LIBERTAD RELIGIOSA, PROTECCIÓN DE DATOS Y DERECHO AL OLVIDO

RELIGIOUS FREEDOM, DATA PROTECTION AND THE RIGHT TO BE FORGOTTEN

Ignacio Ulloa Rubio[a]

Fechas de recepción y aceptación: 29 de noviembre de 2016, 12 de enero de 2017

Resumen: Evolución de la jurisprudencia en el Tribunal de Justicia de la Unión Europea, que está dividido en dos instancias: el Tribunal General, y el Tribunal de Justicia.

Evolución de la jurisprudencia de este último órgano, que es el que el que sienta la doctrina sobre dos derechos fundamentales, que son el derecho a la intimidad y el derecho a la protección de datos, relacionados también con el derecho a la libertad de información, en su última jurisprudencia.

Palabras clave: libertad religiosa, derecho a la intimidad, derecho a la protección de datos, derecho al olvido y derecho a la libertad de información.

Abstract: This lecture on the fundamental rights to privacy, freedom of speech and data protection, in relation to religious freedom, analyses ECJ Case-law on Case C-131/12 Google Spain, C-293/12 Digital Rights Ireland, C-230/14 Welinmmo and C-362/14 Schrems, that led to the annulment of Data Protec-

[a] Magistrado español en el Tribunal de Justicia de las Comunidades Europeas.

Correspondencia: Palais de la Cour de Justice. Boulevard Konrad Adenauer. Kirchberg.L-2925. Luxembourg

E-mail: iurairak@gmail.com

tion Directive 95/46/CE and catalyzed the implementation of new Regulation 2016/679 on Data Protection.

The author elaborates on who might be the "independent control authority" (article 91.2 Regulation 2016/679) in Spain for each religious faith and at ministerial level, what competences and capacities this authority might have within territorial boundaries. The author draws the conclusion that article 9.2 Regulation 2016/679 sets out – also in the field of collective exercise of religious freedom – a fundamental individual right to the non-appearance or concealment of personal data ("right to be forgotten"). The author gives his opinion on Regulation 2016/679 on the limitations on religious data transfer to third countries.

The speaker replies to delegate questions on hate speech on social networks, on limiting freedom of speech (and free press) against religious thought and on data protection in the supposed new agreements between the Catholic Church and Spain.

Keywords: Fundamental rights. Religious freedom. Data protection. ECJ case-law: C-131/12, C-293/12, C-230/14 & C-362/14. Directive 95/46/CE. Regulation 2016/679 on data protection. Fundamental rights conflicts. Independent data protection supervisor. Rectification, concealment and removal of personal data. Data protection transfer out of EU. Hate speech.

Ponencia

La idea que yo tenía era transmitirles una serie de reflexiones sobre lo que es la evolución de la jurisprudencia en el Tribunal de Justicia de la Unión Europea, que –como saben– se divide en dos instancias: el Tribunal General –donde trabajo yo– y el Tribunal –propiamente– de Justicia, es decir, voy a hablarles de la jurisprudencia de este último órgano, que es el que el que sienta la doctrina sobre dos derechos fundamentales, que son el derecho a la intimidad y el derecho a la protección de datos, relacionados también con el derecho a la libertad de información, en su última jurisprudencia. Sentencias que han tenido, o jurisprudencia que ha tenido, un impacto directo en la modificación o en el cambio legislativo que ha tenido que llevar a cabo el legislador de la Unión Europea.

Como consecuencia de las cuatro sentencias que les voy a citar a continuación, que son: la Sentencia *Google Spain*, que es la C-131/12 de 13-5-2014; la

Sentencia *Digital Rights Ireland*, que es el caso C-2093/12 de 4-4-2014; la Sentencia que se denomina *Weltimmo*, que es el caso C-230/14 de 1-10-2015; y la última y más reciente sentencia, Sentencia *Schrems*, Sentencia *Facebook*, que es la C-362/14 de 6-10-2015, el legislador de la Unión Europea se ha visto obligado a modificar aquella Directiva 95/46/CE, de protección de datos, y ha llevado a cabo la edición, o la publicación, de dos nuevas disposiciones, un Reglamento 2016/679 (que, como ustedes saben, son disposiciones de alcance general y de carácter obligatorio para todos los Estados miembros), es decir, hemos pasado –primer detalle que debemos retener– de directiva a reglamento, porque ya se considera que se ha producido una aproximación y homogenización de las regulaciones entre los Estados miembros, y por lo tanto la Unión, en virtud del principio de atribución de competencias y subsidiariedad, ha regulado propiamente y en profundidad toda la temática relativa a la protección de datos, al considerar que la directiva anterior era insuficiente. Y a continuación la UE ha promulgado la Directiva 680/2016, que es la directiva relativa al acceso a datos y comunicaciones en la sociedad de la información, especialmente para la persecución de delitos e infracciones muy graves.

La primera sentencia que les iba a mencionar, como les he dicho, es la sentencia a *Google Spain*, también denominada de la Sentencia *Costeja* (igual por este nombre les suena mucho más), o también conocida como la sentencia del "derecho al olvido". Esta sentencia tiene su origen en una reclamación, que efectúa un ciudadano, que se llama Mario Costeja González, ante la Agencia Española de Protección de Datos, al considerar que la publicación que se efectuó a través del motor de búsqueda de *Google Search*, cuando se introduce en él una búsqueda por su nombre, arroja unos resultados en los cuales aparece la deuda que él contrajo, 16 años atrás (la reclamación la efectuó en el año 2012), con la Seguridad Social, y que se publicó por edictos en un periódico, respecto al embargo de uno de sus bienes inmuebles, en el periódico *La Vanguardia*; y la recopilación de todas esas citas, de ese artículo en este medio, que se efectúa en la red. Es decir, en definitiva, mediante un mecanismo de búsqueda ordinario de la sociedad de la información y en la sociedad de internet, se produce un acceso a información sobre el señor Costeja que no es especialmente ni el idóneo ni el óptimo, según él considera,y en ningún caso parece que sea muy laudable, porque salen ahí sus deudas. El señor Costeja efectuó una reclamación, no solo contra *La Vanguardia*, como diario en el que salió publicado ese edicto y en el que originalmente se

encontraba la información, sino también contra *Google Spain*, y contra *Google Search* como motor de búsqueda.

La Agencia Española de Protección de Datos dictó una resolución en el año 2010, inicialmente, en la cual desestimaba la reclamación contra el diario *La Vanguardia*, al considerar que dicho diario *La Vanguardia*, por obligación de ley, debía publicar los datos relativos al señor Costeja, dado que se trataba de un embargo y un anuncio del embargo del bien que se iba a llevar a cabo, y sin embargo esto estima la reclamación que se efectúa tanto contra *Google Spain* como contra *Google International Corporation*, por entender que es una injerencia en el derecho a la intimidad y a la protección de datos, del señor Costeja.

Google Spain y *Google Search* o *Google International* recurrieron a la Audiencia Nacional. La Audiencia Nacional se planteó la cuestión jurídica, o la elevó en definitiva al TJUE. Se planteó primero quién o qué es lo que constituye la injerencia en el derecho fundamental, segundo, cuál es el grado de responsabilidad en esa hipótesis de existencia de injerencia, y tercero, la discriminación entre quién debe responder (porque una cosa es la publicación que se lleva a cabo en la web y otra cosa el acopio de esa información que se efectúa por los motores de búsqueda de *Google*, mediante la indexación de datos y contenidos por robots, y otra cosa –también distinta– es el grado de difusión que se da a esa información). Y a mayor abundamiento, hay que tener en cuenta que *Google España*, que era una de las empresas demandadas, es únicamente una empresa que emplea *Google* para su publicidad, es decir, esos contenidos asociados a las búsquedas. Cuando nosotros decidimos, por ejemplo, buscar piso, y a continuación en el margen derecho nos pone "alquiler de pisos", "venta de pisos", eso es lo que hacía *Google Spain*, publicidad marginal. Pero el motor de búsqueda, *Google Search*, se encuentra en Estados Unidos, con lo cual también se plantean cuestiones de jurisdicción y fuero. ¿Hasta qué punto se puede llegar a sancionar por la autoridad de supervisión de datos española?, ¿puede esta llegar a sancionar esos datos que existen, o cuya indexación se llevan a cabo en el extranjero?

Cuatro cuestiones sustanciales tratan esta sentencia: la primera, relativa al ámbito material de la competencia, realmente si tiene responsabilidad el motor de búsqueda, o es el gestor del motor de búsqueda el responsable. La segunda cuestión es la relativa a la aplicación territorial: se puede aplicar una norma nacional, aunque sea trasposición de la directiva, antigua Directiva 95/46 para el tratamiento de datos, cuando el establecimiento se encuentra en un Estado miembro,

pero qué pasa cuando realmente el establecimiento no está en el Estado miembro, o se trata de un establecimiento incluso fuera de la Unión Europea. La tercera cuestión que se plantea es la responsabilidad del gestor del motor de búsqueda y cuál es su alcance. Y finalmente la cuarta cuestión que se plantea es cuál es la responsabilidad de la persona que es el administrador de dicho motor de búsqueda.

Respecto a la primera cuestión, que es la relativa al ámbito material, sustancialmente lo que se plantea es si hay tratamiento de datos aquí, o sea, si realmente esa búsqueda llevada a cabo por el motor, y esa indexación y esa publicación de resultados constituyen un tratamiento de datos. A esta cuestión le da la respuesta la jurisprudencia en la Sentencia *Lindqvist*, que consideraba que era tratamiento cualquier referencia a datos, o datos personales, por cualquiera de los medios que se empleasen. Y, por lo tanto, los datos hallados, indexados, almacenados, puestos a disposición que hagan referencia a una persona física, los datos personales a los efectos del artículo 2, de la Directiva 95/46, y, en definitiva, el gestor del motor de búsqueda, que en este caso el motor de búsqueda pertenece a *Google International*, lleva a cabo una explotación de internet recogiendo, extrayendo, registrando, organizando datos, conservándolos, comunicándolos y facilitándolos. De todos estos indicios se concluye que las listas de resultados, en definitiva, pueden ser consideradas como tratamiento de datos a efectos del artículo 2 de la Directiva 95/46.

¿Quién es el responsable de este tratamiento de datos? Es la siguiente cuestión que seplantea el Tribunal de Justicia. Y entonces dice, bueno, vamos a ver, el gestor del motor es –en definitiva– el que determina cuáles son los fines y cuáles son los medios, y es –en un principio– el responsable. Pero, claro, hay que llevar a cabo una amplia definición del gestor, porque de lo contrario, si llevásemos a cabo una interpretación estricta, solo sería responsable quien efectivamente llevase a cabo ese tratamiento, y no habría tratamiento si se lleva a cabo por una máquina, y menos si la máquina se encuentra fuera de la Unión Europea. Entonces, en favor de una máxima protección o máxima tutela de los derechos, se llevó a cabo esta interpretación amplia, e igualmente, la sentencia llevó a cabo la distinción entre dos figuras, la del "gestor del motor de búsqueda", como persona responsable, y la del "editor de los sitios de Internet" o el que publica la página web. Si bien respecto al primero dice que, en definitiva, facilita el acceso a los datos del interesado y lleva a cabo, en su caso, la infracción, al facilitar ese acceso, puede no suceder así –respecto al editor–, en el sentido de que, si lo que estamos

persiguiendo es una búsqueda por nombre a través de un motor de búsqueda, es esa persona que facilita el motor de búsqueda quien debe responder, y no el que ha publicado las páginas web en las que sale el nombre de aquella persona. Es decir, la responsabilidad de la persona que lleva a cabo la publicación (*La Vanguardia*) sería en su caso subsidiaria, pero la responsabilidad prioritaria es del gestor del motor de búsqueda.

En definitiva, se considera que el "gestor de ese motor de búsqueda" lesiona o puede afectar a dos derechos fundamentales de la Carta de Derechos Fundamentales de la Unión Europea, como son el derecho a la intimidad, en el artículo 7 de la Carta de Derechos Fundamentales, el derecho a la protección de datos, artículo 8 de la Carta de Derechos Fundamentales.

Esto es con respecto al ámbito material.

Con respecto al ámbito territorial, aquí reside la cuestión esencial, ¿quién responde a *Google Internacional* por ser titular de *Google Search*, o a *Google España*, que propiamente no realiza ninguna labor de indexación, ni de almacenamiento de datos? No obstante, *Google España* facilita la publicidad, como les he dicho antes. El Tribunal señala en este sentido que *Google España* ejercita efectivamente, en el ámbito de España, una determinada actividad, constituye una filial de *Google Corporation*, de la multinacional, e indirectamente facilita la publicidad; por lo tanto, tampoco puede soslayar la responsabilidad que se derivaría del suministro de determinados datos adicionales. Pero no sería responsable con respecto a la búsqueda. El tratamiento de datos o la búsqueda es responsabilidad exclusiva de *Google Internacional*. Ahora bien, la Directiva 95/46 señala que solo tiene competencia respecto del tratamiento de datos de la Unión Europea, por establecimientos que se encuentren en la Unión Europea, y, ¿qué es lo que sucede?: que esto genera una frontera. Se puede realmente considerar que los datos que están tratados con motor de búsqueda fuera de la Unión Europea son competencia de la UE, o pueden ser objeto de supervisión, por parte de las autoridades comunitarias, y por parte de las autoridades nacionales. La respuesta ya venía dada en sentencias anteriores, en concreto la Sentencia *L'Oréal* en la que se dijo que debía ser la sucursal o el establecimiento, y no solo el establecimiento, sino en el marco de las actividades que tiene que realizar ese establecimiento.

Es decir, la publicidad que suministra *Google España* no tiene sentido si no es en la medida en que va ligada o vinculada a los resultados de la búsqueda. –Y en consecuencia se declara así también la responsabilidad de *Google España*, aunque

sea de otro carácter–. Es decir, el carácter principal es la responsabilidad de *Google Search* (de nuevo Estados Unidos), pero dada la obligación de garantizar, en el marco de las actividades del establecimiento, la protección de los datos, también *Google España* tiene una obligación de proteger los datos.

El tratamiento de datos con el motor de *Google Search* se considera que se lleva a cabo en el marco de las actividades de *Google España*, y es para la promoción y la venta publicitaria en España, y, en consecuencia, *Google España* debe cumplir con la directiva, dice la sentencia. Añadiendo que existe tratamiento de datos cuando el gestor de un motor crea en un Estado miembro una sucursal-filial, con finalidad publicitaria puesta al servicio del motor para las búsquedas en España.

Después de ver el ámbito material y el ámbito territorial, la siguiente cuestión estaría en la responsabilidad del gestor del motor de la búsqueda, en el gestor del motor de búsqueda que es *Google Search*, que debe responder garantizando, aunque sea por ese punto de conexión de su establecimiento con su sucursal en España, debe responder por todas las obligaciones, de la fidelidad de los datos y de la legitimidad y de la calidad de los datos, que se imponen por la Directiva 95/46, y que son también condiciones inherentes a la Ley orgánica de protección de datos en España.

En este sentido –pues– la obligación del gestor del motor de búsqueda parece ser que es mucho más importante que la que se podría establecer con respecto a la autoridad que se dedica a la publicidad, como es la empresa que se dedica a la publicidad (*Google Spain*), y se señala que el tratamiento de datos por el gestor del motor de búsqueda implica una injerencia directa en la vida privada, en la protección de datos, porque facilita una visión estructurada de la información, ya que si no existe el motor de búsqueda, sería bastante más difícil acceder a toda esa información, de tal manera que facilita a los internautas todos esos datos, y además de producirse una injerencia, por el mero suministro de esos datos, o por la mera búsqueda por el motor de esos datos, el gestor potencia la lesión del derecho fundamental, en la medida que lo divulga o lo difunde; es decir, multiplica los efectos de esa injerencia por todo internet. En este sentido se recoge lo que era una doctrina de la sentencia, *eDateAdvertisements*, relativa a las citas por internet, que le fue entregada al Tribunal.

En cuanto a la gravedad de la injerencia, aplicando la técnica de ponderación de derechos en juego, como siempre que hay una injerencia en un derecho fundamental, hay que analizar (dado que no hay ningún derecho fundamental

absoluto) si esa injerencia es necesaria, si esa injerencia es proporcionada y cuál es el grado de afección. Si –en definitiva– se respeta el contenido sustancial de ese derecho, o si no se respeta, en cuyo caso siempre la injerencia será lesiva. Si se respeta el contenido sustancial, hay que ver si esta injerencia está justificada por la presencia de cualquier interés superior, que es lo que haría que entrase en juego lo que se denomina el canon de la proporcionalidad. Y ¿cuáles son los intereses que están aquí en juego? Pues, por un lado, estarían los intereses económicos del gestor del motor de búsqueda de *Google Search*, y por otro lado los intereses legítimos, que podríamos considerar de todos los internautas que quieren acceder a una determinada información, y a quienes provee un servicio Google, en ese sentido.

¿Estos intereses deben prevalecer por encima de los del titular de esa información, de ese derecho a la intimidad, o de ese derecho a la protección de datos? Pues en principio tendría que existir una autoridad de control, por un lado, como es la autoridad de protección de datos, la Agencia de Protección de Datos en España, y, por otro lado, tendría que existir también una autoridad de control judicial posible. Ese es el primer canon que tiene que existir: poder verificar que se ha producido una extra-limitación, y una afección directa a la intimidad, en cuyo caso el interesado puede efectuar una solicitud ante una entidad o autoridad administrativa, y que esa solicitud sea susceptible de ser revisable ante una autoridad judicial, para que la autoridad judicial –o autoridad administrativa– lleve a cabo la eliminación, la rectificación de los datos, de la lista de resultados, porque, en concreto, la protección que trata de obtener el señor Costeja, en el pleito de origen, no es en abstracto, respecto a su derecho a la intimidad, sino que es en concreto, con respecto a la publicación de los datos con su nombre.

En cuanto a la conclusión que saca el Tribunal de Justicia, a este respecto, señala en concreto que ni siquiera la excepción del derecho a la información puede prevalecer sobre el derecho del interesado, puesto que ni siquiera el derecho al conocimiento por el público en general puede estar por encima del derecho del interesado a la divulgación de sus datos (y menos si son datos ignominiosos). Y el Tribunal señala igualmente la importancia, hasta el punto de que ni siquiera el propio interés del editor de la página web en la publicación puede prevalecer sobre el propio derecho del interesado. En definitiva, la publicación en la web y el tratamiento mediante el motor de búsqueda pueden producir un impacto en la vida privada, en cuyo caso debe prevalecer el derecho a la vida privada del intere-

sado. El gestor del motor de búsqueda, en consecuencia, está obligado a eliminar la lista de resultados de la búsqueda por nombre de una persona, mediante vínculos en páginas web publicadas por terceros. Y esto, aunque la información no se hubiere simultáneamente rectificado en la web de origen, ni, aunque la publicación por el motor de búsqueda sea lícita. Es decir, parece que aquí el Tribunal es muy categórico respecto a la preponderancia, o a la prevalencia, del derecho a la intimidad de la vida privada.

La última cuestión, o la cuarta cuestión, es a quién se puede exigir la responsabilidad y cuál es el grado de responsabilidad del motor de búsqueda. Se le puede exigir, partiendo del presupuesto de que la Ley de protección de datos y la directiva de protección de datos permiten un tratamiento de los datos, si bien el único tratamiento que se permite es el tratamiento de datos si es compatible. Así, se está declarando, por parte del Tribunal, que el tratamiento que se ha efectuado es –de por sí– ilícito, y es contrario a lo establecido en la propia directiva. Por lo tanto, habrá que proceder a la protección y tutela de estos derechos, y, en consecuencia, declara el Tribunal que, en el caso de autos, en la lista de resultados obtenidos a partir del nombre, aunque contenga la referencia a las deudas de la Seguridad Social por embargo, que se publicaron en su momento, hace referencia a datos de hace 16 años, cuyo interés público o interés legítimo en ser conocidos es muy relativo. Y señala el Tribunal que el derecho del interesado, a que las interferencias y a que su nombre no conste más en las listas, debe prevalecer; y, en consecuencia, el interesado puede solicitar la protección de su derecho fundamental, con prevalencia a cualquier interés público general. Y sus intereses deben estar por encima de los intereses del gestor, y del principio del acceso a la información.

Como puede apreciarse, ya en esta primera sentencia analizada se llevan a cabo unas declaraciones muy importantes, ¿por qué?, porque se consagra –en definitiva– lo que se ha denominado como "derecho al olvido", el derecho a que cuando una persona tiene un dato que ha sido publicado, en su momento lícitamente, que tiene su origen a su vez en hechos fehacientes y en hechos verídicos, el dominio sobre esa información no corresponde al dominio público, sino que corresponde al propio interesado, con la salvedad que también hace la sentencia de personas que tengan una vida pública, respecto a las cuales sí que debe prevalecer el derecho a la información. Es decir, la regla general es que *para todos los mortales* la publicación de un dato que nos afecte por parte de *Google*, en las búsquedas de *Google*, dato cuya publicación no hace falta que sea ilícita,

es decir, no hace falta que sea un dato falso o un dato injurioso, sino que puede ser incluso un dato lícito que contenga una información veraz. Los ciudadanos, nosotros, tenemos derecho a que ese dato acabe desapareciendo de esa relación de búsquedas, o de esos resultados de la búsqueda, que facilitan los motores de *Google Search*. Ahora bien, para que se produzca esa desaparición tiene que efectuarse la correspondiente solicitud o petición.

Hoy ya se sabe que se ha efectuado por parte de muchos ciudadanos esa solicitud de rectificación, y que incluso en la Audiencia Provincial de Barcelona se han producido, como consecuencia del no-borrado de los datos de la persona interesada, la confirmación jurisdiccional de la imposición de una multa de 8.000 euros.

La segunda sentencia que quería comentarles es una sentencia que se llama *Digital Rights Ireland* (C-293/12), también denominada caso *Seitlinger*. Esta es una sentencia muy importante, que afecta sustancialmente, no a la Directiva 95/46, sino a la Directiva 2006/24, que es la directiva sobre conservación de datos en relación con redes públicas de comunicación electrónicas.

No sé si ustedes saben que normalmente todos los datos que nosotros utilizamos por estos aparatos móviles se recopilan y acopian por parte de los proveedores de los servicios de telefonía e internet, y se conservan por un período transitorio, por razón justificada, por un lado, por el deber de comunicación que se efectúa por parte de las entidades explotadoras de redes a la Agencia de Protección de datos, y, por otro lado, para poner los datos a disposición de las fuerzas y cuerpos de seguridad del Estado y de otras autoridades, en el caso de que haya que investigar delitos graves.

Pues la Sentencia *Digital Rights*, sustancialmente, analiza la Directiva 2006/24, que es la directiva marco, en la que la Unión Europea establece el régimen de conservación de datos en el mercado de las comunicaciones electrónicas. Esta directiva tiene sus antecedentes en la Directiva 95/46 y en otra Directiva 2002/58, y, en definitiva, todas estas directivas ponderan sustancialmente dos aspectos: uno el aspecto mercantil de los datos, en el que hay un interés prioritario por parte de las entidades a que los datos que se trasmitan o transfieran por razones económicas, incluso dentro del ámbito de las grandes libertades de la Unión Europea (la libre circulación de personas, bienes, capitales y servicios), está también la libre circulación de datos, con arreglo a la cual los datos que hayan sido obtenidos de manera lícita pueden ser conservados, almacenados y transmitidos

con arreglo a los parámetros establecidos en la directiva. Por lo tanto, se reconoce el valor económico de esos datos, como un objeto de comercio, pero teniendo como contrapartida que ese valor económico tiene que venir ponderado por los derechos fundamentales que entran en juego o conflicto. Una vez más los derechos fundamentales, en el aspecto europeo de la Carta de Derechos Fundamentales, son el derecho a la vida privada y derecho al tratamiento de datos, sin perjuicio de que también pueda afectarse al derecho a la libertad de información, como hemos visto antes en el asunto *Google*.

En este asunto, Digital Rights, sustancialmente, lo que se planteaba es hasta qué punto puede esa directiva de comunicación y archivo de datos en el mercado de las comunicaciones autorizar la transmisión de datos que debe ser lícita. En principio, la directiva estableció una normativa exhaustiva, hasta el punto de que, les leo así unos artículos, como el artículo 1, que tiene como objetivo armonizar las disposiciones entre los Estados miembros; el artículo 2 define los datos, el usuario, el servicio telefónico, el identificador por razón de usuario, el identificador por celda, en definitiva, de carácter técnico. En el artículo 3 se proclama la obligación de conservar datos. En el artículo 4 se señala qué es lo que se considera como acceso a datos. Y, sustancialmente, en el artículo 5, se señala las categorías de datos, y entonces nos distingue: categorías por origen, de telefonía, o de internet y correo electrónico. De telefonía, número de teléfono, nombre y dirección de la persona afectada. Por razón de internet, nos indica el usuario, número de teléfono y la ubicación IP. Por razón del destino, distingue –de nuevo– por telefonía, internet y correo electrónico. Por telefonía, el número marcado, la transferencia y el desvío de llamadas, el nombre y la dirección del abonado; de internet, el usuario destinatario…, es decir, nos indica –de nuevo pormenorizadamente– cuáles son los supuestos en los que se debe autorizar a la compañía a transferir esos datos por razones en las que prevalece el interés público, que veremos a continuación. También afecta a la fecha, hora y duración, al tipo de comunicación, al equipo de comunicación, a la localización del equipo, a las normas de contenido. El período máximo de conservación se fija entre seis meses y dos años, en la directiva. Creo recordar que en la legislación española la conservación de datos quedó al final en un año. Se establecen determinadas reglas para la protección de la seguridad de estos datos, los requisitos para que las personas puedan tener acceso a esos datos, tanto a la empresa como en el ámbito de la investigación de delitos, las autoridades de control también a nivel nacional,

la correspondiente obligación que existe de las autoridades de control de datos nacionales, de supervisar también a las fuerzas y cuerpos de seguridad del Estado. En este sentido, creo que es una garantía adicional, que marca la directiva y que fue cumplida, el que esta regulaba los recursos judiciales y la responsabilidad por infracciones y sanciones.

¿Qué es lo que se plantea en definitiva?, pues ¿cuál es la validez de esta directiva? Y, para aclararlo, el Tribunal sigue una dinámica de análisis de cuáles son los derechos fundamentales afectados; de nuevo recalca los derechos a la intimidad, a la protección de datos y a la libertad de información, y señala que si el objetivo es armonizar las disposiciones entre los Estados miembros, este es un objetivo muy encomiable; así mismo, si el objetivo también es la libre circulación de datos, estamos ante otro objetivo igualmente destacable.

¿Cuáles son los requisitos que se establecen para que estos datos puedan recogerse o cuál es la extensión? Pues parece ser –como les he contado antes– que en el artículo 5 se recogen datos de origen, de destino, de comunicación, fecha y hora, duración, equipo de localización del móvil, abonado y también usuario, número de origen y número destino, la dirección IP y con qué persona y de qué forma se ha llevado a cabo la comunicación.

Esto es indudable: simplemente combinando todos estos datos se pueden establecer conclusiones muy valiosas; es decir, se está reconociendo implícitamente por el propio legislador comunitario que hay una injerencia en el derecho fundamental, pero lo que hay que analizar es si es injerencia es de significado o calado; y para ello el Tribunal de Justicia de la Unión Europea lleva a cabo –de nuevo– un análisis, una ponderación que es la ponderación habitual en el ámbito de los derechos fundamentales. Concluye el TJUE que hay una injerencia, y dice que el acceso a estos datos por parte de las personas autorizadas es una injerencia; pero, en principio, hay que entender que por razón de intereses prevalentes puede que la injerencia esté autorizada. No obstante, hay que poner de relieve que hasta ahora los únicos datos que se facilitaban hasta el año 2006 (fecha de publicación de esta directiva), por parte de las compañías de telefonía e internet, en la línea con la jurisprudencia de Estados Unidos, eran los datos de tarificación. Es decir, los datos de facturas; incluso de llamadas concretas. Ahora, parece ser que esta Directiva 2006/24 habilita –como les he dicho– a transferir muchos más datos.

Por lo tanto, se considera que el acceso a los datos constituye una injerencia, que el mero hecho de conservar esos datos es otra injerencia en la vida privada,

y que la facilitación y el acceso a esos datos por parte de las autoridades nacionales se considera un acceso autorizado, y que no sería injerencia lesiva el de los derechos fundamentales, y otras dos injerencias, como la conservación y la transmisión de datos, que sí se consideran lesivas. Además, se considera que esto es respecto a la intimidad; pero además, sí se considera que existe otra afección a un derecho fundamental, con respecto a la protección de datos. En definitiva, el Tribunal de Justicia está hablando de al menos tres injerencias.

Luego haré un pequeño excurso para ver cuál es la metodología empleada, porque yo siempre mantengo, y don Juan José González Rivas me podrá confirmar posteriormente, que lo que no se puede hacer nunca es empezar a hacer un análisis sesgado de la realidad. Los jueces siempre tenemos la obligación de efectuar una apreciación global. Si nosotros empezamos a hacer, como dicen los franceses, a "trancher", a cortar en lonchas la realidad, a analizar siempre, haremos un análisis limitado, pudiendo llegar a conclusiones erróneas. Cuando se empieza a hacer un análisis global, tenemos que tener en cuenta todos los elementos, para poder establecer conclusiones *erga omnes*. Y esto lo traigo a colación porque al hablar de una sola acción, al final uno saca tres injerencias; si seguimos con esta metodología, a la exponencial, podemos al final concluir que todos los derechos fundamentales de la sección primera, capítulo segundo, artículo primero de la Constitución, tienen alguna afectación. Por el mero hecho de que nuestros datos sean transferidos a una compañía, son susceptibles de ulterior transmisión a los cuerpos de seguridad.

El segundo escalón en el análisis del TJUE, después de concluir que hay dos o tres injerencias, es el estudio de si existe la justificación de esta injerencia. En la Carta de Derechos Fundamentales de la Unión Europea, en el artículo 52, se sigue –en este sentido– una metodología como la que les he comentado anteriormente. Para cualquier limitación de un derecho fundamental hay que analizar si esa limitación está permitida por la ley, si respeta el contenido esencial del derecho, y luego emplear el canon de la proporcionalidad: que la medida sea necesaria, que satisfaga un interés general, y que se hagan respetar los derechos y las libertades de los demás, de terceros. Vamos a analizar en concreto en el supuesto.

Respecto a los objetivos de interés general, como se ha dicho anteriormente, el objetivo de la directiva, en este caso aumentar la aproximación de las disposiciones de los Estados miembros, y otro objetivo muy importante –que yo creo prevalente– es el objetivo de interés público: la lucha contra la delincuencia grave

y contra el terrorismo. Y además la Unión Europea, no solo en sus disposiciones normativas, sino en la propia jurisprudencia del Tribunal, en la Sentencia *Kadi y Al Barakaat International Foundation*, ya ha reconocido que la lucha contra el terrorismo es una prioridad, y que está incluso por encima de otras libertades. Se ha reconocido también que la lucha contra la delincuencia grave es también una prioridad, y que prevalece respecto a las libertades individuales en el caso *Tsakouridis*. También se ha dicho que existe un derecho colectivo a la libertad y a la seguridad, que es lo que justifica esas injerencias en la intimidad. Y también se ha reconocido, incluso a nivel normativo en los consejos de justicia y asuntos de interior de la Unión Europea, en sus conclusiones, que se reconoce la lucha contra la delincuencia organizada como otra de las prioridades de la Unión Europea. Luego, si el interés económico o la armonización de legislaciones pueden no ser unos intereses prevalentes, sí que parecen serlo una serie de intereses prevalentes, como la lucha contra el terrorismo, la lucha contra la delincuencia grave o la lucha contra la delincuencia organizada.

A continuación, dentro de este segundo estadio del análisis de la reflexión jurídica, el Tribunal aplica el principio de proporcionalidad, y dice: ¿son proporcionadas estas medidas respecto al objetivo legítimo, existe control jurisdiccional para estas medidas? Y concluye que la facultad de obtención de estos datos, y la facultad de su transmisión, aunque sea por delitos graves y aunque sea con el objetivo de armonizar, tiene que ser analizada distinguiendo entre lo que son casos de conservación y los supuestos de conservación en concreto, y las garantías que se presentan suficientes. Respecto a los casos y medios de conservación, ya los hemos citado anteriormente, y son supuestos de teléfono fijo, teléfono móvil, internet, correo electrónico y teléfono por internet. Respecto a la población, en principio afectaría a los abonados, y también a los usuarios. Respecto a las personas, afecta a todo tipo de personas, afecta a todo medio de comunicación, y de ahí se concluye que incluso podría afectar al tercero no interesado, afectando incluso a casos de secreto profesional. Es decir, se podría tener acceso a datos que estarían protegidos por el secreto profesional.

Además, se puede producir el acceso posterior, para la persecución de los delitos de terrorismo y de crimen organizado, pero con la paradoja de que la definición de estos delitos no se ha llevado a cabo en la legislación europea, sino que ha sido llevada a cabo en la legislación nacional. Luego parece que también hay un trasvase, o trasferencia a la legislación nacional en esta materia.

¿Y en cuanto a las garantías? El Tribunal concluye que parece ser que no se especifican en la propia directiva, ni siquiera las garantías de procedimiento para el acceso, tampoco se establece un límite concreto de las personas que puedan tener un acceso posterior. Respecto al plazo, concluye el Tribunal que el plazo de seis meses a dos años que se otorga es demasiado extenso y no se distingue en función de las categorías de datos. Y–en definitiva– concluye que no existen garantías suficientes para proveer que no se tenga acceso a la integridad de la información, ni que incluso no se tenga acceso a la confidencialidad.

Porque tengan en cuenta que cuando se transfieren los datos, normalmente lo que no se tiene acceso es al contenido de la conversación, pero sí que se tiene acceso a que ha tenido lugar la comunicación de la información entre una determinada persona y otra, a determinada hora, con determinada extensión, y por determinado medio de comunicación. Pero el TJUE considera que la falta de garantías puede acabar afectando incluso a los contenidos, y que al final la persona que tiene acceso a esos datos pueda tener acceso, por vía indirecta, a los contenidos, sacando determinadas conclusiones directas y, en consecuencia, concluye, que la directiva sobrepase los límites de lo estrictamente necesario.

Quisiera hacer aquí un paréntesis –que ya les he anticipado anteriormente que haría–, y que me parece que en esta sentencia no está de más. Don Juan José González Rivas lo podrá confirmar, pues este método empleado en *Digital Rights* ya "nos suena de algo", porque en el Tribunal Constitucional lo hemos "padecido" con mucha frecuencia. Y es cierto. No daré ningún dato más, porque algún jurista español "reconocido" es el "padre" de este método empleado en alguna sentencia constitucional. Pero el método empleado –yo creo– no es del todo honesto, porque desconoce una realidad. Es cierto que la Carta de Derechos Fundamentales de la Unión Europea reconoce o trata de otorgar la máxima protección a los derechos a la intimidad, a la protección de datos, o a la libertad de información. Pero la carta es mucho más respetuosa y fija un canon de enjuiciamiento mucho más limitado en el artículo 52, de lo que se podría hacer en España. En España somos mucho más intuitivos que en la Unión Europea, y esto ¿por qué?

Pues por la sencilla razón de que la Unión Europea el legislar solo establece unos mínimos imprescindibles. El denominador común mínimo para que los Estados puedan funcionar y desarrollar su legislación y sus acciones. Por lo tanto, estimo que no se puede, por un lado, reprochar la falta de pormenorización al legislador europeo cuando entre sus obligaciones está el no agotar la materia (pues

resulta que, si la directiva regula exhaustivamente y a fondo la materia, tanto en lo relativo a las personas como en la duración de las conversaciones, respecto a las personas que tienen que tener acceso, entonces la directiva se estaría extralimitando legislativamente, y la responsabilidad sería para la Unión Europea). Por ello, yo creo que el Tribunal de Justicia peca aquí –un poco– de llevar a cabo un análisis parcial, porque tendría que haber tenido en cuenta que suposición –precisamente– es la de juzgador comunitario, no de juzgador nacional. Emplear la metodología, la técnica de los Derechos Fundamentales, empleada a nivel nacional, en el ámbito de los Derechos Fundamentales de la Unión Europea (a pesar de que todos los derechos fundamentales tienen identidad de contenido y su interpretación debe efectuarse con arreglo a los cánones europeos del Tribunal de Estrasburgo no los del Tribunal de Luxemburgo), no es correcto.

No obstante, no se puede reprochar al legislador comunitario su falta de especificidad, cuando –precisamente–, si el legislador hubiese estado más autolimitado, habría cometido otra infracción mucho más grave, al no haber cubierto sus fines u objetivos comunitarios. Y, por otro lado, a mí me parece que lo que no se puede es ir fraccionando el análisis de la realidad a juzgar (–que es un poco lo que rezuma en el trasfondo de esta sentencia–, esto es una cosa que también hemos visto muchas veces en casa) porque presumir que la persona, o presumir que las personas que van a tener acceso a esos datos, habiendo sido autorizada la transferencia (es decir, cuando las compañías transfieren los datos a fuerzas y cuerpos de seguridad para persecución de delitos), que esas personas operan ilícitamente o van a obrar mal, sin que exista prueba en el procedimiento en concreto de que ha habido una extralimitación, sin que haya habido una injerencia, ni un revelación ilícita de datos; presumir que esos funcionarios van a actuar mal, *a priori* normativamente, es algo que no viene en el texto de la ley; y además a mí me parece que es "torticero" –como decimos los juristas–, pues manipula la realidad. Porque no existe ningún dato en el procedimiento acerca de esa presunción de acción ilícita de los agentes.

Ahora bien, ¿qué es lo que sucede?, ¡claro!, que es muy fascinante decir que se ha hecho mal una directiva de aproximación de legislaciones de Estados, en materia conservación de datos, cuando los responsables son las empresas de telecomunicación y los "beneficiarios ulteriores", entre comillas, porque los beneficiarios somos los ciudadanos, en la medida en que se garantiza más nuestra libertad, puesto que los instrumentos mayores de garantía van a ser las fuerzas y

el cuerpo de seguridad del Estado. Esto es políticamente correcto –en la línea de lo que decía don Ignacio Sánchez Cámara–. Entonces, está muy bien decir que esta conservación de datos está fatal, que menuda falta de especificidad, que menuda extralimitación legislativa, que –en definitiva– esto es un auténtico abuso de derecho por parte del legislador de la Unión Europea (cosa que a mí me parece falso –por lo que les he comentado–, porque se lleva a cabo un análisis parcial de la realidad). Y porque hay que partir del presupuesto conceptual de lo que es una directiva (¡una directiva no es un reglamento!). Una directiva, no entraña una regulación pormenorizada. Si a usted la directiva le plantea dudas con respecto al tercero (como plantea dicha intervención respecto al tercero en casa, porque también las hacemos con respecto a las intervenciones telefónicas). El tercero no investigado en España, cuando hay una intervención telefónica, ocasionalmente también resulta escuchado el contenido de su conversación. Pero eso el Tribunal Constitucional siempre ha considerado que es una intervención accidental en el contenido de una conversación; y en la medida que el diligente funcionario la va a excluir (juez de instrucción o fiscal), de su instrucción o investigación, cabe entender que se puede delegar en las fuerzas de seguridad, que están supervisados por jueces y fiscales, esas "extralimitaciones" sin padecimiento para el contenido esencial del derecho fundamental. ¡Pues no!, el Tribunal de Justicia –como muchas veces hace nuestro Tribunal Constitucional– consideró que la directiva no era concorde o acorde con la Carta de Derechos Fundamentales y decretó la nulidad de esta directiva de 2006.

La tercera sentencia que quería comentarles es la Sentencia *Weltimmo*, del caso C-230/14. Es una sentencia relativamente interesante porque se trata de un supuesto en el que el *Weltinmmo* es una compañía residenciada en Eslovaquia, que se dedica a la venta y promoción de inmuebles en Hungría, donde tiene una página web que recoge inmuebles húngaros y los trata en un servidor en el extranjero. Entonces la cuestión que se plantea es si la sanción que le impone la autoridad de supervisión de datos húngara es pertinente. La cuestión prejudicial es planteada por el Tribunal Supremo de Hungría, porque considera que no entiende hasta qué punto, si de acuerdo con la Directiva 95/46 (la que vimos anteriormente de protección de datos en el primer caso) la responsabilidad es para el titular del establecimiento, y el establecimiento está en Eslovaquia, cómo es que en este caso una autoridad de Hungría puede imponer una multa a una compañía eslovaca.

Hay una serie de matices en el caso *Weltinmmo* que hacen comprender por qué al final se acaba diciendo que las autoridades húngaras tienen competencia para la supervisión de actividades de establecimientos con entidades de tratamiento de protección de datos que se sitúan en otro Estado miembro, y en el que transfieren datos a un ulterior Estado.

El caso *Weltinmmo* tiene –como les estaba diciendo– la gran peculiaridad de que *Weltinmmo* no es que simplemente se hubiese constituido en Eslovaquia, sino que desarrollaba principalmente su actividad en Hungría, porque tenía allí la página web, porque los inmuebles eran húngaros, porque había un administrador que estaba en Hungría, porque tenía una cuenta corriente en Hungría. Es decir, hay más datos, más allá de la pregunta formulada por el Tribunal Supremo Húngaro, que hacen intuir que existe un punto de conexión para que las autoridades de protección de datos de Hungría, las cuales puedan acabar conociendo de actos de tratamiento de datos llevados a cabo por una compañía extranjera.

Pero lo que yo quería destacarles de esta sentencia del *Weltinmmo* es la conclusión a la que llega, que es un poco paradójica. Dice el Tribunal: es cierto que la autoridad húngara puede acabar conociendo de este tratamiento de datos que se lleva a cabo por la compañía del *Weltinmmo* de Hungría, porque aquí hay un servidor, porque tiene inmuebles húngaros, porque además allí había una cuestión de consumo interesante, que es que *Weltinmmo* lleva a cabo *la picaresca* de que hacía que la gente, las agencias inmobiliarias, se diesen de alta en la página web en Hungría, y que durante el primer año *Weltinmmo* les daba el servicio gratis de difusión de sus inmuebles. Pero después del primer año les empezaba a cobrar, de oficio. Entonces, ahí había un cierto fraude al consumidor, que también justificaba que la autoridad húngara interviniese.

Pero hay una cosa que es paradójica: la autoridad húngara tiene competencia para llevar a cabo esta supervisión en materia de protección de datos, pero no tiene la competencia para llevar a cabo la ejecución de la sanción. En el artículo 28 de la Directiva 95/46 dice que las autoridades, quienes se consideren autoridades encargadas de la supervisión, tendrán competencias de intervención y competencias de sanción. Entonces, en este sentido, la Sentencia *Weltinmmo* –a mi modo de ver– constituye un paso regresivo, porque considera que no hay una competencia para imponer la sanción a la compañía constituida en Eslovaquia, que lleva acabo la gestión de la página web en Hungría, porque –en definitiva– dice que quien debería sancionar al establecimiento es la autoridad eslovaca. Esto

creo que –como les digo– es un paso atrás, porque es la primera vez que se limita de forma territorial la competencia de las autoridades de supervisión en materia protección de datos.

La última sentencia que les quería comentar es la Sentencia Schrems, que es la sentencia que se denomina de Facebook. El señor Schrems es un ciudadano que contrata sus servicios con *Facebook Irlanda*. Él firma el contrato para su cuenta de Facebook, pero no se da cuenta de que en la letra pequeña de ese contrato pone que *Facebook Irlanda* trasferirá sus datos a *Facebook Estados Unidos*. Y ¿qué es lo que sucede? Que *Facebook Estados Unidos* tiene, por una serie de obligaciones que se llaman de "puerto seguro" la obligación de registrarse frente a las autoridades de comercio de Estados Unidos. Hasta aquí no hay ningún problema, pero cuando vienen los programas de investigación de la autoridad de la NSA, la autoridad de inteligencia americana, se establece una serie de excepciones, por razones de protección de la ley nacional y de la seguridad nacional, conforme a las cuales la NSA puede recabar de todas las empresas que haya en Estados Unidos los datos que tengan en sus bases de datos. Ahí es cuando se acaba produciendo una injerencia.

El señor Schrems dice: la Unión Europea tiene que hacer algo, porque yo estoy dando mis datos a una compañía europea, y se está produciendo una transmisión autorizada de datos, por un convenio que se ha llevado a cabo entre la Unión Europea y Estados Unidos conforme a la Decisión 2000/520 para la transferencia de datos entre empresas multinacionales, pero es que ustedes no se dan cuenta de que al final de la cadena de transmisión se produce una injerencia por parte de las autoridades de seguridad de Estados Unidos que ni la Comisión Europea ni ningún Estado miembro han verificado cuál es el grado de protección de mis derechos fundamentales, de mis datos, cuando están en Estados Unidos. Esto es lo que pone de relieve el señor Schrems: ¡Mucho cuidado!, yo estoy transmitiendo datos o cediendo datos voluntariamente, la transmisión de esos datos a otra compañía se puede considerar también conforme a la directiva, porque hay un convenio firmado en el marco de la Decisión 2000/520 que ha sido supervisado por la Unión Europea, pero lo que sería el último tramo de la transferencia de datos, o el acceso a esos datos por parte de las autoridades de seguridad nacional de Estados Unidos, eso está fuera del control de la Unión Europea, y si nosotros –Unión Europea– queremos garantizar una máxima protección al del derecho a la intimidad, o una máxima protección de los datos que son transferidos, en fin… esto hay que analizarlo.

¿Qué es lo que sucedía? Que la Unión Europea llevó a cabo una cierta fiscalización en principio más allá de la Directiva 95/46, y dictó una decisión, que es la Decisión 2000/520, en la que consideraba que definía suficientemente lo que era el "puerto seguro", y decía: bueno, pues el "puerto seguro" consiste en que gente –usuarios y operadoras– han adquirido un cierto grado de compromiso, unilateralmente, en la materia de protección de datos, lo cual nos garantiza que tienen una persona encargada de la protección de datos en su empresa, y que va a cumplir determinados estándares que son altos, que suscriben un compromiso de indemnización de daños y perjuicios, en el supuesto de que se produzca una filtración de datos de algún tipo, y –bueno– con este régimen de compromiso de derecho privado, que se denomina el "puerto seguro", podemos considerar que es suficiente para proteger la intimidad y la cesión autorizada de datos. Y además –dicen–, si no sabemos cómo funciona esto del "puerto seguro" privado, las autoridades comerciales americanas han elaborado unas Frequently Asked Questions, las FAQ (preguntas frecuentes); y como en las autoridades que se adhieran al "puerto seguro" tienen que tener y dar una explicación en sus *Frequently Asked Questions*, en las páginas web respectivas, sobre cómo funciona, y cuál es el grado de compromiso que ellos adquieren con la protección de datos, pues con esto la Unión Europea se da por satisfecha.

Aquí, si estuviésemos a nivel comercial, podríamos llegar a aceptarlo. Pero cuando estamos hablando de un contenido sustantivo o sustancial, y si se puede llegar a saber quién se comunica con quién, a qué hora y de qué modo, y cuando ya –encima– las autoridades americanas pueden tener acceso a los contenidos de esas conversaciones, no directamente (porque el proveedor del tratamiento de datos no se los facilite, sino porque por otros medios pueden llegar al contenido de esas conversaciones), pues –en fin– habría que ser muy cautelosos. Y, además, la Unión Europea –ya, ¡la propia Unión Europea!– dictó dos comunicaciones en el año 2013 advirtiendo de las carencias del sistema. Esto es, en el año 2000 la UE llevó a cabo una supervisión y dijo: vamos a aceptar este protocolo de "puerto seguro" siempre y cuando se cumplan las condiciones mínimas. Pero en el año 2013, la propia Unión Europea empieza a llamar la atención sobre el incumplimiento de las normas de "puerto seguro" por parte de proveedores de servicios de internet, en relación con la protección de datos en Estados Unidos.

Al final, ¿qué es lo que sucede? Pues que la jurisprudencia del Tribunal de Justicia tiene que solventar cuál es el grado de fiscalización que se puede efectuar

respecto a un convenio, firmado por la Unión Europea, de transferencia de datos con Estados Unidos, y cuáles son los impactos en los derechos fundamentales de la carta que se producen en Estados Unidos. Y en este sentido la Sentencia Schrems sí que es pionera.

La primera cuestión que se plantea la sentencia es cuáles son las facultades de las autoridades nacionales respecto del control no ya de las autoridades comunitarias, sino de las autoridades nacionales. Y concluye que las autoridades nacionales deben tener facultades de investigación e intervención. Lo hemos visto en el caso anterior *Weltinmmo*. Por lo tanto, se debe garantizar que cualquier persona que presenta una solicitud en el territorio de la Unión tenga la garantía a una autoridad de protección de datos, en la propia Unión; que tenga acceso a una posibilidad de decisión judicial frente a esa decisión de la autoridad de protección de datos. Pero, claro –una vez más–, ¿cuál es el grado de control que tienen las autoridades de protección de datos o los jueces nacionales respecto de las potenciales injerencias o eventuales injerencias que se llevan a cabo en Estados Unidos? Pues bien, ahí se suscita la extraterritorialidad del derecho de la Unión Europea, y la extraterritorialidad de las competencias de las propias autoridades europeas, para cuya resolución hay que acudir al convenio, y ver cuáles son los límites del convenio. Y ahí tenemos lo que expresamente planteó el señor Schrems ante las autoridades judiciales, la High Court de Irlanda, que reconoció, y dijo: los tribunales irlandeses no tienen ninguna capacidad de verificar qué es lo que están llevando a cabo por las autoridades comerciales de Estados Unidos, ni por las autoridades de seguridad nacional estadounidenses, y –en consecuencia– lo que suceda de aquí (Europa) hacia allá (Estados Unidos de Norteamérica) no podemos fiscalizarlo los tribunales irlandeses.

Entonces –en definitiva– lo que se pone en tela de juicio es la propia validez de la Decisión 2000/520, en cuyo marco se acordó el convenio de trasferencia automatizada de datos. Se acaba –en definitiva– diciendo que hay que garantizar el mismo nivel de protección adecuado en el seno de la Unión Europea que fuera de la Unión Europea. La Comisión tiene que apreciar si con los datos jurídicos que se le han facilitado, con las prácticas de los Estados destinatarios (EE. UU), se puede verificar cuál es su régimen de seguridad nacional, cuál es su régimen de legislación, su régimen jurisprudencial, y concluir sobre cuál es el grado de respeto que se produce a los derechos y libertades fundamentales europeos en EE. UU. Y, en concreto, concluye el Tribunal que la Comisión –en este caso con-

creto–, analizando tanto en el anexo primero de la Decisión 2000/520 que hace referencia al "puerto seguro", como en el anexo segundo, que hace referencia a las *Frequently Asked Questions* (es decir, el Tribunal llevando a cabo un análisis un poco abstracto, tratando de no entrar en cuál es el grado concreto en que Estados Unidos tiene acceso a esa información), dice: oiga, no sabemos si Estados Unidos tiene el mismo grado de protección que nosotros los europeos. No tenemos constatación de cuáles son las garantías que se proveen en Estados Unidos en la recepción y el tratamiento de los datos provenientes de Europa. Desconocemos cuál es la utilización que se lleva a cabo por las autoridades de seguridad nacional americanas, o cómo opera la ponderación del interés público que permite estas autorizaciones explícitas de acceso por parte de la NSA. En definitiva –dice el Tribunal–, no tenemos conocimiento de cuáles sean las reglas de Estados Unidos destinadas a limitar las injerencias, y a proteger los derechos y libertades, y –en conclusión, dice el Tribunal– tenemos que considerar que se está llevando a cabo una injerencia en el derecho a la intimidad, que se está llevando a cabo una injerencia en el derecho a la protección de datos, y que no nos constan garantías suficientes. Por lo cual –concluye el Tribunal– tenemos que pronunciarnos en el sentido de que, *a priori*, dado que alguien –un ciudadano europeo– nos ha puesto de manifiesto una sospecha, tras el debido análisis, no percibimos que las garantías de protección en la utilización de los datos sean suficientes. Pero es que, además, luego hay una evidencia incontestable: que la propia Comisión, al haber dictado dos decisiones en 2013, en las que decía que tenía sospechas de que la recogida y tratamiento de datos a gran escala en Estados Unidos estaba infringiendo los derechos fundamentales, que las empresas de Estados Unidos, de programas de vigilancia, aun estando certificadas con "puerto seguro", no lo cumplía. El Tribunal añade que, a pesar de que se tiene que mejorar el régimen del "puerto seguro", las excepciones, los motivos de seguridad nacional siguen prevaleciendo que el puerto seguro al final se ha convertido en una interfaz para la transferencia de datos a las autoridades de seguridad americanas. Es decir, si en dos comunicaciones, las COM (2013) 846 final y 847 final, la Comisión está reconociendo que hay infracciones, en este análisis cautelar, el Tribunal concluye diciendo que *a priori* podrían producirse infracciones; viene a constatar por la propia actividad de la Comisión en sus dos comunicaciones de 2013, 846 final y 847 final, que se reconoce que Estados Unidos infringe de modo sistemático. Y el Tribunal tiene el recelo de proteger los derechos y libertades.

En definitiva, se acaba diciendo –a mayor abundamiento– que no existe ninguna posibilidad de control por parte de las autoridades de certificación de los Estados miembros de la UE. No existe ninguna posibilidad de fiscalización, por lo tanto, lo más sencillo es confirmar que se ha producido una infracción de los derechos y libertades a la intimidad y a la protección de datos en la adopción de esta Decisión 2000/520, y lleva a cabo una anulación de la Decisión 2000/520 de la Comisión.

¿Cuáles son las conclusiones que yo extraería de estas sentencias que les he expuesto, y ya entrando en el ámbito de la libertad religiosa? Porque claro, al final, aquí les he contado un rollo –como decía Paco Umbral: "*¡Yo he venido a hablar de mi libro!*"–, pero qué podemos sacar en claro de lo expuesto.

Como primera reflexión, como consecuencia de todas estas resoluciones judiciales se ha producido un nuevo reglamento comunitario para la protección de datos. Un nuevo Reglamento 2016/679 que, en los puntos 4, 55, 71 y 75 de su exposición de motivos, contiene menciones a la libertad religiosa, y donde expresamente, respecto al tratamiento de datos personales, se recoge, por ejemplo, en el artículo 9. 1, que

> "*queda prohibido en el tratamiento de datos que se revele el origen étnico, racial, ideas políticas, convicciones religiosas o filosóficas, o la afiliación sindical; y queda prohibido el tratamiento de datos genéricos, datos biométricos, dirigidos a identificar de manera unívoca la persona física, su salud; u otros datos relativos a la vida sexual, o la orientación sexual de la persona*".

Y en este artículo 9.2 del nuevo Reglamento 2016/679 se recoge que "*no será de aplicación, es decir, los motivos de oposición anteriores no serán de aplicación*"; y en la letra d), del apartado 2, dice:

> "*el tratamiento es autorizado cuando sea efectuado en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos, o a personas que mantengan contactos regulares con ellos en relación con sus fines, y siempre que los datos personales no se comuniquen fuera de dichas entidades sin el consentimiento de los interesados*".

Y, por otra parte, el artículo 91 del Reglamento 2016/679 nos expresa, como normas específicas, las normas vigentes sobre protección de datos de las iglesias, y asociaciones religiosas:

> "*Cuando en un Estado miembro, las iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente reglamento, apliquen un conjunto de normas relativas a la protección de las personas físicas, en lo que respecta al tratamiento de tales datos, podrán seguir aplicándose las anteriores normas, siempre que sean conformes con el presente reglamento*".

Y el punto 2 de este artículo 91 dice: "*las iglesias y asociaciones religiosas que apliquen las normas generales, de conformidad con el apartado 1 del presente artículo*" (es decir, las normas anteriores), "*estarán sujetas al control de la autoridad*", al control independiente, "*que podrá ser específica, siempre que cumpla con las condiciones establecidas en el capítulo 6*" (el capítulo 6, sección 1.ª, artículos 51 y 52, se refieren a las condiciones de autoridad de control, de control independiente, cuál es su ámbito, su establecimiento, sus poderes, las funciones, etc.).

Y existe también otra disposición, es una directiva posterior, que es la directiva para la investigación, Directiva 2016/680 para la protección de las personas físicas en el tratamiento de datos personales por parte de las autoridades competentes con fines de prevención, investigación y detección de infracciones penales (cuya versión anterior también resultó modificada y anulada como consecuencia de estas sentencias que he mencionado), la cual distingue el tratamiento de datos, por categorías especiales. En el artículo 10 distingue en el tratamiento de datos personales, en función de si tienen "*un origen étnico o racial, si contienen opiniones políticas, convicciones religiosas o filosóficas*"; y siempre y cuando "*se adopten las salvaguardias previstas por el derecho de la Unión Europea*", que "*el tratamiento sea necesario para satisfacer los intereses vitales*", y que "*los datos que se hayan hecho manifiestamente públicos*", en cuyo caso sí que se puede dar acceso.

Por lo tanto, con este nuevo régimen, cuáles son las conclusiones que yo extraigo respecto del tratamiento de datos en el ámbito religioso, por impacto de la Sentencia Schrems. Pues, en primer lugar, que en el Reglamento 2016/679, el nuevo reglamento de protección de datos, está claro que en el artículo 91.2 se establece una posibilidad de una autoridad de control independiente; es decir, la Iglesia católica española podría plantearse tener su propia autoridad de control, o

que las otras iglesias o confesiones podrían plantearse tener sus propias autoridades de control, y esto es un tema por regular en España. Si tu antigua Subdirección de Asuntos Religiosos del Ministerio de Justicia de España, donde trabajó don Ricardo García, tuviese que asumir esta competencia de supervisión…, pues resultaría una importante cuestión que analizar y reflexionar, pero que analizar en el marco de la Sentencia *Weltinmmo*. Es decir, que las autoridades de control ministeriales españolas tendrían competencia para supervisar, pero como en el caso entre Hungría y Eslovaquia en el caso *Weltinmmo*, si el establecimiento estaba en Eslovaquia, respecto del tratamiento de datos en Hungría, se dijo en *Weltinmmo* que la autoridad húngara solo podría supervisar, pero no podría imponer multas, porque esto correspondía a la autoridad eslovaca. Pues este es un tema interesante, porque si la autoridad de supervisión específica, para entidades religiosas en España, se viese en la tesitura de que –normalmente– las entidades religiosas tienen ámbito extraterritorial (porque la religión y la Iglesia tienen una dimensión universal, tienen vocación de proyección universal), resultaría que –según *Weltinmmo*– no tendrían capacidad para imponer sanciones. Esta es mi pregunta, y a lo mejor hay que reflexionar sobre cuál sería la capacidad para imponer sanciones extraterritoriales, porque en la Sentencia Schrems parecía que sí que existía dicha posibilidad, pero la Sentencia *Weltinmmo*, que es más reciente, parece que hay una restricción, y parece que le "mete ahí un tajo" a lo que es la protección extraterritorial, a la protección de derechos fundamentales relacionados con la protección de datos, en el ámbito internacional.

Mi segunda conclusión versa sobre el Reglamento 2016/679, pues este mismo reglamento, en el artículo 9.2, dice que, en el tratamiento de los datos de categorías especiales, estos pueden ser objeto de tratamiento (de datos). Aquí me surge una duda: ¿qué pasaría respecto a los antiguos miembros de confesiones o antiguos miembros de institutos religiosos? ¿Existe, o no, un derecho a protección de sus datos personales respecto de la asociación u organismo religioso al que han pertenecido? Porque aquí ya no estamos –yo creo que hay un matiz–, ahora no estamos en el caso de los registros parroquiales, respecto de los apóstatas, que se consideró que eran registros de "valor histórico o científico", o incluso "a efectos estadísticos". Aquí ya estaríamos en un supuesto en el que se produce, efectivamente, un tratamiento de datos, y –claro– la Sentencia *Google Spain* (que es esta que les presentaba al comienzo), en principio parece que reconoce el "derecho al olvido", con lo cual, si se lleva a cabo esta recopilación de datos,

tiene que reconocerse los correspondientes derechos al tratamiento de datos, con las fórmulas de "rectificación" y "conservación", y los derechos de "oposición", y evidentemente, este nuevo derecho que es el "derecho al olvido".

Mi tercera conclusión versa sobre el marco de la libertad religiosa, también en ámbito del Reglamento 2016/679, respecto de las transferencias de datos a países u organizaciones internacionales, esto es, la transferencia de datos a la Santa Sede por parte de la Iglesia católica. Las sentencias *Digital Rights* y *Schrems* dicen que cuál es el grado de control que se puede efectuar, aunque sea para persecución de delitos. Si hacemos un paralelismo entre Estados Unidos, como equivalente a la Santa Sede y, por otra parte, la Comisión Europea, que en el caso Schrems había autorizado esa trasferencia de datos. Si el Concordato de España y la Santa Sede (y pido perdón a los oyentes que pertenecen a otras confesiones religiosas, sin perjuicio de que creo que –al final– les afecta igual, porque casi todas las confesiones tienen un convenio con el Estado español), ¿qué es lo que sucede si la transferencia de datos por una iglesia o confesión se lleva a cabo fuera de la Unión Europea?, ¿cuál es el grado de control? Y si, en el caso de la Iglesia católica, ¿el Concordato del 79 no previó en los acuerdos jurídicos disposición alguna respecto de la transferencia de datos?, pues a lo mejor hay que reflexionar en el seno de la Iglesia católica española (porque sabemos que hay gente que quiere poner en tela de juicio y en jaque el Concordato del 79). Pues a lo mejor la Santa Sede, quien sí que tiene la capacidad de negociar con la Comisión Europea, debe alcanzar un convenio –como hemos visto que hizo Estados Unidos, en el Caso Schrems– cara a transferencia de datos, y así quedar cubierto el panorama y el aspecto de las eventuales reclamaciones sobre protección de datos personales de fieles o exmiembros de asociaciones religiosas.

O sea, que las cuestiones que en la jurisprudencia del TJUE –que les he expuesto inicialmente– parecían un poco etéreas o hipotéticas, y que parecía que yo les estaba citando inocentemente, pues resulta que ¡no era tan inocente la referencia! Es innegable que de aquellas sentencias uno puede extraer consecuencias respecto a la libertad religiosa, en su aspecto organizativo, en su vertiente colectiva o aspecto organizativo, como confesiones religiosas, en relación con la protección de datos de los miembros de la confesión religiosa y en relación con la protección de datos de las propias confesiones.

Estas son –un poco– las preguntas que yo quería dejar aquí en el aire, para no aburrirles mucho más.

Quiero agradecerles la paciencia y atención que han tenido para escucharme sobre estas cuestiones jurisprudenciales (que yo entiendo que son un poco pesadas, si uno no las vive en primera persona –¡incluso para mí ocasionalmente son algo pesadas! –), pero creo que les ponen muy de relieve cómo se lleva a cabo la actividad jurisdiccional que se desarrolla en Luxemburgo. No se trata simplemente de un ejercicio de especulación jurisdiccional o de "piruetas jurídicas" carentes de interés o virtualidad concreta para los ciudadanos. Sino que, realmente, sí que las sentencias de Luxemburgo tienen sus consecuencias, que se perciben porque la mayoría de los casos, como *Digital Rigths*, o *Schrems*, han dado pie a dos cuestiones sustanciales, como son, primero, la de que *Facebook*, o *Google Search*, que son mecanismos o herramientas que empleamos a diario, deben garantizar la protección de datos, de nuestros datos, en ese ámbito; y segundo se nos plantean muchos interrogantes, muchas cuestiones jurídicas que debemos resolver específicamente para el ámbito de la libertad religiosa.

Turno de preguntas

1.ª pregunta:

Yo quería preguntar si en el caso de los ataques a la libertad religiosa en redes sociales como Twitter, donde prima el anonimato, se ha legislado, se ha estudiado cómo se puede parar esto o cómo se puede legislar este asunto.

Ponente:

Yo creo que no existe una regulación específica. Desde luego, a nivel europeo siempre se puede invocar la protección equivalente a la libertad religiosa existente a nivel nacional, pero el desarrollo normativo por parte de la Unión Europea con respecto a la libertad religiosa, que se recoge en los artículos 17 y 18 de la Carta de los Derechos Fundamentales UE, pues no se ha llevado a cabo en el ordenamiento comunitario. Y en este sentido, si tu invocas simplemente la libertad religiosa como digna de protección, para solicitar un acceso a determinada información, que es confidencial, como es la de Twitter, pues es muy poco probable que en el marco europeo –a estas alturas– encuentres una directiva que te habilite o permita dicho acceso, ni incluso el reglamento que te habilite. Sin embargo, si lo personalizas, si tú dices: oiga, se me ha lastimado en mi credo, o se me han lesionado

mis sentimientos religiosos, creo que ahí ya cambiaría mucho la efectividad de la protección. Lo que sí creo es que en el ámbito interno está debidamente protegido el derecho a la libertad religiosa y a la intimidad, lo que pasa es que ahí, en ese ámbito nacional, la efectividad de la protección depende siempre del valor, el coraje y la percepción que tenga –muchas veces– el receptor de tu denuncia, tanto en las entidades (porque uno tiene que proceder con carácter previo a denunciar ante la policía, y la policía puede considerar "*pues mira, esto no va a prosperar*", o incluso "*puede llegar al juzgado*"), como por el juez, que diga: "*¿Cómo voy a llevar a cabo yo una injerencia en el derecho a la intimidad para proteger tu libertad o tu sentimiento religioso?*". Pero lo que sí que es cierto –y yo insisto, sin perjuicio del principio de intervención mínima– es que los delitos contra los sentimientos religiosos siguen estando en el título XXI del Código Penal; la blasfemia no. Pero *la persona que hace escarnio a las creencias religiosas*, igual que *la persona que profana tumbas*, son delitos que siguen estando ahí tipificados, y yo creo que tienen que tener su virtualidad. Otra cosa es que las medidas cautelares que uno pida cuando presenta una querella por la comisión de delitos contra la libertad de conciencia, o cuando presenta la denuncia a la policía, y solicite como medida cautelar, o como medida de investigación, la medida de embargo o secuestro de la difusión de ese tuit, y solicita que se tenga acceso a los datos de esa persona presuntamente infractora, pues te tienes que encontrar con jueces muy valientes, que sean capaces de afrontar eso, no como una lesión a un determinado credo, sino como una lesión a la convivencia. Porque yo estoy convencido de que, al final, esos delitos contra la libertad de conciencia y sentimientos religiosos, cuando se introdujeron en el Código Penal, no se tipificaron simplemente porque considerábamos muy digno el valor jurídico de la protección a la religión, sino porque la protección a la religión es una garantía de la convivencia pacífica, y en ese sentido estoy de acuerdo con la exposición y advertencia que han llevado el cardenal Cañizares y a don Ignacio Sánchez Cámara. ¡Mucho ojo con lo que estamos haciendo!, porque en sí resulta que hay un tratamiento asimétrico, totalmente dispar, en función del bien jurídico protegido y de quien lo invoca; con esa discriminación de trato en función del derecho fundamental y quien lo invoca corremos el riesgo de que al final se pierda la paz social.

Yo creo que la garantía constitucional de la seguridad jurídica implica que cualquier persona que presenta una querella tiene derecho a que esa querella se investigue y que se practiquen diligencias de investigación, porque esas diligen-

cias van encaminadas al descubrimiento del autor de los hechos y de la entidad criminal del hecho. Entonces, si resulta que, *porque los jueces tenemos mucho trabajo*, o *porque tenemos una percepción subjetiva*, no llevamos a cabo esa labor de investigación liminar, creo que no estamos contribuyendo en nada a la convivencia pacífica. Y lo digo en primera persona, porque al final también soy un juez nacional, aunque ahora esté en otra jurisdicción.

En resumen, no existe un mecanismo de protección de la libertad religiosa a nivel de la Unión Europea.

2.ª pregunta:

Yo quería preguntar la situación que estamos viviendo en estos momentos de listados públicos, de maltratadores, de defraudadores, que en el fondo vemos claramente que sin procedimientos finalizados, hay la figura del presunto –entre comillas– culpable, ¿en qué medida las nuevas tecnologías están abundando en esa idea tan tenebrosa en la que ya no hay igualdad plena ante la ley, en que la presunción de inocencia queda disipada?, y, por otra parte, ¿en qué medida –pues– la inseguridad, la falta de convicción, también de no pocos profesiones de su ramo hacen asimismo que en determinadas cuestiones, igualmente de origen atinente a la libertad religiosa, se quedan muchas veces en la imprecisión y, por qué no decirlo –pues–, en la desidia, en la dejación de funciones, generando –como no podía ser menos– una profunda incertidumbre para todos? Eso es lo que quería trasladar.

Ponente:

Con respecto al tema los listados, para mí es una paradoja, porque una sociedad que está preconizando la importancia de los derechos individuales reconoce también que todo derecho individual se encuadra en una vertiente social. Nuestros derechos no solo se ejercitan, se ejercitan en el medio social. Pero sí es una paradoja que se esté tratando de proteger tanto a la intimidad, o a la protección de datos, y que luego no se tenga tanto reparo, ni tanta cautela, cara a la publicación de listados con el efecto lesivo multiplicador. El efecto multiplicador cara al impacto individual. Al final, no es que simplemente publiquen en el tablón oficial del Ayuntamiento, como se hacía antiguamente en los edictos, de que tienes una deuda, sino que el problema es que eso ahora se publica en una página

web, que tiene acceso universal, a la que un motor de búsqueda o varios motores de búsqueda tienen acceso, y automáticamente el grado de trascendencia en la información que ahí se ha divulgado se multiplica, porque estamos en la "sociedad de la información". Entonces internet resulta una herramienta de comunicación "brutal", que expande y multiplica a la exponencial cualquier información y cualquier contenido lesivo.

Bueno, pues la sociedad de la información es muy beneficiosa, es un medio de comunicación y divulgación extraordinario; pero hay que analizar también hasta qué punto, si no se introducen algunos mecanismos de contrapeso y equilibrio, como consejos reguladores auténticos, consejos participados por estas entidades y por entidades públicas de autorregulación, con sanciones efectivas, ¡a la primera!, es decir cautelarmente: usted, autoridad, sanciona, y luego recurra usted administrado (que es la posición fuerte, porque así se ha producido en muchos ámbitos, como en el de la contratación). En todos los ámbitos de la contratación, para protección del consumidor, no se duda en disminuir la carga de la prueba y decirle al banco acreedor: "Oiga usted, provea la prueba de que no se ha lesionado el derecho del consumidor". Sin embargo, en materia de protección de datos, no se ha alcanzado todavía esa inversión de la carga probatoria. Y yo creo que ahí el Estado tiene que reaccionar, y tiene que darse cuenta de que "la información siempre ha sido poder", pero que el poder puede ser absoluto, y que realmente, cuando este nuevo poder le esté causando al ciudadano un impacto de deterioro en su imagen, o simplemente –ya no hablo de que se proyecte la imagen–, sino que el ciudadano quiera realmente –o no quiera– la divulgación de la información que le concierne. Verán, yo pasé un año por la política, y todavía, cuando voy a buscar en Google alguna cosa con mi nombre, me quedo asustado de las cosas que salen sobre mí, porque –saben–, según Google, yo pertenezco a *Los Genoveses* –que no sé quiénes son–, pero parecen ser unos señores que hay por ahí, súper siniestros. Y yo me dirijo a Google y le solicito que rectifique mi información. Y me contesta: "No, usted es un personaje público, usted no tiene derecho a que le rectifiquemos su información".

Entonces, son cosas que uno tiene que reflexionar, y ya vuelvo a la primera parte de su pregunta, y estimo que también el Estado tiene un "deber de diligencia" y "el deber de tutela" con respeto a los derechos y libertades de los ciudadanos, y si el Estado tiene constancia de que se está produciendo una vulneración indiscriminada y masiva de los derechos, y no introduce ningún tipo de super-

visión, o que la supervisión se lleva a cabo *ex post*, pues yo creo que tiene que pensarse que, por muy malo que haya sido el crimen, no tiene que divulgarse. Los antecedentes penales siempre los hemos tenido a disposición judicial. Los antecedentes de Hacienda también; lo que no tiene es que estigmatizarse. ¿Es que somos mejores como sociedad si linchamos a la gente mala, por muy mala, por muy grave que haya sido la infracción que se haya cometido? ¿Es que somos mejores cuando metemos a Mario Conde en la lista de morosos de Hacienda, como el *number one*?, y ¿no estamos entonces nosotros –todos– haciendo murmuración o comidilla de eso? Yo no creo que, dentro de lo que es la tutela de los derechos y libertades, al proponer esos listados se estuviese ulteriormente pensando –o persiguiendo– producir ese efecto lesivo reflejo. Y creo que la Administración tiene un "deber de diligencia", y un deber de diligencia serio respecto a la tutela de los derechos y libertades.

Y entonces esto es una cosa sobre la cual hay que reflexionar, para ver cuáles son las medidas que se adoptan. Porque si los listados pueden ser muy eficaces, por ejemplo, cara al cobro del crédito de los morosos, ¿hasta qué punto se encuentra dentro de los principios constitucionales, como cara a la reeducación y reinserción social del criminal, la publicación de los datos de los criminales, incluso no –presuntos– como en el mundo anglosajón, la lista de agresores sexuales (que eso, en el mundo anglosajón, lo hacían particulares, asociaciones de víctimas, etc.,)? Pero es que debemos tener en cuenta que, en España, los listados los hace el Estado, y hace público directamente datos de determinas personas (mucho más allá del registro central de penados y rebeldes). Yo creo que son cuestiones para reflexionar colectivamente.

3.ª pregunta:

Una última pregunta más, dos últimas preguntas más, y yo no me resisto a hacer una pregunta al ponente. La pregunta que le quiero hacer al ponente es que, en ocasiones, podemos entrar en contenidos; hemos hablado de *Google*, pero hoy nuestros alumnos en esta Facultad de Derecho, y muchos usuarios de la red, por llamarlos así, utilizan algunas aplicaciones muy conocidas, como puede ser *YouTube*. Si entras en *YouTube* puedes ver vídeos, que están grabados hace años, y es fácil encontrar vídeos que contienen ataques contra iglesias evangélicas, contra mezquitas musulmanas, donde aparece la reproducción –que está

prohibida como tal– de Mahoma, o podemos encontrar ataques contra la Iglesia católica. Tal es el caso, por ejemplo, me viene a la cabeza, de un supuesto que ha sido respondido hace poco, me parece que por un juzgado de Sevilla, con un auto de archivo de una querella por un derecho de reunión y manifestación, que tendremos ocasión de ver durante el curso. Pero no me resisto a hacer una pregunta muy concreta. ¿Existe el "derecho al olvido" cuando están hablando sobre una de manera indirecta? Quiero decir, el problema que tiene que mañana salga en un periódico publicada –con todo el respeto para los compañeros de la comunidad musulmana– una viñeta de Mahoma, es que el periódico es en formato papel y el tiempo lo va poniendo amarillo –y aquí en Valencia con el sol más–. Pero si esto lo tenemos en Internet, eso se puede ir no solo con el efecto multiplicador que bien decía, sino qué queda, y al contrario tiene un *lifting* diario, de tal forma que cuando entras en la aplicación no sabes si ha ocurrido ayer o ha ocurrido hace diez años, o, en fin, ¿ahí existe el "derecho al olvido" de *Google*? Yo, si fuera musulmán, puedo pedir a *Google* que retire esa imagen porque está hiriendo mi conciencia, o si fuera católico, puedo pedir que el vídeo de la manifestación aquella por Málaga sea retirado de la red, aunque un juzgado haya dicho que no es un delito, pero sí reconoce el propio auto que es ofensivo.

Ponente:

La pregunta es acertada, y es difícil de contestar, porque tiene un alto componente de sentido común y de razonamiento. Así, yo entiendo que estamos en presencia de lo que se denominaba *delitos permanentes*, aquello que estudiábamos en la oposición en Derecho Penal como el delito en el que, mientras perseverara la actitud del sujeto activo, se seguiría lesionando el bien jurídico.

Entonces, al final –desde luego– se me suscita, si hacemos abstracción –siempre– del campo en el cual se encuentran los intereses en conflicto, y los derechos fundamentales en conflicto, los podemos ponderar en tanto que sean impersonales. Decimos, así en abstracto, esto es un conflicto entre la libertad de expresión e información, y el hecho de que se haya producido un hecho noticiable, o que haya sido noticiable (pues primero es noticiable, y después pasa a hecho histórico). Entonces revestiría algún tipo de interés en la libertad de información, existiría.

Sin embargo, por otro lado, los derechos individuales, o su derecho a sus sentimientos religiosos –como siempre podemos decir– son derechos "más prio-

ritarios" –o derechos "menos prioritarios"–; pero yo creo que cuando te pones a analizar los conflictos entre derechos fundamentales, necesariamente uno tiene que tener en cuenta que no se puede singularizar, porque el derecho a la libertad informativa es un derecho únicamente instrumental, o de herramienta para la construcción de la sociedad democrática plural (los medios de información); pero el derecho que realmente entra en juego es única y exclusivamente mi derecho a los sentimientos religiosos, o también es mi derecho a no ser herido, o también mi derecho a la intimidad, y al ulteriormente mi derecho a la convivencia pacífica. Porque yo creo que en la ponderación debe realzarse *in concreto* y tiene que salir a relucir realmente cuál es el alcance y la trascendencia de cada uno de los derechos y libertades en juego. Yo –en ese sentido– siempre he tenido una concepción liberal –y a lo mejor individualista– del origen de los derechos fundamentales. La sociedad se constituye por la suma de individuos y nuestros derechos individuales son, cada uno de ellos, los que construyen los derechos sociales y la sociedad. No puede haber ningún derecho social –y menos aún instrumental– que, entre comillas, prevalezca sobre los derechos individuales, sobre la vida y la libertad individual. A mi modo de ver, no puede haber nada de eso.

Te pueden decir, "*es que la libertad de expresión es una vertiente de la libertad*". Sí y no. También la libertad de ambulatoria es una variante de la libertad, pero si estás en la cárcel, no hay libertad.

Creo que en la libertad de expresión lo primero que habría que confiar es en la autorregulación y en la deontología profesional de los periodistas. Lo segundo, habría que confiar también –aunque no sé si es mucha confianza– en la libertad, y en la competencia o capacidad profesional de las propias empresas de medios de comunicación, y de las empresas de difusión –de lo que tú, Ricardo García, dices de YouTube, de Google–. Aquí, en España, tiene que abrirse una reflexión por parte de estas entidades, porque no puede seguir publicándose datos *como un pollo sin cabeza*, como mi objetivo es publicar y vender, pues todo vale y se publica. ¡Tiene que haber algún código o algún límite!, porque nosotros, nuestra sociedad, erróneamente, parte de que la libertad de información es una libertad absoluta –y eso lo digo así de claro–. Lo ha dicho la jurisprudencia del Tribunal Constitucional, la del Tribunal de los Derechos Humanos de Estrasburgo. Pero será en la medida en que los derechos fundamentales no lesionen los derechos y libertades de los demás, que se puedan ejercer. Pero, cuando se comienzan a lesionar indiferenciadamente los derechos y libertades de los demás, tenemos un

problema como sociedad, porque al final esa injerencia puede acabar rompiendo la convivencia pacífica. Por eso insisto en que incluso la libertad de información no es un derecho absoluto, y se tiene que ponderar hasta qué punto, cuando lleva a cabo una divulgación ofensiva, no están lesionando los derechos de muchas personas como individuos, que sumando componen una colectividad, que tienen una forma de pensar, y que para ellos las creencias son una cosa seria. Porque hay gente que dice, como Groucho Marx: "*Estos son mis principios, pero si no le gustan los cambios ahora mismo, tengo otros*". Pero también hay mucha gente que no es así, hay gente que vive coherentemente con sus principios, y hay que saberles respetar. Yo lo que no entiendo es por qué, para informar, tengo que lesionar los derechos y libertades de los demás. Entonces, creo personalmente que este es un canon que hay que meterlo en algún sitio en la Constitución. Porque está ahí en los convenios internacionales, está en jurisprudencia constitucional, y sin embargo ¡no se utiliza!

4.ª pregunta:

Me ha parecido muy interesante el planteamiento que ha hecho cuando, en un supuesto de renegociación de los acuerdos con la Santa Sede, el dar protagonismo es una forma de solucionar este problema, sería al dar protagonismo a la Santa Sede como actor negociador de estos acuerdos. Me gustaría saber si ese supuesto se daba antes de la existencia, en el caso de España, de la Conferencia Episcopal. Pero la pregunta es cómo gestionar este supuesto, en el caso de que actualmente existe en España una Conferencia Episcopal. Cómo la Santa Sede podría gestionar este protagonismo en la negociación de unos acuerdos.

Ponente:

La Santa Sede, cuando tiene que negociar un convenio internacional, lo hace como Estado y a nivel universal. Cuando anteriormente intentaba establecer ese paralelismo que existe entre el convenio entre EE. UU. y la Comisión que da lugar a la Decisión 2000/520, si resulta que los acuerdos entre España y la Santa Sede (pienso en voz alta: ¡mejor no tocarlos!, porque tal y como está el panorama en este país puede suceder cualquier cosa), nadie puede privar a la Santa Sede de su legitimidad internacional como Estado y como organismo de derecho internacional, de negociar con la Comisión Europea, todo un régimen jurídico

en materia de protección de datos respecto de los católicos, en cada uno de los Estados miembros de la Unión Europea.

Otra cosa es que esto tiene una limitación: no sé hasta qué punto la Santa Sede podría negociar con la Comisión respecto a los Estados con católicos de África, pero incluso puede ser que quede abierta esa posibilidad… Lo que parece ser es que el nuevo Reglamento 2016/679 deja abierta una posibilidad semejante, indudablemente respecto a los Estados miembros. Esa posibilidad de negociar directamente de la Santa Sede, y de que la Santa Sede establezca cuál va a ser el régimen de comunicación de transferencia de datos y de tratamiento de datos por parte de las entidades que dependen de la Santa Sede (Iglesia y órdenes e institutos religiosos), son en definitiva la confesión religiosa católica en España, en Italia e incluso a nivel global. Lo que no sé es si, a lo mejor, es más duro para la santa Sede negociar con los eurócratas que negociar en bilateral con el Gobierno de España. Eso también es una cuestión de discrecionalidad de los negociadores; pero sí que existe esa posibilidad, y además es que aparece expresamente prevista en el Reglamento 2016/679. Me parece que era el artículo 51 el que reconocía el estatuto de las confesiones religiosas que tuvieran propiamente reconocido un régimen jurídico en cada uno de los Estados miembros; y el principio de cooperación también lo implicaba a través de otros artículos, me parece, de la propia Carta de Derechos Fundamentales de la UE.