Procedimiento Nº: A/00179/2012

RESOLUCIÓN: R/01994/2012

En el procedimiento A/00179/2012, instruido por la Agencia Española de Protección de Datos a D. ***C.C.C.***, vista la denuncia presentada por doña ***E.E.E.,*** don ***A.A.A.,*** doña ***G.G.G.*** y doña ***D.D.D.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 27 de diciembre de 2011 tiene entrada en esta Agencia un escrito firmado por doña ***E.E.E.,*** don ***A.A.A.,*** doña ***G.G.G.*** y doña ***D.D.D.*** (en lo sucesivo, los denunciantes), profesores de un colegio rural de la provincia de Córdoba, denunciando la creación de un perfil en la red social *Facebook* a través del cual se han publicado, de forma no consentida, fotografías con la imagen de alguno de los profesores (obtenidas a partir de sus respectivos perfiles en la red social), acompañadas de distintos insultos y alusiones dirigidos a ellos, algunos de contenido sexual.

SEGUNDO: A la vista de los hechos denunciados, por la Subdirección de Inspección, se realizaron actuaciones de investigación solicitando información al denunciado, teniendo conocimiento de los siguientes hechos:

a) Los denunciantes han aportado a la Agencia copia de las respectivas diligencias de su comparecencia ante la Guardia Civil el 17 de diciembre de 2011 (atestado nº ***NÚMERO-ATESTADO.1), para denunciar los mismos hechos. Han aportado asimismo copia impresa de varias páginas de la red social *Facebook* reproduciendo el muro del perfil " ***B.B.B.***", en el que figuran conversaciones mantenidas con otra usuaria, " ***F.F.F.***", incluyendo alusiones despectivas a los cuatro profesores, así como fotografías de varias profesoras. Los nombres de ambos perfiles son identificados por los profesores como correspondientes a dos alumnas del centro educativo, si bien no tienen constancia de que los autores de ambos perfiles sean efectivamente esas alumnas.

b) En fecha 3 de enero de 2012 desde la Inspección se verificó que esos contenidos seguían siendo accesibles públicamente, para cualquier usuario de la red social *Facebook*, a través del perfil " ***B.B.B.***".

c) A partir de las actuaciones practicadas por la Inspección se ha tenido conocimiento de que el citado perfil fue creado y actualizado entre los días 15 y 19 de diciembre de 2011 a través de 9 conexiones distintas realizadas desde un terminal conectado a una línea telefónica de la que es titular don ***C.C.C.***.

d) En respuesta al requerimiento de la Inspección, en el que se indagaba sobre el perfil denunciado, don ***C.C.C.*** ha declarado que desconocía los hechos denunciados y que "*Una vez realizada las comprobaciones oportunas resulta que mi hija menor de edad,* ***F.F.F.*** *con D.N.I. […] presuntamente creó dicho perfil, desconociendo si lo hizo sola o acompañada de otros compañeros*". De acuerdo con la documentación aportada,

la menor tenía diez años en el momento de producirse los hechos.

TERCERO: Con fecha 22 de junio de 2012, el Director de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00179/2012. Dicho acuerdo fue notificado a los denunciantes y al denunciado.

CUARTO: Con fecha 24/07/2012 se recibe en esta Agencia escrito del denunciado en el que comunica: *"…He procedido dar de baja el Internet de mi línea* ***H.H.H.****, adjunto recibo de la compañía telefónica para comprobación.*

SEGUNDO.- Tras multitud de intentos para eliminar el perfil, lo hemos conseguido con fecha actual, pudiéndolo comprobar por ustedes mismos.

TERCERO.- Le suplico adopte las medidas necesarias para solucionar este problema, y me reitero en mi desconocimiento en todo este asunto…"

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

Los hechos expuestos, tratamiento de los datos personales de los profesores en la red social *Facebook*, sin su consentimiento previo, suponen una infracción del artículo 6.1 de la LOPD, que señala que: *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa",* infracción tipificada como grave en el artículo 44.3.b) de dicha norma, que considera como tal: *"Tratar los datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo*". Dicha infracción podría ser sancionada con multa de 40.001 a 300.000 euros, de acuerdo con el artículo 45.2 de la LOPD.

III

El artículo 6.2 de la LOPD establece que *"no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del*

interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado."

Por su parte, resulta necesario indicar que el Tribunal Supremo, en una reciente sentencia de la Sala de lo Contencioso, de fecha 8 de febrero de 2012 ha declarado el requisito de que los datos personales figuren en fuentes accesibles al público contrario a derecho, concretamente, al artículo 7 letra f) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. Este último, si bien requiere que el tratamiento sea necesario para la satisfacción del interés legítimo perseguido y que no prevalezca el interés o los derechos y libertades fundamentales del interesado, no exige que los datos personales figuren en fuentes accesibles al público.

De acuerdo con el criterio mantenido por la Audiencia Nacional, al tratamiento de datos de carácter personal en Internet le resulta de aplicación la normativa española de protección de datos. En particular, resulta relevante la sentencia de 20/04/2009 (recurso 561/2007), donde el órgano judicial aplica los fundamentos de la sentencia de 7/11/2003, del Tribunal de Justicia de la Unión Europea (caso Lindqvist*. Asunto C-101/01)*, al entender 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."*

IV

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 el Dictamen 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 el Dictamen 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 el Dictamen 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.

No obstante, en el apartado 3.9 del Dictamen 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.

Una gran proporción de los servicios de los SRS son utilizados por niños o menores de edad. Un dictamen previo del GT29 se había centrado en la aplicación de los principios de protección de datos en el entorno escolar y educativo, enfatizando la necesidad de tener en cuenta el mejor interés del niño, como también se destaca en la Convención sobre los Derechos del Niño de la ONU. El GT29 subraya la importancia de este principio también en el contexto de los SRS.

Las Autoridades de Protección de Datos han acometido algunas iniciativas importantes en todo el mundo, que se centran principalmente en la concienciación sobre los SRS y sus posibles riesgos. El GT29 anima a que se investigue más en cómo afrontar las dificultades relacionadas con la adecuada verificación de la edad y la obtención de pruebas del consentimiento informado, con el fin de gestionar mejor estos retos. Basándose en las consideraciones efectuadas hasta ahora, el GT29 considera que una estrategia diversificada sería apropiada para gestionar la protección de los datos de niños en el contexto de los SRS. Dicha estrategia se basaría en:

- iniciativas de concienciación, que son fundamentales para garantizar la implicación activa de los niños (a través de las escuelas, la inclusión de los elementos esenciales de la protección de datos en el currículo educativo, la creación de herramientas educativas específicas y la colaboración de los organismos nacionales competentes);
- un proceso justo y legítimo con relación a los menores, como no pedir datos sensibles en los formularios de suscripción, no utilizar márketing dirigido específicamente a menores, el consentimiento previo de los padres antes de suscribirse y grados adecuados de separación lógica entre las comunidades de niños y adultos;
- la implementación de Tecnologías de Mejora de la Privacidad (*PET*, por sus siglas en inglés) - por ejemplo, una configuración respetuosa con la privacidad por defecto, cuadros emergentes de advertencia en los pasos adecuados, software de verificación de la edad;
- la autorregulación de los proveedores, para fomentar la adopción de códigos de práctica, que se deberán equipar con medidas de aplicación efectivas, también disciplinarias en su naturaleza;
- si es necesario, medidas legislativas específicas para disuadir de prácticas engañosas o injustas en el contexto de los SRS.

En el presente caso, se ha constatado por la Inspección que los datos de carácter personal de los denunciantes, incluyendo fotografías con la imagen de alguno de ellos, han sido tratados en *Facebook* sin el consentimiento previo de los afectados, siendo accesibles por cualquier usuario de esta red social. En consecuencia, de acuerdo

con los criterios expuestos, no resulta de aplicación la "exención doméstica", siendo plenamente aplicable a ese tratamiento la normativa de protección de datos.

V

En Sentencia de 20/10/2011 la Audiencia Nacional confirmaba la sanción impuesta por la Agencia al titular de una línea telefónica desde la que se había colgado un video en internet. En esta Sentencia se argumentaba: "*En este caso, quien incluye el video en YouTube es el responsable del tratamiento pues decide, a través de dicha inclusión en Internet, sobre la publicación y difusión del citado video, y en definitiva sobre la finalidad del tratamiento, ostentando la condición de responsable del tratamiento. Puesto que, como se ha expuesto anteriormente de forma detallada, el vídeo fue incluido en la cuenta de usuario utilizando la "Contraseña' de YouTube y la cuenta y contraseña fueron creadas desde la línea titularidad del recurrente instalada en su domicilio, debe considerarse al recurrente responsable del tratamiento y, por tanto, responsable de la infracción por el tratamiento inconsentido de datos consecuencia de la inclusión del video en YouTube.*"

En el presente caso se ha logrado acreditar por la Inspección de Datos que desde la línea de la que es titular don ***C.C.C.*** se creó y actualizó un perfil en la red social *Facebook* con los datos de carácter personal de los denunciantes, sin el consentimiento de estos, por lo que, de acuerdo con la referida Sentencia, la responsabilidad por el tratamiento ha de ser imputada a dicho titular, habida cuenta de que no se ha concretado la identidad del autor material de los hechos, si bien los indicios apuntan a la participación en los mismos de su hija menor de edad.

VI

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) ha añadido un nuevo apartado 6 al artículo 45 de la LOPD, en lugar del existente hasta su promulgación del siguiente tenor:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine**,** acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

La Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las

Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC), en su artículo 128. 1 establece: *"1. Serán de aplicación las disposiciones sancionadoras vigentes en el momento de producirse los hechos que constituyan infracción administrativa."*

No obstante, dicha ley que, al decir de su Exposición de Motivos (punto 14) recoge "*los principios básicos a que debe someterse el ejercicio de la potestad sancionadora de la Administración y los correspondientes derechos que de tales principios se derivan para los ciudadanos extraídos del Texto Constitucional y de la ya consolidada jurisprudencia sobre la materia*"- consagra el principio de aplicación retroactiva de la norma más favorable, estableciendo en el artículo 128.2 que "*las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor*".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6. Junto a ello se constata una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de su actividad con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

En el presente caso, ha quedado acreditado que el denunciado ha comunicado a esta Agencia las medidas correctoras adoptadas. Desde esta Agencia se ha verificado la medida adoptada (baja del perfil en la red social *Facebook* del perfil " ***B.B.B.***"). Teniendo en cuenta estas circunstancias, no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00179/2012**) a D. ***C.C.C.*** con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.b) de la citada Ley Orgánica.

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- NOTIFICAR el presente Acuerdo a D. ***C.C.C.***.

3.- NOTIFICAR el presente Acuerdo a doña ***E.E.E.***, don ***A.A.A.***, doña ***G.G.G.*** y doña ***D.D.D.***

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.