Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

CN11-013

DICTAMEN QUE SE EMITE EN RELACION CON LA CONSULTA FORMULADA POR EL INSTITUTO MUNICIPAL DE DEPORTES DE XXXXX RELATIVA A LAS MEDIDAS A ADOPTAR POR LAS ADMINISTRACIONES PÚBLICAS QUE PRETENDEN UTILIZAR LOS SERVICIOS DE LA WEB 2.0

ANTECEDENTES

PRIMERO. Con fecha 18 de marzo de 2011 tuvo entrada en la Agencia Vasca de Protección de Datos solicitud de informe remitida por el Instituto Municipal de Deportes de XXXXX en el que se solicita respuesta a la cuestión recogida en el encabezamiento y que reproducimos a continuación:

> *"El Instituto Municipal de Deportes de XXXXX (IMD) es un organismo autónomo municipal dependiente del Ayuntamiento de XXXXX. Recientemente, este IMD ha comenzado un nuevo proyecto comunicativo basado en la utilización de las redes sociales para establecer diferentes canales de comunicación con sus clientes y trazar así diferentes campañas de publicidad y marketing.*
>
> *Para ello, este IMD ha procedido a autentificarse en las siguientes utilidades web:*
>
> - *Facebook: se ha creado una página bajo la dirección IMD XXXXX-XXXXXko UKE.*
> - *Twitter: dispone de un perfil con la dirección @imdXXXXX*
> - *Flickr: Dispone del perfil IMDXXXXX*
> - *Youtube: Dispone de la cuenta IMDXXXXX*
> - *Picasa: Dispone del perfil IMDXXXXX*
> - *Tuenti: se ha creado una página bajo la dirección IMD XXXXX – XXXXXko Uke.*
>
> *Todas estas herramientas pretenden ser utilizadas como medio de difusión de todas nuestras actividades, así como de plataforma para la conversación y*

comunicación entre las diferentes personas que están interesados/as en nuestro servicio.

En estos momentos, toda la información que se ha volcado en la nube obra en el poder de los ficheros internos del IMD XXXXX Del mismo modo, tal y como podrán comprobar, todas las fotografías que se han exportado a las plataformas web son imágenes sin presencia de ninguna persona y de espacios deportivos dependientes en su totalidad de este IMD.

La consulta que se formula a la Agencia Vasca de Protección de Datos, en el marco de las funciones que el encomienda el artículo 37 de la Ley orgánicas 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, se refiere a si, al amparo de la dicha Ley y de cualquier otra normativa que pueda resultar de aplicación, este IMD debe poner en marcha algún tipo de acción con el objeto de regular y normalizar el volcado de información que se pueda producir a la nube.

A la vista de lo expuesto este IMD solicito dictamen a la Asesoría Jurídica de esa Agencia Vasca de Protección de Datos con la finalidad de que se nos de traslado de cuál es su criterio en el dicho supuesto."

SEGUNDO. El artículo 17.1 n) de la Ley 2/2004 de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos establece que es Función de seta Institución:

"n) Atender a la s consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley."

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa más arriba citada, la emisión del informe en respuesta a la consulta formulada.

CONSIDERACIONES

I

La cuestión formulada por el Ayuntamiento de XXXXX exige analizar las implicaciones que para la el derecho fundamental a la protección de datos se derivan de la utilización por parte de las Administraciones públicas, de nuevos servicios que ofrece la Sociedad de la Información, servicios como las redes sociales o la computación en la nube. Se trata de una consulta de tal magnitud que excede con mucho de las posibilidades de un dictamen al uso, tratándose más bien de una cuestión propia de un extenso análisis doctrinal.

Ha de tenerse en cuenta que en el ámbito de la Administración Pública, la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, está aún en fase de implantación en la mayor parte de las

Administraciones; sin embargo, la velocidad con que las nuevas tecnologías modifican la vida cotidiana hace que surjan cuestiones como la planteada por el Instituto Municipal de Deportes de Ermua, nuevas cuestiones a las que dar respuesta, sin que se hayan aún consolidado anteriores soluciones jurídicas a retos tecnológicos, como la Ley de acceso electrónico mencionada.

En resumen, se solicita a la Agencia que determine cuáles son las medidas a adoptar para solucionar o evitar los problemas que para el derecho fundamental a la protección de datos de carácter personal supone la implantación de la Administración 2.0

Una dificultad añadida estriba además en que, tal y como señala la doctrina (Ricard Martínez en su obra "protección de datos personales y redes sociales: un cambio de paradigma"), gran parte de los servicios vinculados a la web 2.0 *"se orientan al ocio y a fomentar aspectos directamente relacionados con la vida personal o privada como compartir fotografías, escuchar música o compartir vídeo o expresar opinión mediante breves píldoras de 140 caracteres."* Esta finalidad lúdica o doméstica, muy mayoritaria en la web 2.0 se aparta en gran medida del quehacer diario de una Administración Pública, y su adaptación a la vida administrativa origina algunas dificultades.

Entre los recursos jurídicos existentes para dar una respuesta cabal a la cuestión planteada podemos citar el Dictamen del Grupo del Artículo 29, (órgano consultivo de la Comisión Europea en materia de protección de datos) nº 5/2009 sobre las redes sociales en línea o el Dictamen del Supervisor Europeo de Protección de datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad, de 18 de marzo de 2010. Trataremos de ahondar en los problemas jurídicos y las posibilidades de respuesta existentes.

II

Expuesto el problema general, es necesario ahora ahondar en las implicaciones que la web 2.0 genera al derecho fundamental a la protección de datos. En primer lugar hay que señalar que los servicios de la web 2.0 se nutren de datos de carácter personal, siendo el papel activo de los usuarios en este caso el elemento diferenciador con respecto a la web 1.0 basada en páginas estáticas, meramente informativas, en las que no existía participación. La Web 2.0, web social o colaborativa facilita la creación de redes, plataformas, grupos, en base a criterios comunes creando un espacio virtual retroalimentado, espacio en el que no sólo se consume, sino que también se aporta información.

Como consideración general, si tenemos en cuenta que no se abona ninguna contraprestación económica por estos servicios, es fácil deducir que la moneda de cambio que aporta el usuario es su información personal, pudiendo verse su derecho a la protección de datos de carácter personal claramente afectado; pensemos en tratamientos lesivos tales como etiquetado de fotografías, difusión de imágenes sin

consentimiento, publicación de información personal sensible sin cumplir los requisitos legales, etc.

Si bien pueden verse también afectados otros derechos, como el de propiedad intelectual, el derecho al honor etc., vamos a centrar nuestro análisis en el derecho a la protección de datos de carácter personal.

Las conductas que hemos citado con anterioridad, etiquetado, difusión de datos personales, imágenes, etc. responden al concepto de tratamiento de datos. El tratamiento se define en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en su artículo 3 c) como

> *"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."*

Una referencia importante de cara a la aplicación a las redes sociales de la normativa en materia de protección de datos, fue la denominada Sentencia Lindqvist, Sentencia del Tribunal de Justicia de las Comunidades Europeas de 6 de noviembre de 2003. En esta Sentencia se analizaba el célebre caso de una catequista sueca que en la página web que había creado para ayudar a los feligreses de su parroquia incluyó información sobre una de sus compañeras, concretamente, información de que estaba en situación de baja por enfermedad. Denunciada esta conducta, será el alto tribunal europeo quien considere incluido en el concepto de tratamiento el colgar información de carácter personal en una página web.

Así, los usuarios de los servicios de la web 2.0, al editar contenidos en la red se convierten asimismo en responsables de tratamiento de los datos, salvo que sea de aplicación la excepción relativa a actividades domésticas, excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46. También tienen la consideración de responsables de tratamiento los proveedores de los servicios, salvo que, como decimos, resulte de aplicación la excepción doméstica. El artículo 3.2 de la Directiva dice lo siguiente:

> *"Las Disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:*
>
> *Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas."*

La excepción doméstica se interpreta en la sentencia Lindqvist cuando señala:

> *"En consecuencia, esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es ése el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas."*

Efectivamente, en el caso de utilización corporativa de servicios de la web 2.0 los destinatarios de la información son indeterminados, y por tanto, no sería de

aplicación la exención doméstica prevista en la Directiva, siendo plenamente aplicable la normativa de protección de datos.

Una vez expuesta la aplicabilidad de la normativa reguladora del derecho fundamental, debemos recordar lo señalado por el Supervisor Europeo de Protección de Datos en su Dictamen de 18 de marzo de 2010:

> *"Los usuarios deberían saber y entender que al procesar su información personal y la de otros están sujetos a la legislación de la UE sobre protección de datos, que exige, entre otras cosas, que se obtenga el consentimiento informado de aquéllos cuya información se introduzca y que se conceda a los afectados el derecho de rectificación, objeción, etc. Del mismo modo, los servicios de redes sociales deben, entre otras cosas, aplicar medidas técnicas y de organización adecuadas para evitar tratamientos no autorizados, teniendo en cuenta los riesgos que entraña el tratamiento y el carácter de los datos. Esto, a su vez, significa que los servicios de redes sociales deben garantizar parámetros por defecto que faciliten la intimidad, incluidos parámetros que sólo permitan acceder a los contactos seleccionados por el propio usuario. Los parámetros deberían también exigir el consentimiento expreso del usuario antes de que ningún perfil sea accesible a otras terceras partes, y los motores de búsqueda no deberían tener acceso a los perfiles de acceso restringido."*
>
> *"Lamentablemente, no todas las exigencias jurídicas están cubiertas. Aunque desde la perspectiva jurídica los usuarios de Internet se consideran responsables del tratamiento y están sujetos a lo dispuesto en el marco jurídico comunitario sobre protección de datos y privacidad, en realidad no suelen ser conscientes de esta función. En general, difícilmente saben que están tratando datos personales y que la publicación de esa información entraña riesgos en materia de privacidad y protección de datos. En particular cuando los jóvenes publican contenidos en idónea subestiman las consecuencias que pueden tener en ellos mismos y en otros, por ejemplo, en el contexto de su posterior matriculación en centros educativos o en sus solicitudes de trabajo."*

De los servicios mencionados en la consulta, tres son redes sociales (Facebook, Twitter y Tuenti), los problemas más importantes que estos servicios generan al derecho fundamental son la publicación excesiva de información personal, bien sea información propia o de terceras personas, la indexación del perfil del usuario por los buscadores de Internet, la recepción de publicidad hipercontextualizada, suplantaciones de identidad, recepción de spam, conservación de datos de tráfico, la recogida de datos sin aportar información etc.

En el denominado *"estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*" publicado por INTECO (Instituto Nacional de Tecnologías de la Comunicación) y la Agencia Española de Protección de Datos, se recogen una serie de medidas o acciones a emplear para proteger los datos personales de los usuarios:

"A nivel técnico, cabe señalar las siguientes acciones:

Eliminar los datos obsoletos que pudieran existir en distintos servidores, así como el cifrado de aquellos que estén en uso, minimizando así los daños que pudieran resultar de un ataque desde el exterior por parte de usuarios malintencionados

Establecer mecanismos de análisis respecto de la fortaleza de la contraseña de manera que se obligue al usuario a seleccionar una que no sea fácilmente descifrable por terceros.

Disociar los datos incluidos dentro de un perfil de usuario para que en el caso de acceso por terceros no autorizados estos no puedan acceder a los datos de los usuarios y emplearlos con fines malintencionados.

Crear categorías de perfiles para controlar el volumen de datos personales que el usuario permite que resulten visibles al resto de usuarios.

La creación de categorías de autorizaciones por ellos mismos sobre quién puede visionar sus perfiles. En este sentido cabe destacar los siguientes elementos:

Limitar el grado de publicidad del perfil del usuario conforme a los criterios anteriormente expuestos.

La posibilidad de limitar y regular el alcance de publicidad de un perfil permite al usuario modular el grado de exposición de las informaciones y datos personales que incorpora en la plataforma respecto al resto de usuarios. Esta medida otorga al usuario un control real sobre las informaciones que incorpora en la plataforma.

Limitar la indexación de los perfiles por parte de los principales buscadores de Internet.

Con esta medida se protege a los usuarios de una determinada plataforma de las búsquedas indiscriminadas que en ocasiones se realizan a través de los motores de búsqueda y que en un momento dado puedan proporcionar a la persona que realiza la búsqueda, información personal del usuario de la red social.

Limitar la visualización del perfil de manera geográfica.

Limitar la cantidad de datos que los usuarios pueden introducir: así por ejemplo ciertas plataformas deciden operar con perfiles de nickname o seudónimo para que sean los propios usuarios los que consideren a quien mostrarse (por ejemplo vi.vu).

En el caso concreto de Facebook, existen diferentes opciones dependiendo de si el usuario actúe por sí mismo o a una empresa o a una institución, pudiendo crearse un perfil, una página o un grupo según cuáles sean los objetivos de la red social.

En la Guía de usos y estilo en las redes sociales de la Generalidad de Cataluña se establece que *"la página es la solución corporativa que han escogido los diferentes departamentos de la Generalidad. De hecho, es la opción más adecuada para las instituciones y para los órganos que las constituyen, ya que Facebook atribuye un*

carácter diferencial a las organizaciones de todo tipo para distinguirlas de los perfiles personales….Las páginas tienen una serie de características que las hacen muy interesantes a la hora de monitorizar lo que sucede en la Red. Disponen de estadísticas completas de los usuarios que se asocian, con información sobre su edad, sexo, idioma, país, etc."

Siguiendo con el mismo documento y por si pudiera ser de utilidad se incluye parte del apartado "gestión de comentarios":

> *"El administrador gestiona quién puede escribir en el muro de la página: sólo él, sólo los admiradores o todos. Se recomienda que sólo el administrador pueda escribir en el muro. Para ello, en el apartado de Configuración que se encuentra justo debajo de la caja de escritura del muro, hay que desmarcar la opción Los admiradores pueden escribir o publicar contenido en el muro y seleccionar que la Vista por defecto del muro sea Sólo escritos por página. Además, escogeremos Nuestra página de entre las opciones que se encuentran encima del muro, de manera que sólo se puedan ver los mensajes escritos por los administradores de la página."*

Son muchos los apartados del citado documento que pueden resultar de interés para la consultante, por lo que dejamos anotado el vínculo con la página web correspondiente a fin de facilitar su consulta:

http://www.gencat.cat/web/meugencat/documents/20100607_GUIA_USOS_XARXA_CAS.pdf

También la recientísima "guía de usos y estilo en las Redes Sociales del Gobierno Vasco", presentada el día 27 de mayo de 2011, incide en la idea de la página de Facebook como mejor solución corporativa; así, señala que *"la página es la solución corporativa idónea para los diferentes departamentos, servicios o marcas del Gobierno. De hecho, es la opción adecuada para las instituciones y para los órganos que las constituyen, ya que Facebook atribuye un carácter diferencial a las organizaciones de todo tipo para distinguirlas de los perfiles personales."* La guía completa está disponible en la siguiente dirección de Internet:
http://www.irekia.euskadi.net/eu/site/snetworking

III

En cuanto al resto de servicios, Youtube, Flicr y Picasa, el primero es una plataforma para que los usuarios publiquen, vean y compartan videos, lo mismo que los dos últimos, sólo que en este caso el objeto son imágenes, fotografías. En estos supuestos, así como en las redes sociales antes citadas, no cabe sino insistir en la necesidad de cumplir con los principios de calidad, consentimiento y en el deber de informar en los supuestos de recogida de datos.

El principio de calidad se regula en el artículo 4 de la LOPD que en su apartado 1 señala

> *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

Este principio también exige que los datos no sean utilizados para finalidades distintas de aquellas que motivaron la recogida y que los datos registrados sean exactos y puestos al día.

El principio de información se regula en el artículo 5 de la LOPD, mereciendo destacarse el apartado 1 de dicho artículo:

> *"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
>
> *De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
>
> *Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
>
> *De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
>
> *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
>
> *De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*
>
> *Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento."*

Por último, profundamente ligado al principio de información se encuentra el principio del consentimiento regulado en el artículo 6.1 de la LOPD cuando establece

> *"El tratamiento de datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa."*

Este es el bloque fundamental de legalidad en materia de protección de datos que debe ser observado por la Administración al tratar datos personales. Piénsese además que en los supuestos en que se traten datos de colectivos más vulnerables, jóvenes y menores, que por otro lado son los que con más asiduidad utilizan los servicios de la web 2.0 deben extremarse las cautelas. En relación con estos colectivos, debe recordarse que en el caso de los menores de catorce años necesitan consentimiento de los padres o tutores, según el artículo 13.1 del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Tal y como ha señalado la mejor doctrina, sin poner en duda en ningún momento las ventajas que suponen estas tecnologías, teniendo en cuenta que los datos personales son el soporte de estos servicios el usuario debe ser consciente en todo

momento de las reglas por las que éstos se rigen y de la necesidad de mantener el control tanto sobre los propios datos, como sobre los de otras personas.

Por todas las consideraciones anteriores, por el Director de la Agencia Vasca de Protección de Datos se establecen las siguientes

CONCLUSIONES

La utilización por parte de las Administraciones Públicas de los servicios de la web 2.0 suponen unos tratamientos de datos de carácter personal, por lo que deberá cumplirse la normativa en materia de protección de datos, respetándose los principios contenidos en la LOPD, siendo fundamental la observancia de los principios de calidad, información y consentimiento del interesado.

En Vitoria-Gasteiz, a 14 de julio de 2011