organizativa acordes con la normativa de seguridad vigente, especificando entre otros aspectos: el ámbito de aplicación del documento, las medidas y procedimientos encaminados a garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, los procedimientos de notificación, gestión y respuesta ante las incidencias, la gestión de soportes o documentos y los procedimientos de realización de copias de respaldo y de recuperación.

En lo que se refiere al acceso a datos a través de redes de comunicaciones el artículo 85 del Reglamento prevé que *"Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de*

redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80."

En cuanto a la determinación del nivel aplicable en cada caso dispone el artículo número primero del artículo 81 del Reglamento que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico", s*eñalando en sus números segundo y tercero que tipo de datos exigen medidas de seguridad de nivel medio y alto, respectivamente.

Dentro de las medidas de nivel básico el artículo 90 impone la existencia de un registro de incidencias con los siguientes requerimientos "*Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas*."

El artículo 100 establece que en los ficheros cuyo nivel de seguridad deba ser medio deberán añadirse al contenido del registro de incidencias regulado en el artículo 90 "*los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación."*

En el caso planteado, parece evidente que el suceso descrito en al consulta encaja en el concepto de incidencia, al que el artículo 5.2.g) del Reglamento describe como "*cualquier anomalía que afecte o pueda afectar a la seguridad de los datos*" al haberse producido un acceso no autorizado a datos personales de que disponía el consultante, con independencia de que fuesen o no requeridos para el desarrollo del servicio de juego que prestaba, por lo que dicha anomalía debe hacerse constar en el Registro de incidencias en la forma examinada. Ello sin perjuicio de las responsabilidades administrativas a que el incumplimiento de las correspondientes medidas de seguridad, en su caso, pudiera dar lugar.

Por último, en relación con lo indicado en la consulta respecto a que la base de datos se encontraba alojada en un servidor en el extranjero, debe recordarse que el artículo 33.1 de la Ley Orgánica 15/1999 dispone que "*no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que,*

además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas".

El artículo 33.2 de la Ley Orgánica 15/1999 señala los criterios para determinar el carácter adecuado del nivel de protección que ofrece el país de destino al disponer que aquél "*se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".*

Esta autorización sólo se verá exceptuada en los supuestos previstos en el artículo 34 de la Ley, entre los que resulta destacable el supuesto de que el interesado haya dado su consentimiento (art. 34.e).) o que la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de su competencia, haya declarado que garantiza un nivel de protección adecuado (art. 34.k).

Por su parte, el Reglamento de desarrollo de la Ley Orgánica 15/1999 se refiere en su artículo 5.1 a la transferencia internacional de datos describiéndola como el "Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."

Por tanto, dado que en la consulta no se indica en que país se encontraba alojada la base de datos, deberá tenerse en cuenta que las transferencias internacionales de datos requieren autorización del Director de la Agencia Española de Protección de Datos. Esta autorización no será precisa para el movimiento de datos dentro de los países del Espacio Económico Europeo, cuando la transferencia tenga como destino un país que proporcione un nivel de protección equiparable al nuestro o cuando la transferencia se encuentre en alguno de los supuestos contemplados en el artículo 34 de la Ley Orgánica en los que se exceptúa la necesidad de autorización. No obstante, la transferencia internacional de datos deberá declararse en todo caso en el Registro General de Protección de Datos.