

EL CASO DE LA QUINCENA

Google, datos personales y el ordenamiento español

La compañía Finjan Inc. (www.finjan.com), ha informado recientemente que Google ha expuesto, por un fallo de seguridad en sus sistemas, información confidencial sobre algunos de sus usuarios en Internet. Dichos datos de carácter personal (tales como nombres de usuarios, direcciones de mail y contraseñas) suponen un atentado contra la privacidad de dichos usuarios.

Según la misma fuente, con fecha 3 de enero de 2007, en Finjan Inc. descubrieron una lista de URLs que contenía información confidencial, y que se encontraba disponible y desprotegida en los servidores de Google, por lo que desde la compañía se procedió a comunicar de forma inmediata este hecho a Google. Según confirman desde Finjan Inc., el problema ha sido resuelto y Google ha notificado de este incidente a todos los usuarios afectados.

La situación se ha solventado pero creemos que merece la pena ver cual habría sido la respuesta del ordenamiento español si la violación de la privacidad aludida hubiera estado sometida al ordenamiento español. Conviene aclarar desde un primer momento que las consideraciones que aquí hacemos no confirman ni niegan la información de referencia pues las fuentes son las ya dichas; y que Cremades & Calvo-Sotelo

Google se compromete a implementar los más altos estándares de seguridad para proteger la información confidencial

ni ninguno de sus más del centenar de abogados tenemos representación o interés directo en este asunto; por tanto este artículo ha de entenderse con un afán divulgativo y no como una "alegación de parte".

Hay que tomar en consideración que empresas como

Google otorgan la máxima importancia a la seguridad de la información que generan, reciben y almacenan. En su política de privacidad Google se compromete a implementar los más altos estándares de seguridad para proteger la información confidencial de cualquier acceso no autorizado. Por lo tanto, partiremos de la premisa de una actuación diligente y responsable por parte de la citada compañía.

Sin perjuicio de lo anterior, y tomando en consideración los hechos mencionados con anterioridad, como un supuesto que nos sirva para analizar la conducta siempre que la normativa aplicable a este caso concreto fuera la española, y con el fin de determinar la posible responsabilidad de Google, se hace necesario analizar la normativa vigente en materia de protección de datos en España.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. La LOPD califica como dato de carácter personal cualquier información concerniente a personas físicas identificadas e identificables. La Agencia Española de Protección de Datos (AEPD) ha concretado más aún este término, aclarando que datos tales como la IP de un usuario así como su correo electrónico, tendrían la consideración de datos de carácter personal.

En virtud de ello, se hace necesario que los responsables de los ficheros que contengan datos de carácter personal adopten determinadas cautelas en cuanto al tratamiento de dicho tipo de información.



JUAN IGNACIO PEINADO GRACIA
Catedrático de Derecho mercantil de la Universidad de Jaén
Socio de Cremades & Calvo-Sotelo



MIGUEL ANGEL MATA GONZÁLEZ
Asociado de Cremades & Calvo-Sotelo

Con la finalidad de proteger información tan sensible, la LOPD recoge de forma clara el deber de secreto profesional, tanto del responsa-

La LOPD califica como dato de carácter personal cualquier información concerniente a personas físicas identificadas

ble y del encargado de tratamiento de datos de carácter personal, así como de todos aquellos que intervengan en el mismo. Junto a este deber de confidencialidad se exige, asimismo, un deber de seguridad en el tratamiento de dichos datos. En concreto, el artículo 9 de la LOPD obliga

al responsable del tratamiento a designar a un responsable que ofrezca garantías suficientes para que se produzca un tratamiento de datos seguro. Asimismo, a través del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, se regulan detalladamente las técnicas y las medidas organizativas que deberán ser adoptadas con el fin de que se garantice la seguridad de los datos de carácter personal y se evite un acceso no autorizado, considerando el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.

La LOPD impide, por tanto, que puedan registrarse datos de carácter personal en ficheros que no reúnan las condiciones de seguridad necesarias, ni tampoco en centros de tratamiento, locales, equipos, sistemas y programas que no aseguren la seguridad de los datos en ellos contenidos.

El artículo 37 de la LOPD, por su parte, otorga a la AEPD la potestad sancionadora, de acuerdo con el régimen de infracciones y sanciones establecidas en la LOPD. El artículo 44 f) de la LOPD, tipifica como infracción grave el mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad, pudiendo ser sancionada con multa de entre sesenta mil y trescientos mil euros.

En nuestra opinión, y siempre bajo las premisas del supuesto, esta sería la sanción a la que se vería expuesta cualquier compañía, en el supuesto de que la AEPD considerase que no se han impuesto las medidas de seguridad oportunas para mantener la seguridad en los datos.

En cualquier caso, la cuantía de las sanciones vendrá de-

terminada por la naturaleza de los derechos personales afectados, el grado de intencionalidad, los posibles daños y perjuicios causados a las personas interesadas y a terceras personas, así como cualquier otra circunstancia relevante que permita determinar el grado de culpabilidad presente en la concreta actuación infractora.

Queda dada pues la información sin otra finalidad, como es obvio, que la meramente divulgativa. No obstante, quizás merezca la pena que el lector se pregunte por la proporcionalidad entre el mal hecho, daño causado y la sanción prevista. El sistema punitivo tiene por supuesto una función preventiva, de creación de estímulos mediante un sistema de premios y castigos para estimular en las empresas que manejan estos datos sensibles un comportamiento extremadamente diligente.

Junto a estas respuestas legales, el mismo mercado exige unos estándares de seguridad que empresas como Google cumplen y, por ello, incluso los incorporan a sus políticas de privacidad. Éstas tienen la consideración de declaraciones unilaterales que generan exigibilidad por terceros. Los daños, si los hubiera, quedan satisfechos a través de acciones indemnizatorias. Llegado a este punto, es la mera infracción, independientemente del daño, la que genera la sanción.

Junto al deber de confidencialidad se exige asimismo, un deber de seguridad en el tratamiento de dichos datos

El lector llegará a sus propias conclusiones, la nuestra es que el mecanismo español de protección de datos y las sanciones previstas presentan una gran desproporción y, por ello un plus de protección que puede llegar a convertirse en una amenaza para el desarrollo del propio sector. □