



CIUDADANÍA Y VALORES  
FUNDACIÓN

# **EL DERECHO A LA PROTECCIÓN DE DATOS: NOVEDADES Y PROBLEMAS**

CURSO DE VERANO: ORGANISMOS INTERNACIONALES Y NUEVO  
ORDEN MUNDIAL

ARANJUEZ 2010

*Pablo Lucas Murillo de la Cueva  
Magistrado del Tribunal Supremo  
Catedrático de Derecho Constitucional*

## EL DERECHO A LA PROTECCIÓN DE DATOS: NOVEDADES Y PROBLEMAS

*SUMARIO:* 1. Algunas novedades significativas. 2. La libertad de información y la protección de datos personales. 3. La responsabilidad de los proveedores de servicios de *Internet*. 4. La conservación de los datos asociados a las comunicaciones y el acceso a ellos. La sentencia del Tribunal Constitucional Federal de 2 de marzo de 2010. 5. Referencias al régimen común de protección de los datos personales y a las redes sociales.

### *1. Algunas novedades significativas*

En los últimos meses se han producido algunas novedades significativas en torno al derecho a la protección de datos personales. Son acontecimientos de distinta naturaleza que se han producido en España y en otros países europeos y, como veremos, alguno de esos hechos tiene relevancia universal. Todos ellos tienen un rasgo común: contribuyen a poner de manifiesto la importancia de este derecho fundamental al mismo tiempo que sacan a la luz las grandes dificultades a las que se enfrenta.

Digo que son de diferente naturaleza porque consisten, por un lado, en sentencias dictadas por diversos órganos judiciales que han provocado vivas polémicas en torno a diversos aspectos relacionados con este derecho fundamental que merece la pena analizar. Una de ellas es la que *condenó a dos periodistas de la Cadena SER* por incluir en una información los nombres y apellidos de un grupo de afiliados a un partido político, sentencia posteriormente revocada por la Audiencia Provincial de Madrid. Otra dictada, en Alemania ha abordado el *régimen de conservación de los datos asociados a las telecomunicaciones*. En efecto, el Tribunal Constitucional Federal ha declarado nulos por violación del secreto de las comunicaciones los preceptos legales que traspusieron la Directiva sobre conservación de datos asociados a las mismas. Asimismo, ha alcanzado gran notoriedad *la condena que el Tribunal de Milán ha impuesto a tres directivos de Google* tras la inclusión de un video que muestra abusos y maltratos a un menor afectado por el síndrome de Down.

Por otro lado, no se debe pasar por alto que está abierto un *debate sobre las redes sociales y, en particular, sobre la protección de los menores* que participan en ellas masivamente. Y, en relación con las dificultades que trae consigo la naturaleza de la red de redes y, en general, con las dificultades que crea el carácter global de *Internet* frente a la dimensión territorial de los ordenamientos estatales, debe destacarse que, en noviembre de 2009, la IX Conferencia Internacional de Autoridades de Protección de Datos y de la Privacidad, reunida en Madrid los días 3, 4 y 5, aprobó los *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*.

Merece, pues, la pena hacer algunas consideraciones sobre estos acontecimientos.

## 2. La libertad de información y la protección de datos personales

De los tres casos judiciales a los que me he referido, comenzaré por el que ha tenido lugar en España que, como veremos, tiene algunos puntos en común con el que se ha dado en Italia.

En efecto, la *sentencia del Juzgado de lo Penal nº 16 de los de Madrid, de 18 de diciembre de 2009 condenó a dos periodistas de la Cadena SER a un año y nueve meses de prisión y a seis meses de multa más las accesorias correspondientes, por considerarlos autores del delito de revelación de secretos del artículo 197.2, 3 y 5 del Código Penal<sup>1</sup>, con la atenuante de obrar en ejercicio de un derecho, el de informar. Los hechos considerados probados consisten en que, en cuanto director y subdirector de la cadena de radio *Cadena SER*, cedieron a la sociedad *SER.com* los nombres y apellidos, domicilio y afiliación al Partido Popular de 78 vecinos del municipio de Villaviciosa de Odón. Datos obtenidos de personas que no quisieron identificar en virtud de su derecho al secreto profesional. La citada relación era de uso exclusivo del partido y los afectados no consintieron el uso que les dieron los condenados.*

La sentencia se extiende sobre el contenido del derecho fundamental a la protección de datos personales y cita la sentencia del Tribunal Europeo de Derechos Humanos de 6 de junio de 2006 (*caso Segerstedt-Wiberg y otros contra Suecia*) según la cual el almacenamiento de información sobre la afiliación y las actividades políticas constituye una interferencia en el derecho a la vida privada. Seguidamente, subsume en el artículo 197 del Código Penal los hechos antes mencionados y concluye que unos profesionales de la información experimentados como los condenados, no pueden desconocer que hay datos personales a los que, por su naturaleza, no tienen derecho a acceder ni a publicar o ceder para su publicación. Y, si bien, constata que no se propusieron perjudicar a los afectados, terminaron aceptando ese resultado.

En cuanto a la invocación de la libertad de información efectuada por los acusados, la sentencia dice que la protección que le asegura el artículo 20 de la

---

<sup>1</sup> El artículo 197 del Código Penal dice en los apartados aplicados por la sentencia: “1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado (...). 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior (...). 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior”.

Constitución ha de matizarse cuando, en vez de a través de medios de comunicación social, como la televisión, la radio o la prensa escrita, se realiza por *Internet* que --dice-- “no es un medio de comunicación social en sentido estricto, sino universal”.

A partir de aquí, acoge la tesis del Ministerio Fiscal para el que debía apreciarse la exigente incompleta de obrar en el ejercicio de un derecho y señala que las posibles irregularidades en la afiliación al partido y su relación con la corrupción urbanística, siendo ciertamente hechos noticiables, aportan un principio de justificación. Ahora bien, precisa la sentencia, no es plena porque para ello hubiera sido necesario que la publicación de la identidad de las personas afectadas hubiera sido imprescindible para informar a la opinión pública. Y esta necesidad no se daba.

Vemos que aquí entran en conflicto la libertad de información y el derecho a la protección de datos personales, en este caso, en relación con los derechos a la libertad ideológica y a la intimidad de los afectados. Sabemos que esta colisión puede darse pues entra en la lógica de las relaciones que surgen del ejercicio de los derechos que el ordenamiento jurídico reconoce. Por lo demás, ya la propia Directiva 95/46 dedica su artículo 9 a esta cuestión y dice:

“En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión”.

Y la sentencia del Tribunal de Justicia de las Comunidades Europeas de 6 de noviembre de 2003 (*caso Bodil Lindqvist*) abordó el problema.

En esa ocasión lo sucedido fue según la propia sentencia lo siguiente:

“12. Además de su trabajo retribuido como empleada de mantenimiento, la Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en *Internet*. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran. A petición suya, el administrador del sitio *Internet* de la Iglesia de Suecia creó un enlace entre las citadas páginas y dicho sitio.

13. Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, sólo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad.

14. La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion (organismo público para la protección de los datos transmitidos por vía informática). En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió.

15. El ministerio fiscal inició un proceso penal contra la Sra. Lindqvist por infracción de la PUL y solicitó que se le condenara por:

- haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datainspektion (artículo 36 de la PUL);
- haber tratado sin autorización datos personales delicados, como los relativos a la lesión en un pie y a la baja parcial por enfermedad (artículo 13 de la PUL);
- haber transferido datos de carácter personal a países terceros sin autorización (artículo 33 de la PUL).

16. La Sra. Lindqvist reconoció los hechos, pero negó que hubiera cometido una infracción. El Eksjötingsrätt (Suecia) la condenó al pago de una multa; la Sra. Lindqvist recurrió en apelación esta resolución ante el órgano jurisdiccional remitente.

17. El importe de la multa ascendía a 4.000 SEK, tras haber aplicado a la suma de 100 SEK, que se calculó teniendo en cuenta la situación financiera de la Sra. Lindqvist, un multiplicador de 40 que representaba la gravedad de la infracción. Asimismo se condenó a la Sra. Lindqvist a abonar 300 SEK a un fondo sueco que tiene por objeto ayudar a las víctimas de las infracciones”.

Pues bien, la sentencia estableció la necesidad de ponderar, de un lado, la libertad de expresión de la Sra. Lindqvist en el marco de su trabajo como catequista y su libertad de ejercer actividades que contribuyen a la vida religiosa y, de otro lado, la tutela de la intimidad de las personas cuyos datos incluyó la Sra. Lindqvist en su sitio *Internet*. Y que corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros “no sólo interpretar su Derecho nacional de conformidad con la Directiva 95/46, sino también procurar que la interpretación de ésta que tomen como base no entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico comunitario o con los otros principios generales del Derecho comunitario como el principio de proporcionalidad”. Proporcionalidad sobre la que insiste a propósito de las sanciones que se impongan a quienes infrinjan las normas sobre protección de datos personales.

Desde estas premisas respondió a la cuestión prejudicial diciendo:

“1) 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/CE (...).

2) Un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el artículo 3, apartado 2, de la Directiva 95/46.

3) La indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva 95/46.

4) No existe una “transferencia a un país tercero de datos” en el sentido del artículo 25 e la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio *Internet* en el que se puede consultar la página web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a *Internet*, incluidas aquellas que se encuentren en países terceros.

5) Las disposiciones de la Directiva 95/46 no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (...). Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario.

6) Las medidas adoptadas por los Estados miembros para garantizar la protección de los datos personales deben atenerse tanto a las disposiciones de la Directiva 95/46 como a su objetivo, que consiste en mantener el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad. En cambio, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a lo dispuesto en la Directiva 95/46 a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello”.

Volviendo con estas referencias al caso afrontado por el Juzgado de lo Penal nº 16 de Madrid, parece claro que los problemas que plantea su sentencia no son los relacionados con si estamos o no ante un tratamiento de datos personales, ni tampoco si el derecho fundamental que los protege merece la tutela penal frente a las agresiones más graves de las que sea objeto, sino si, en este caso, mediaba una causa de justificación plena y, de no ser así, si es proporcionada la condena.

Que estamos dentro del ámbito del derecho fundamental a la protección de datos es indudable y también lo es que la garantía penal forma parte de su contenido. Por otro lado, es igualmente evidente que los condenados ejercían su función profesional de

informar verazmente --este extremo no se discute-- de un hecho noticiable, tal como reconoce la sentencia. El conflicto entre la libertad de información y este derecho fundamental lo ha resuelto la sentencia a favor del último, visto que el propio artículo 20 de la Constitución erige el derecho a la intimidad personal en límite a esa libertad y que, para el juzgador, no era preciso para ejercerla en este caso facilitar los nombres de las personas afiliadas al partido político señalado. De la lectura de los fundamentos de la misma se desprende que no aprecia la eximente plena de obrar en ejercicio legítimo de un derecho, precisamente, porque la información controvertida no era necesaria, cosa que debían saber dos periodistas expertos. No parece, en cambio, que haya influido en este punto el hecho de que no se acepte que *Internet* sea un medio de comunicación social, extremo en el que no se puede coincidir con la sentencia.

Así, las cosas, me parece que, efectivamente, se vio afectado el derecho a la protección de los datos personales de los ciudadanos mencionados en la información. Afectación que se produjo, además, en los que merecen ser especialmente protegidos, como son los relativos a la afiliación política, según el artículo 7 de la Ley Orgánica 15/1999. Esa injerencia tuvo lugar desde el momento en que se difundió a través de una página *web* una información personal de carácter sensible, sin autorización de los afectados. Y puede coincidir con la sentencia en que no era imprescindible divulgar su identidad para informar verazmente de los hechos. No estoy seguro, en cambio, de que la respuesta penal sea proporcionada a la gravedad de los hechos. No deja de ser significativo que en el caso *Linqvist* se impuso una multa.

El pasado 10 de junio de 2010 la Sección Sexta de la Audiencia Provincial de Madrid ha dictado sentencia acogiendo el recurso de apelación de los dos periodistas condenados y absolviéndolos del delito por el que fueron condenados. A juicio de este tribunal, la conducta enjuiciada no es subsumible en el tipo de revelación de secretos aplicado por el Juzgado y, al no ser típica, no procede imponerles ninguna sanción penal. Asimismo, por esa razón considera que no es necesario hacer ninguna otra consideración al respecto. La falta de tipicidad la aprecia porque el artículo 197 del Código Penal castiga en sus apartados 3 y 5 la revelación de datos registrados en ficheros, archivos o registros. Y, dice la sentencia:

“Sentado lo anterior tras la lectura del apartado de hechos de la sentencia recurrida (...) debe afirmarse que en la descripción de hechos probados no se hace expresión alguna a que los datos cedidos por los acusados estuvieran registrados en ningún tipo de fichero, archivo o registro. Por lo que no cabe la subsunción de los hechos en el tipo delictivo por el que se condena en la sentencia recurrida (...). Debe señalarse que el que los datos fueran del uso exclusivo del Partido Popular (...) no implica que necesariamente (...) estuvieran registrados en ningún fichero o archivo, pues tal uso exclusivo es compatible con que los datos estuvieran simplemente anotados en un documento cuyo manejo estuviera reservado o limitado a los miembros de dicho partido. Por otra parte, la referencia que se hace el apartado de hechos probados de la sentencia recurrida a que los datos aparecían en una lista de afiliados, y en lo que parece que se funda el Ministerio Fiscal en su escrito de impugnación del recurso formulado por los acusados, en el que se equipara el listado de datos con un archivo, público o privado, no puede compartirse por este Tribunal, ya que *archivo* significa según el significado gramatical que se da al término en el Diccionario la Lengua Española, publicado por la Real Academia de la Lengua,

en las acepciones que ahora interesan al exigirse en el artículo 197.2 del Código Penal que los datos estén registrados en el archivo, al conjunto ordenado de documentos que una persona, una sociedad, una institución, etc., producen en el ejercicio de sus funciones o actividades o al lugar donde se custodian uno o varios archivos, o espacio que se reserva en el dispositivo de memoria de un computador para almacenar porciones de información que tienen la misma estructura o que pueden manejarse mediante una instrucción única, o conjunto de información almacenada de esa manera, siendo por ello un término cuyo significado excede en mucho del que tiene el término listado o lista que, también, según el significado de dicho término en el Diccionario antes indicado, equivale a numeración, generalmente en forma de columna, de personas, cosas, cantidades, etc., que se hace con determinado propósito.

Debe destacarse también que la acusación particular (...) afirma que había resultado acreditado que los datos cedidos estaban contenidos en los archivos del Partido Popular, pero se omite por dicha parte la expresión de qué pruebas en concreto hubieran acreditado ese extremo. En todo caso, la hipotética existencia de pruebas de que los datos hubieran estado registrados en los archivos del citado partido nada opondría a que los concretos hechos que se declaran probados en la sentencia recurrida no fueran subsumibles en el delito de revelación de secretos por falta de tipicidad penal”.

Si parece claro que el castigo impuesto por el Juzgado era desproporcionado a la entidad de los hechos, la fundamentación de la sentencia dictada en apelación --no susceptible de recurso ulterior-- no deja de producir dudas. En particular, la de si la interpretación del término archivo que hace es la más coherente con los principios de la Ley Orgánica de Protección de Datos Personales. Seguramente, el rigor de las penas previstas e impuestas, junto con la observancia del criterio restrictivo que ha de tenerse presente en materia sancionadora, están en la base de la solución alcanzada por la sentencia de apelación. No obstante, de confirmarse la interpretación sentada por la Audiencia Provincial de Madrid, será cuestión de plantearse si debe mantenerse en el Código Penal el castigo de hechos como los enjuiciados en estas sentencias y, en caso de respuesta afirmativa, será necesario afrontar la modificación del artículo 197 del Código Penal.

### *3. La responsabilidad de los proveedores de servicios de Internet*

Otra sentencia reciente, bien llamativa, es la dictada por la Sección Cuarta Penal del Tribunal de Milán el 12 de abril de 2010 condenando a tres directivos de *Google* por violar el derecho a la intimidad de un menor afectado por el síndrome de Down mediante la difusión de un video que muestra el trato vejatorio que le infligen. Veamos los hechos y los pronunciamientos de la sentencia.

El video en cuestión --de unos tres minutos y medio-- mostraba al menor cuando era insultado y golpeado por cuatro estudiantes de un instituto técnico de Turín, ante la indiferencia del resto de la clase. Se cargó en *Google* el 8 de septiembre de 2006, en la sección de los catalogados como más divertidos y fue retirado el 7 de noviembre. Entre tanto recibió 5.500 visitas.

Los directivos de *Google* --David Carl Drummond, ex presidente del Consejo de Administración de *Google Italy* y ahora vicepresidente *senior*, George de los Reyes, antiguo miembro del Consejo de Administración de *Google Italy*, actualmente jubilado, y Peter Fleischer, responsable de estrategias para la privacidad para Europa de *Google Inc.*-- fueron *condenados a seis meses de prisión por un delito contra la privacidad* -- quedando suspendida la pena-- porque su falta de diligencia llevó a la inclusión en *Google Video* de esas imágenes. Fueron absueltos, en cambio, del delito de difamación del que les acusaba el Ayuntamiento de Milán y la asociación *Vivi Down*<sup>2</sup>. Un cuarto directivo, Arvind Desikan, responsable de *Google Video* para Europa fue absuelto plenamente.

La familia del niño retiró su querrela contra los acusados. Fue el Ministerio Fiscal el que mantuvo la acusación con el propósito de hacer valer los derechos humanos por encima de la lógica de la empresa. Según informó la prensa, se trata del primer proceso penal en el que se imputó y condenó a responsables de *Google* por los contenidos de la *web*.

*Google* y la Embajada de los Estados Unidos en Italia han criticado la sentencia, que ha sido apelada, porque consideran que supone un ataque a los principios fundamentales de libertad sobre los que ha sido construido *Internet*. Los recursos de los condenados se basan, además, en que no tuvieron nada que ver con el video pues no lo distribuyeron, ni cargaron, ni vieron y en que, de prosperar el criterio de la sentencia de hacer responsables a los proveedores de servicios de los contenidos que cargan los usuarios, se hará imposible ofrecer servicios en *Internet*. Insisten en que actuaron correctamente y en que *Google* no tenía ninguna obligación de ejercer un control preventivo sobre los videos y mensajes que se cuelgan en la Red. Y subrayan que tan pronto como tuvieron noticia del contenido de video lo retiraron inmediatamente.

En contra de esta sentencia, se ha afirmado también que desconoce el valor de la libertad de expresión y que ejercerla en *Internet* es un derecho humano inalienable que debe ser protegido en las sociedades libres y que, si bien se debe prestar atención a los abusos, sin embargo, el eventual material ofensivo no debe convertirse en un pretexto para vulnerar este derecho fundamental.

Aquí vuelven a aparecer los problemas ya apuntados en relación con la sentencia de la *Cadena SER*, junto con otros de indudable alcance. Además, de cuanto se refiere a la proporcionalidad de las penas impuestas, aquí está en discusión la responsabilidad de los directivos de *Google*, no por haber introducido el video en su buscador, sino por no haber tomado las medidas necesarias que lo hubieran impedido. Parece que en estos casos hay que medir, no ya la participación en el establecimiento de los contenidos expuestos en la red, sino la diligencia o la falta de ella para evitar su introducción cuando incurran en ilicitud. Criterios estos que el legislador español ha tomando en consideración al referirse a la responsabilidad de los prestadores de servicios de la sociedad de la información en las cláusulas correspondientes de la Ley 34/2002.

En el proceso, *Google Italy* alegó que cuanto se pone a disposición de los usuarios a través de <http://video.google.it> es un material que obra en servidores americanos y que existe un equipo de personas en América que ve los videos emitidos,

<sup>2</sup> Asociación Italiana para la investigación científica y para la tutela de la Persona Down, con sede en Milán.

del mismo modo que se utiliza un *software* de valoración de contenidos y que, a petición de *Google Italy*, se retiró el video origen del proceso penal. También insistieron los responsables de *Google Italy* en que el servicio estaba enteramente elaborado en la casa madre, o sea *Google Inc.*, y en que no había habido beneficios para *Google Italy*. Sucede, sin embargo, que para la sentencia estas manifestaciones no eran veraces. Y, también, consideró limitado el control ejercido sobre los contenidos, que este descansaba principalmente en las denuncias y comentarios de los propios usuarios y dejó constancia de que hubo diversas denuncias del video sin que fuera retirado hasta varias semanas más tarde. Estas comprobaciones y otras --a partir de declaraciones de empleados de la empresa-- llevaron al juzgador a concluir que entre los objetivos de *Google* no figura la pronta remoción de contenidos, dada la insuficiencia de los controles que practica. En este sentido, dice que, ya en 2004, los asesores jurídicos de *Google UK* recomendaron la revisión de los procedimientos en materia de *privacy* de *Google Italy*.

En cuanto a la naturaleza de las sociedades implicadas explica la sentencia que “la ramificación europea de *Google* parece inspirada en el principio de las cajas chinas, todas distintas aparentemente pero, en realidad, necesariamente enlazadas entre sí desde el momento en que la actividad de *marketing* en el territorio de cada Estado de la Unión Europea resulta esencial para la difusión de un servicio y, por tanto, fundamental en una óptica de realización de beneficios económicos”. Señala, después, la manera de obtenerlos a través de la publicidad y comprueba el papel activo de *Google Italy* en el servicio de *Google Video* y las posibilidades de control que tenía a su disposición respecto de la carga del video.

Sobre la propia competencia del Tribunal que enjuicia el caso, la sentencia afirma que también Milán puede ser considerado el lugar de comisión del delito desde el punto de vista del tratamiento de los datos y que *Google Italy, S.R.L.* tiene su sede en esta ciudad. Y, tras constatar que trató datos sensibles del menor sin el debido consentimiento, dice lo siguiente:

“En este sentido el IP (es decir el proveedor de *Internet*) que suministre a los usuarios un simple servicio de interconexión y que avise correctamente a los mismos de las obligaciones legales concernientes a la *privacy* no puede ser considerado punible si no controla previamente el cumplimiento por parte del usuario de tales obligaciones.

*Ad impossibilia nemo tenetur* y, por tanto no cabe imponer a nadie una obligación a la que no puede hacer frente con los medios normales a su disposición: sería del todo imposible pretender que un IP pueda verificar que en todos los millares de videos que se cargan en cada momento en su sitio web se hayan respetado las obligaciones concernientes a la *privacy* de todos los sujetos reproducidos en ellos. Es, sin embargo, necesario (y es, por tanto, legítimo reclamar el respeto de tal comportamiento) que el IP provea a los usuarios mismos de todas las advertencias necesarias en orden al respeto de las normas citadas, con particular atención a las que conciernen a la necesidad de procurarse el obligatorio consentimiento en orden a la difusión de datos personales sensibles. Existe, pues, a juicio de quien escribe, una obligación NO de control preventivo de los datos introducidos en el sistema sino de una correcta y puntual

información por parte de quien acepte y se haga con datos procedentes de terceros hacia estos últimos.

(...) Sobre la base de tal interpretación debería, pues, ser considerado responsable del delito (...) aquél tipo de IP que (como en el caso en examen) no se limite a suministrar una simple relación de interconexión, sino que, gestionando los datos en su posesión, se convierta, de algún modo en “dominus” y, por tanto, titular del tratamiento en el sentido legalmente establecido y con las obligaciones correspondientes”.

Y concluye de este modo: 1º) *Google Italy* era la “mano operativa y comercial” de *Google Inc.* en Italia. 2º) A través del sistema *AD Words* y del reconocimiento de palabras clave *Google Italy* tenía con toda seguridad la posibilidad de gestionar y organizar los datos contenidos en *Google Video*. 3º) *Google Italy* trataba los datos de esos videos y, en consecuencia, era responsable a los efectos de la legislación sobre la *privacy* y sucede que la información que facilitaba al usuario a ese respecto estaba de tal modo “escondida” que era totalmente ineficaz. 4º) El beneficio perseguido estaba unido a la interacción comercial y operativa existente entre *Google Italy* y *Google Video* mediante el sistema *AD Words* y palabras clave. 5º) Todo esto prueba, para el juez, “una clara aceptación consciente del riesgo concreto de la inserción y divulgación de datos, también y, sobre todo, sensibles, que habrían debido ser objeto de particular tutela” y demuestra “el interés económico vinculado a esa aceptación del riesgo y la clara consciencia de este último”.

Dicho llanamente:

“no es lo escrito en el muro lo que constituye delito para su propietario, sino su aprovechamiento comercial en determinados casos y en presencia de determinadas circunstancias”.

Me parece interesante recoger también la glosa final que el juez se ha decidido a incluir en esta sentencia a la vista del gran impacto mediático que ha tenido el caso<sup>3</sup>:

“Habría que decir, parafraseando el título de una famosa comedia de Shakespeare, “*too much ado about nothing*” (mucho ruido para nada); es decir, no le parece, a este juez, haber alterado de manera significativa los parámetros valorativos y jurisdiccionales que presiden la decisión de los casos como el tratado (...). La condena del *webmaster* en orden al delito de tratamiento ilícito de datos personales, en efecto, no ha sido construida aquí sobre la base de una obligación preventiva de control sobre los datos introducidos, sino sobre la base de un perfil valorativo diferente que es, como se ha dicho, el de una insuficiente (y culpable) comunicación de las obligaciones legales de los *uploaders* por razón de lucro. El Decreto Legislativo sobre la *privacy* (...) cubre de modo completo (...) el comportamiento de quien se encuentre en situación de “manejar” datos sensibles y, por tanto, no puede ser ignorado en el momento en que se advierta la posibilidad de intervenir. La distinción entre *content provider* y *service provider* es sin duda significativa pero en el estado actual y a falta de una normativa específica sobre la materia no puede constituir el único parámetro

<sup>3</sup> Debemos tener presente que el fallo condenatorio se hizo público el 23 de febrero de 2010 y que la sentencia no se depositó en la secretaría hasta el 12 de abril siguiente.

de referencia para construir la responsabilidad penal de los *Internet providers*. Sin embargo, este proceso penal supone (...) una importante señal de aproximación a una zona de peligro en lo que concierne a la responsabilidad penal de los *webmasters*: no hay duda de que la tremenda velocidad del progreso técnico en la materia consentirá, antes o después, al gestor del sitio web “controlar” de manera cada vez más intensa y atenta la carga de datos y la existencia de filtros preventivos cada vez más refinados obligará a una mayor responsabilidad a quien se encuentre en la situación de operar con ellos. En tal caso, la construcción de la responsabilidad penal (sea culposa o dolosa) por la omisión del control será más fácil de lo que resulta ahora. En todo caso, este juez, como cualquier otro, permanece a la espera de una buena ley sobre la cuestión: *Internet* ha sido y continuará siendo un formidable instrumento de comunicación entre las personas y, donde hay libertad de comunicación hay en conjunto más libertad, entendida como vehículo de conocimiento y de cultura, de consciencia y de opción; pero todo ejercicio de un derecho ligado a la libertad no puede ser absoluto so pena de que degenera en arbitrio. Y no hay peor dictadura que la ejercida en nombre de la libertad absoluta: *legum servi essere debemus, ut liberi esse possumus* decían los antiguos y, a pesar del tiempo transcurrido, no se ha llegado todavía a encontrar una definición mejor”.

No me parece preciso insistir en las cuestiones de toda índole que suscita esta sentencia.

La relevancia que alcanzó cuando se hizo público el fallo es suficiente para poner de manifiesto su importancia. No obstante, sin perjuicio de los demás extremos que cabe resaltar de ella, junto a la proporcionalidad de las penas impuestas, entre los más significativos están los relativos a la discutida competencia del Tribunal de Milán para enjuiciar un caso en el que se plantea la comisión de un delito por tratamientos realizados en *Internet* y los criterios que llevaron a considerar autores del delito a los condenados. Y, obviamente, está el problema central de la responsabilidad de los proveedores de servicios cuando, más allá de facilitar enlaces o accesos a sitios determinados, suministran contenidos susceptibles de lesionar derechos y, en particular, derechos fundamentales. En este caso, hemos visto cómo, con unos razonamientos muy matizados, la sentencia hace descansar la atribución de responsabilidad penal en la comprobación de que la sociedad implicada antepuso el lícito fin de obtener ganancias y omitió la diligencia mínima que le era exigible frente a un riesgo que acabó materializándose, no haciendo ver a quienes le suministraron el video las obligaciones que la ley les impone para proteger la *privacy* de las personas afectadas.

Según sugiere el juez en sus consideraciones finales, ha sido la aplicación de reglas elementales del razonamiento jurídico la que han guiado su decisión que, por tanto, no contempla como especialmente innovadora. En todo caso, sea cual sea la suerte que corra al ser revisada en apelación, es lo cierto que ha planteado un vivo debate del que, sin duda, surgirán nuevas ideas y reflexiones que redundarán en avances en la salvaguardia del derecho a la autodeterminación informativa en el complejo mundo de *Internet* y de las redes de comunicaciones.

*4. La conservación de los datos asociados a las comunicaciones y el acceso a ellos. La sentencia del Tribunal Constitucional Federal de 2 de marzo de 2010*

En otro plano diferente se sitúa el tercer caso judicial que se trae a colación. Diferente porque, en vez de consistir en un proceso penal, se trata de juicio sobre normas: el que ha contrastado la conformidad con la Ley Fundamental de Bonn de los preceptos legales con los que se traspuso en Alemania la Directiva 2006/24/CE sobre conservación de datos asociados a las telecomunicaciones. Y porque, en lugar de afrontar únicamente actuaciones de sujetos privados, se adentra también en las de los poderes públicos. En efecto, el Tribunal Constitucional Federal de Alemania ha declarado en su sentencia de 2 de marzo de 2010<sup>4</sup> la nulidad de los § 100 g) del Código Procesal Penal y 113 a) y b) de la Ley Federal de Telecomunicaciones, introducidos por la Ley de 21 de diciembre de 2007. En particular, los ha encontrado, no sólo incompatibles con la Ley Fundamental de Bonn, por infringir su artículo 10.1 que protege el secreto de las comunicaciones y vulnerar el derecho a la autodeterminación informativa, sino radicalmente nulos.

Esos apartados del § 113 establecían el deber de los proveedores de servicios de telecomunicaciones accesibles públicamente de conservar todo el tráfico de datos de las comunicaciones por teléfono (fijo y móvil), fax, SMS, MMS, correo electrónico y de los servicios de *Internet*. El deber afectaba a toda la información necesaria para reconstruir quién realizaba o intentaba hacer la comunicación, cuándo, por cuánto tiempo, con quien y desde dónde, pero no del contenido de la misma. Esos datos debían conservarse durante seis meses, debiendo ser borrados en el mes sucesivo al vencimiento de ese plazo. Los fines que legitimaban ese deber los definía la Ley en términos generales, necesitados de concreción por ulteriores normas legales sectoriales, federales o de los *Länder*. Son el uso directo de los datos para la persecución de las infracciones criminales, la prevención de peligros sustanciales para la seguridad pública y el cumplimiento de las funciones de los servicios de inteligencia. Indirectamente, se autorizaba su uso al habilitar a las autoridades, al amparo del Código Procesal Penal, a requerir información relativa al usuario de una dirección de *Internet*<sup>5</sup> de la que ya dispusieran cuando fuera necesario para la persecución de infracciones criminales, faltas administrativas o la prevención de riesgos, todo ello sin autorización judicial ni notificación al afectado.

La cuestión sometida al Tribunal Constitucional Federal por los recurrentes<sup>6</sup> fue la de que dichos artículos eran contrarios al secreto de las comunicaciones y al derecho a la autodeterminación informativa. Insistían en la desproporción de la Ley y en que los datos almacenados podían ser usados para crear perfiles de personalidad y para rastrear los movimientos de las personas. Asimismo, alegaban que el coste del almacenamiento de esa información perjudicaba de manera también desproporcionada la libertad de

---

<sup>4</sup> Se puede consultar en [www.bundesverfassungsgericht.de](http://www.bundesverfassungsgericht.de) donde se ofrece el texto completo en alemán una versión en inglés que es la que he manejado. Véase un resumen de ese proceso constitucional en Mariano Daranas Peláez, “Sentencia del Tribunal Constitucional Federal (Sala Primera) de la República Federal de Alemania de 2 de marzo de 2010 sobre los tres recursos de inconstitucionalidad BvR 256/08, BvR 263/08 y BvR 568/708 contra los artículos 113a y 113b de la Ley de Telecomunicaciones (texto modificado de 2007) y 100g, apartado 1, inciso primero, de la Ley de Enjuiciamiento Criminal (texto modificado por la propia Ley de Telecomunicaciones)”, en *Asamblea. Revista Parlamentaria de la Asamblea de Madrid*, nº 22/2010, págs. 383 y sigs.

<sup>5</sup> Se trata del IP: *Internet Protocol* que identifica un Terminal determinado.

<sup>6</sup> Fueron tres los recursos interpuestos por diversos grupos de ciudadanos. Uno de ellos contó con la adhesión de miles de ciudadanos, más de 84.000. Entre ellos cuarenta diputados del Partido Liberal y la propia Ministra de Justicia Sabine Leutheusser-Schnarrenberger a iniciativa de un grupo de trabajo sobre la retención de datos *AK Vorrat*.

empresa de los proveedores de servicios de telecomunicaciones. Sus argumentos principales fueron estimados por la sentencia. Debe resaltarse, al respecto que la Sala Primera del Tribunal Constitucional se pronunció por unanimidad sobre la conformidad a la Constitución del deber de conservación de los datos para determinadas finalidades. No obstante, se dividió siete a uno y seis a dos a la hora de fallar sobre inconstitucionalidad de la definición de tales finalidades y la falta de transparencia y seguridad de los datos por violación del artículo 10.1 de la Ley Fundamental de Bonn, y cuatro a cuatro sobre la declaración de nulidad y no mera incompatibilidad con la Constitución de esos preceptos.

Veamos algunos de los razonamientos más relevantes del Tribunal Constitucional Federal de Alemania.

Dice la sentencia que el almacenamiento de los datos relativos al tráfico de telecomunicaciones durante seis meses para fines estrictamente limitados a la persecución de delitos, la prevención de riesgos y las funciones de los servicios de inteligencia no es en sí mismo incompatible con el artículo 10.1 de la Ley Fundamental si la ley que lo prevé tiene suficientemente en cuenta los derechos e intereses en conflicto e integra ese deber de conservación en una estructura legislativa adecuada e idónea para satisfacer las exigencias del principio de proporcionalidad.

Añade que dicho almacenamiento constituye una intromisión particularmente seria pues, aunque no se extienda al contenido de las comunicaciones, los datos a los que afecta pueden ser usados para extraer conclusiones sobre él y entrar en la esfera privada de los usuarios. En su conjunto, los receptores, las fechas, hora y lugar de las conversaciones telefónicas, si se observan a lo largo de un período prolongado de tiempo, ofrecen una detallada información sobre la afiliación social o política y sobre las preferencias personales, inclinaciones y debilidades. Dependiendo del uso de las telecomunicaciones, esa conservación puede llevar a la creación de perfiles personales de virtualmente todos los ciudadanos y reconstruir sus movimientos. También incrementa el peligro de que los ciudadanos se vean expuestos a ulteriores investigaciones sin que hayan dado motivo para ello y las posibilidades de abuso asociadas a tal recolección de datos agravan esa pesada carga. En particular, porque el almacenamiento y uso de los datos no se notifican, la conservación de los datos asociados al tráfico de telecomunicaciones es susceptible de crear una sensación amenazante de estar siendo observado que puede perjudicar el libre ejercicio de los derechos fundamentales en muchos ámbitos.

Para que esa conservación sea compatible con el artículo 10.1 de la Ley Fundamental, sigue la sentencia, deben darse determinadas condiciones. El primer factor relevante es que no se lleve a cabo directamente por el Estado sino mediante la imposición de un deber a los proveedores de servicios privados. Así, los datos quedan repartidos entre muchas empresas diferentes y no son accesibles en su conjunto por el Estado. Tampoco debe concebirse esa retención como una medida dirigida a la grabación de todas las comunicaciones de los ciudadanos. Debe, por el contrario, definirse de una manera limitada, partir de la especial significación de las telecomunicaciones en el mundo moderno y reaccionar frente a los potenciales peligros que trae consigo para la efectiva persecución de los delincuentes y la prevención de los posibles peligros. En definitiva, para que la conservación de estos datos sea constitucionalmente inobjetable debe ser una excepción a la regla pues forma parte de la

identidad constitucional de la República Federal de Alemania que el disfrute por los ciudadanos de su libertad no pueda ser totalmente grabado y registrado.

Establece, seguidamente, la sentencia las exigencias que desde los principios de proporcionalidad, transparencia y seguridad en la conservación y utilización de los datos debe cumplir el legislador y al contrastarlos con los preceptos impugnados concluye que estos no los satisfacen. En efecto, dice que no son inconstitucionales solamente por la desproporción del deber de conservación, sino también porque las normas sobre las finalidades y la transparencia en el uso de los datos y sobre las garantías no cumplen dichos requisitos. La regulación legal, dice, carece de una estructura que cumpla el principio de proporcionalidad. En efecto, falta la necesaria garantía de un elevado nivel de seguridad de los datos, pues la ley se refiere sólo al cuidado generalmente necesario en el campo de las telecomunicaciones y, de ese modo, califica las exigencias de seguridad de una manera indeterminada y las somete a consideraciones de adecuación económica. La concreción de esas medidas, prosigue, se deja a los proveedores de servicios los cuales deben prestarlos bajo la presión de las condiciones de competencia y de su coste y no se requiere a las personas sobre las que recae el deber de conservar los datos el uso de instrumentos aconsejados por los expertos para garantizar su seguridad ni se demanda un nivel definido de la misma. Tampoco cuenta la ley con un sistema equilibrado de sanciones que no atribuya menos peso a las violaciones de la seguridad de los datos que al incumplimiento de los deberes de conservación.

En cuanto al uso de los datos para fines de persecución criminal, dice la sentencia que los preceptos legales no son compatibles con el principio de proporcionalidad ya que no aseguran que, en general, y también en los casos concretos, solamente los delitos graves justifiquen la recuperación de los datos relevantes, pues consideran suficiente cualquier delito. La consecuencia, teniendo en cuenta la creciente importancia de las telecomunicaciones en la vida cotidiana es que el uso de los datos pierde su carácter excepcional, desconociendo, además, el límite impuesto a este respecto por la Directiva. Tampoco es constitucional la previsión del Código Procesal Penal que permite, en determinados supuestos que la recuperación de los datos conservados se produzca sin el conocimiento de la persona afectada. En cambio, no aprecia la sentencia problemas en lo relativo al control judicial del acceso a los datos objeto de retención, pero sí ve objetable que no se contemplara el seguimiento judicial del cumplimiento del deber de notificación al afectado.

Ve igualmente contrario a la Constitución la sentencia el precepto que autoriza la conservación de los datos para su utilización por los servicios de inteligencia en el cumplimiento de sus funciones: con el establecimiento del deber de los proveedores de servicios de retenerlos y, al mismo tiempo, con la autorización del acceso a ellos por la policía y los servicios de inteligencia en el ejercicio de sus funciones, la ley crea una fuente de datos abierta a múltiples e ilimitados usos solamente circunscritos por unos objetivos ampliamente definidos por el legislador estatal o territorial. De este modo, dice, el legislador ha removido la necesaria conexión que debe haber entre la conservación y la finalidad de la misma, lo que es incompatible con la Constitución. Además, subraya, la formulación del uso de los datos es también desproporcionada pues no protege las relaciones confidenciales.

La sentencia juzga inconstitucional, asimismo, la utilización de los datos almacenados para perseguir faltas administrativas.

En cambio, no aprecia la infracción que denunciaban los recurrentes del artículo 12 de la Ley Fundamental que protege la libertad de profesión y prohíbe el trabajo forzoso porque no ve en la imposición del deber de conservar los datos una carga excesiva para los proveedores de servicios afectados. Lo juzga, en efecto, proporcionado y dice que, del mismo modo que las empresas de telecomunicaciones pueden aprovechar las nuevas oportunidades de la tecnología para obtener beneficios, deben asumir igualmente los costes de afrontar los nuevos riesgos para la seguridad asociados a ellas y deben incluirlos en sus precios.

##### 5. Breves referencias al régimen común de protección de los datos personales y a las redes sociales

Entre las novedades a que me refería al principio de las que conviene dejar constancia, una muy importante es la que tiene que ver con los progresos efectuados recientemente para superar las dificultades que para la protección de los datos personales derivan de la naturaleza de *Internet*, desde hace tiempo imprescindible fuente de información, de relación y de servicios de todo tipo que por su carácter descentralizado y universal escapa a las posibilidades de control que pueden ejercerse desde un determinado Estado y demanda soluciones globales que, por ahora, están lejos de alcanzarse<sup>7</sup>. Así, no existen normas internacionales que establezcan un marco jurídico uniforme y son diferentes los niveles de protección de la información personal que se exigen en distintos ordenamientos. En este sentido, mientras en la Unión Europea la Carta de los Derechos Fundamentales y la Directiva 95/46/CE aseguran un régimen sustancialmente homogéneo que no impide a sus miembros dotarse de regulaciones más exigentes, otros países, algunos tan decisivos política y económicamente como los Estados Unidos de América, se rigen por criterios que descansan principalmente en la autorregulación, en las buenas prácticas y en los códigos de conducta y son, en general, menos rigurosos. Pautas estas que también se observan en los flujos de datos en el seno de las grandes empresas multinacionales<sup>8</sup>.

Estas dificultades explican el esfuerzo de las autoridades de protección de datos por avanzar hacia la definición de unos criterios mínimos aceptados internacionalmente que vayan preparando ulteriores desarrollos hacia una disciplina universal de la protección de datos personales. Un fruto muy destacado de ese empeño lo constituyen los *Estándares Internacionales sobre Protección de Datos Personales y Privacidad*, aprobados en Madrid el 5 de octubre de 2009<sup>9</sup>. Suministran una base compartida sobre la que, además de promover acuerdos de autorregulación, se podrá progresar en la consecución de una normativa homogénea que supere los obstáculos derivados de la territorialidad de los ordenamientos estatales y responda al carácter global de *Internet* y de las redes que se han ido extendido por el mundo.

<sup>7</sup> Sobre la cuestión, cfr. GUERRERO PICÓ, María del Carmen, *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Thomson-Civitas, Madrid, 2006.

<sup>8</sup> Sobre esas formas de autorregulación, véase SANCHO VILLA; Diana, “Normas corporativas vinculantes (*binding corporate rules*): aspectos sustantivos y de cooperación internacional de autoridades”, en *Revista Española de Protección de Datos*, nº 4/2008, págs. 35 y sigs.

<sup>9</sup> Su aprobación se produjo en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid los días 3 a 5 de octubre de 2009 bajo los auspicios de la Agencia Española de Protección de Datos. En [www.agpd.es](http://www.agpd.es) se puede consultar la llamada Resolución de Madrid que aprobó esos estándares.

Estos Estándares descansan, como ya lo hacen las leyes estatales, sobre principios vertebradores que ofrecen un fundamento sólido para construir ese imprescindible régimen homogéneo en la materia: son los de lealtad y legalidad en los tratamientos de datos personales, el de proporcionalidad, el de calidad, transparencia y responsabilidad. A ellos se añade el de legitimación para el tratamiento en cuya virtud solamente cabrá cuando medie consentimiento previo del interesado, lo justifique un interés legítimo del responsable siempre que no prevalezcan los intereses de los afectados, venga exigido por una relación jurídica con éste, sea necesario para el cumplimiento de una obligación del responsable o concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del afectado o de otra persona.

Por último, me parece que se debe llamar la atención sobre un especial frente de riesgos para la protección de los datos personales de todos pero, especialmente, de los menores, que participan masivamente en ellas, abierto con su reciente y rapidísima extensión. Me refiero al relacionado con las redes sociales. Me parece suficiente, para no alargar más estas páginas, remitirme al informe que sobre el particular ha elaborado la Agencia Española de Protección de Datos y que puede consultarse en [www.agpd.es](http://www.agpd.es)

<sup>10</sup>

---

<sup>10</sup> Se trata del *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*.