Expediente Nº: E/03166/2010

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de denuncia presentada ante la misma por doña ***B.B.B.*** y en base a los siguientes

HECHOS

PRIMERO: Con fecha de 11 de octubre de 2010 tiene entrada en esta Agencia un escrito de la denunciante en el que denuncia a una usuaria de *TUENTI* por publicar, de forma sucesiva en dos eventos de la red social, una fotografía (tomada sin su consentimiento en el entorno escolar) de su hija, menor de edad.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. La denunciante ha aportado copia impresa de varias páginas aparentemente extraídas de la red social *TUENTI*, en las que figura una fotografía de su hija, asociada a dos eventos distintos: "*quien no ha tenido a una hija de puta por amiga?*" y "*yo también tengo más de un@ amig@ fals@s que inventan*". En ambos casos se hace constar que la foto fue subida el 28 de septiembre a las 16:10 por la usuaria ***C.C.C.***, que según la denunciante cuenta con 13 años de edad.

2. TUENTI TECHNOLOGIES, S.L. ha confirmado a la Agencia que los documentos aportados por la denunciante parecen indicar "*que la usuaria ' **C.C.C.**' se unió a esas páginas y colgó esas fotografías en ambas*". La compañía tiene constancia de que en la actualidad existe un evento con nombre idéntico al primero de los mencionados, creado por otra usuaria, con 3.867 usuarios adheridos y configuración de privacidad '*abierta*' (no siendo posible determinar el número de usuarios que tienen o han tenido acceso a la misma), pero que no contiene actualmente la fotografía de la hija de la denunciante. Respecto del segundo de los eventos, la compañía ha declarado no conservar ningún rastro. En definitiva, TUENTI TECHNOLOGIES, S.L. no puede certificar que la fotografía hubiera sido efectivamente colgada en ninguno de los dos eventos.

3. TUENTI TECHNOLOGIES, S.L. ha manifestado que, en contestación a la solicitud de cancelación presentada por la denunciante ante .....@tuenti.com en fecha no determinada, la compañía requirió información adicional acerca de la identificación del perfil denunciado, no obteniendo respuesta de la denunciante.

4. En relación con la fecha de nacimiento que la usuaria denunciada consignó en su perfil (2 de septiembre de 1991), TUENTI TECHNOLOGIES, S.L. ha manifestado que, tras analizar el perfil, pudo confirmar que la usuaria había "*falseado su edad*", procediendo a solicitarle copia de su DNI, siguiendo el procedimiento habitual de verificación en caso de sospecha. No obstante, la compañía también ha declarado que "*como medida preventiva, procedemos a la eliminación del perfil de la usuaria ' **C.C.C.**', por considerarlo contrario a nuestras Normas y Condiciones de Uso.*"

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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos,* define el fichero en su artículo 2 como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

La LOPD lo define en su artículo 3 como "*b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.* Así, todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados. El mero cúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la Ley.

Íntimamente vinculado al concepto de fichero está el de tratamiento de datos. La Directiva establece que el concepto de "*tratamiento*" no puede depender de la técnica utilizada para el manejo de los datos, de ahí que incluya tanto el tratamiento automatizado como el manual (considerando 27 de su Preámbulo). Así, lo relevante para que estemos ante un "*tratamiento de datos personales*" es la realización de determinadas actuaciones en relación con los mismos, actuaciones que en su descripción son muy amplias y variadas.

Desarrollando este principio, el artículo 2 de la Directiva describe las actuaciones que, aplicadas a los datos personales, constituyen "*tratamiento*": "*cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción*".

La LOPD lo define de forma muy similar en el *art. 3.c) de la Ley Orgánica 15/1999*: "*c) Tratamiento de datos: 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.*"

No basta, sin embargo, la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y sus garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, grabación,

conservación,... se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero.

La Directiva fija en su artículo 3 que sus disposiciones se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

La LOPD, por su parte, describe en su artículo 2 su ámbito de aplicación mediante una descripción general positiva más genérica que la de la Directiva: "*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"*.

En sentencia de 20 de abril de 2009, la Audiencia Nacional confirmó: "*Un sitio web exige siempre, cualquiera que sea su finalidad, una organización o estructura que permita el acceso por terceros a la información en él contenida. Cumpliría así la primera de las exigencias de un fichero, la estructural u organizativa.*" La propia Audiencia Nacional reproduce parcialmente el contenido de la sentencia de 6 de noviembre de 2003 del Tribunal de Justicia de la Unión Europea (*caso Lindqvist*):

"*El concepto de «datos personales» que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva «toda información sobre una persona física identificada o identificable». Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones.*

En cuanto al concepto de «tratamiento» de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46 , éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales». Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole.

Queda por determinar si dicho tratamiento está «parcial o totalmente automatizado». A este respecto, es preciso observar que difundir información en una página web implica, de acuerdo con los procedimientos técnicos e informáticos que se aplican actualmente, publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada.

Por tanto, procede responder a la primera cuestión que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46."

El artículo 6 de la LOPD dispone, en sus apartados 1 y 2, que el tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público o bien que existe

una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento, siempre que los datos de que se trate sean necesarios para el mantenimiento o cumplimiento del contrato.

III

El Grupo de Trabajo del artículo 29 (GT29), órgano consultivo europeo independiente establecido en virtud del artículo 29 de la Directiva 95/46/CE, adoptó el 12 de junio de 2009 la Opinión 5/2009, sobre las redes sociales en línea. Este documento se centra en cómo el funcionamiento de los servicios de redes sociales (SRS) puede satisfacer los requisitos de la legislación sobre protección de datos de la Unión Europea.

En particular, en el documento se destaca cómo muchos usuarios de las redes sociales se mueven dentro de una esfera puramente personal, poniéndose en contacto con gente como parte de la gestión de sus asuntos personales, familiares o domésticos. Según destaca el GT29, la citada Directiva no impone las obligaciones de un responsable de datos a un individuo que procesa datos personales "*en el transcurso de actividades estrictamente personales o domésticas*". Siguiendo este precepto, el GT29 estima que, con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un SRS debe aplicarse lo que denomina "*exención doméstica*", en lugar de la normativa de protección de datos.

Ahora bien, en la Opinión se especifican así mismo tres supuestos en los que tales actividades no estarían cubiertas por la "*exención doméstica*". El primer supuesto se refiere a los casos en los que se utiliza el SRS como plataforma de colaboración para una asociación o una empresa. Si un usuario de SRS actúa en nombre de una sociedad o asociación, o utiliza el SRS principalmente como una plataforma para conseguir objetivos comerciales, políticos o benéficos, la exención no se aplica. En este caso, el usuario asume todas las obligaciones de un responsable de datos que está revelando datos personales a otro responsable de datos (el SRS) y a terceros (otros usuarios del SRS o, potencialmente, otros responsables de datos con acceso a los mismos). En estas circunstancias, el usuario necesita el consentimiento de las personas concernidas o algún otro fundamento legítimo dispuesto en la Directiva de Protección de Datos.

El GT29 expone que los prestadores del SRS deben garantizar la instauración de configuraciones por defecto gratuitas y que respeten la privacidad, restringiendo el acceso a los contactos seleccionados. En estas condiciones, cuando el acceso a la información del perfil se amplía hasta más allá de los contactos seleccionados, como cuando se facilita el acceso al perfil a todos los miembros del SRS o cuando los datos son indexables por motores de búsqueda, el acceso se sale de la esfera personal o doméstica. De igual manera, si un usuario toma una decisión informada de ampliar el acceso más allá de los "amigos" seleccionados, las responsabilidades inherentes a un responsable de datos se activan. Efectivamente, se aplicará el mismo régimen legal que cuando cualquier persona utiliza otras plataformas tecnológicas para divulgar datos personales en Internet. En varios Estados Miembros, la falta de restricciones de acceso (y así el carácter público) significa que la Directiva de Protección de Datos se aplica en el sentido de que el usuario de Internet adquiere

responsabilidades de un responsable de datos. No obstante, el GT29 hace constar que, aunque la exención doméstica no se aplique, el usuario de SRS puede beneficiarse de otras exenciones como la exención con fines periodísticos o de expresión literaria o artística. En dichos casos, se ha de llegar a un equilibrio entre la libertad de expresión y el derecho a la privacidad.

Finalmente, el GT29 aborda un tercer escenario en que la "*exención doméstica*" no sería aplicable. Se trata de aquellos supuestos en los que es preciso garantizar los derechos de terceros, particularmente en relación con datos sensibles. No obstante, se hace constar que, aun cuando se aplique la "*exención doméstica*", un usuario podría ser responsable de acuerdo con las disposiciones generales de la legislación civil o penal nacional en cuestión (por ejemplo, por difamación, responsabilidad civil extracontractual por suplantación de personalidad, responsabilidad penal).

En la Opinión se aclara el concepto de "*datos sensibles*". Así, los datos que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la vida sexual se consideran sensibles. Los datos personales sensibles solo se pueden publicar en Internet con el consentimiento explícito del sujeto de datos o si el sujeto de datos ha hecho que los datos sean manifiestamente públicos él mismo.

El GT29 expone que en algunos Estados Miembros de la UE, las imágenes de los sujetos de datos se consideran una categoría especial de datos personales, ya que se pueden utilizar para distinguir entre orígenes raciales/étnicos o pueden utilizarse para deducir las creencias religiosas o los datos sobre la salud. El GT29, en general, no considera que las imágenes en Internet sean datos sensibles, a menos que éstas se utilicen claramente para revelar datos sensibles acerca de los individuos.

En consecuencia, de conformidad con el criterio interpretativo mantenido por el GT29, es preciso que concurra alguno de los escenarios expuestos, en los que la "*exención doméstica*" no resulta de aplicación, para que sean aplicables los requisitos previstos en la LOPD.

Sin embargo, en el apartado 3.9 de la Opinión el GT29 aborda los derechos de los individuos afectados que, de acuerdo con las disposiciones expuestas en los artículos 12 y 14 de la Directiva 95/46/CE, deben respetar los SRS. Así, el GT29 concluye que los derechos de acceso, rectificación y cancelación no se limitan a los usuarios del servicio, sino a cualquier persona física cuyos datos se procesen. Los miembros y no miembros de los SRS deberán tener un medio de ejercitar tales derechos.

IV

Al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".* De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que *"Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el art. 137 de LRJPAC: *"1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan esta imputación.

En el caso que nos ocupa, a partir de las actuaciones de inspección practicadas no se han hallado elementos probatorios suficientes que permitan establecer de forma fehaciente que hubieran sido tratados los datos de la hija de la denunciante en el perfil de la denunciada, ni tampoco el número de usuarios que habrían tenido acceso efectivo a tales datos. No obstante, es preciso incidir en la necesidad de que los usuarios de redes sociales (y sus padres o tutores, cuando aquéllos son menores de edad) tomen conciencia de la responsabilidad que adquieren al difundir a través de Internet datos personales de terceros (incluyendo su imagen) sin el consentimiento de éstos, siendo en todo caso aplicable el régimen sancionador previsto en el artículo 44 de la LOPD, de conformidad con el criterio mantenido por esta Agencia y ratificado por la Audiencia Nacional.

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 ***B.B.B.*** y a ***A.A.A..***

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, 16 de noviembre de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte