LOS RETOS DE LA PROTECCIÓN DE DATOS EN INTERNET. CASO GOOGLE SPAIN Y DERECHO AL OLVIDO (1)

Diego CÓRDOBA CASTROVERDE*

Resumen

Los riesgos a la privacidad de las personas físicas en el entorno digital se han multiplicado, surgiendo nuevos problemas que no aparecen directamente relacionados con la protección del honor o la intimidad sino con el control de los datos personales de las personas físicas y de la información que estos proporcionan sobre sus personas, sus gustos y actividades.

La tutela opera no solo frente a las autoridades públicas sino también frente a particulares.

La protección de datos adquiere una dimensión distinta en un entorno digital. Se presentan nuevos retos derivados del medio en que estas lesiones se producen que inciden sobre aspectos tan diversos como al ámbito territorial de protección y su tutela judicial o la creación de perfiles de los usuarios.

Ha surgido el llamado «derecho al olvido» que ha de ser ponderado de forma diferente en relación con los agentes que actúan en internet y el perjuicio que su actividad genera. En la ponderación de este derecho con otros intereses y derechos enfrentados ha contribuido de forma decisiva la jurisprudencia dictada por el TJUE y su aplicación a los casos concretos realizada por el Tribunal Supremo y otros tribunales nacionales, proporcionando pautas y criterios de ponderación en los que se distingue entre la permanencia de la información en la fuente de origen y su localización e indexación por los motores de búsqueda que operan en internet.

Palabras clave

Protección de datos. Derecho al olvido. Eficacia horizontal de los derechos fundamentales. Criterios de ponderación.

Abstract

The risks towards natural persons in the digital environment have multiplied. New issues are emerging that do not appear directly related to the protection of honour or priva-

(1) Conferencia pronunciada en la Facultad de Derecho de la Universidad Autónoma de Madrid. XXI Jornadas del Anuario de la Facultad de Derecho: «Los derechos fundamentales en las relaciones entre particulares».

* Magistrado de la Sala Tercera del Tribunal Supremo.

cy, but with the control of personal data and the personal information provided, such as tastes and activites.

The judicial protection operates not only before public authorities but also before individuals.

Data protection acquires a different dimension in a digital environment. New challenges deriving from the way in which harm is produced are presented. These challenges have a bearing on aspects as diverse as the territorial scope of protection and its judicial protection, or the creation of users' profiles.

The so-called «right to be forgotten» has emerged, and it must be balanced in different ways in relation to the agents acting on the Internet and the harm its activities cause. In the balancing of this right with other interests and rights, there has been a significant contribution from the CJEU's jurisprudence and its application to concrete cases done by the Supreme Court and other national courts. These courts have provided with guidance and balancing criteria that distinguish between the permanence of information in the originating source and its location and indexation by Internet search engines.

Key words

Data Protection. Right to be forgotten. Horizontal effectiveness of human rights. Weighing criteria.

I. **INTRODUCCIÓN**

La protección de datos es un caso típico de eficacia horizontal de los derechos fundamentales de la Unión incidiendo, aunque no solo, en las relaciones jurídicas entre particulares.

Sentada esta apreciación inicial, el análisis de esta cuestión exige hacer algunas consideraciones sobre los riesgos que representa en la sociedad actual la privacidad de las personas.

Nos movemos un entorno tecnológico, que asumimos voluntariamente por las enormes ventajas que reporta y del que ya no podemos prescindir, y que, sin embargo, escapa a nuestro control. De modo que tanto en la forma de comunicarse y de relacionarse socialmente o al entablar relaciones comerciales «on line» no ejercemos un control sobre los datos que proporcionamos. La información que un usuario incorpora a internet forma parte de una gran red en la que actúan compañías que operan a nivel mundial con una tecnología que dificulta enormemente el control de los datos personales que se incorporan.

El uso de las nuevas tecnologías y la existencia de compañías que operan a nivel global con diferentes emplazamientos, y con la posibilidad de modificar su sede con gran facilidad determina que la protección a nivel nacional haya dejado de ser efectiva frente a ellas. Por otra parte, los Estados también pueden hacer uso de esta información con diferentes objetivos, no siempre lícitos pero difícilmente controlables.

La protección del ciudadano frente a tales riesgos ha dejado de ser un problema que pueda ser abordado por las autoridades de un país, pues la comunicación ha pasado a ser global y transfronteriza, de forma que los riesgos a la privacidad de las personas ha de ser abordado de forma mucho más amplia y compleja que dificulta la labor de los juristas.

En este contexto se observa, sin embargo, que los estándares de privacidad existentes en la sociedad actual han cambiado, apreciándose tendencias contradictorias en sí mismas que plantean varias paradojas:

A. PRIVACIDAD *VERSUS* DIFUSIÓN VOLUNTARIA DE LA INFORMACIÓN

En la sociedad actual existe una generalizada relajación de lo que debe permanece en la esfera de lo privado, al incorporarse voluntariamente a las redes sociales una gran cantidad de datos e imágenes de la vida privada y de nuestra familia y amigos. Pero, en el otro lado de la balanza, existe una creciente tendencia a solicitar de los organismos públicos y entidades privadas que se supriman datos o acontecimientos relativos a nuestra persona y que sean fácilmente localizables en Internet.

Esta contradicción en la que se desenvuelve nuestra sociedad, se basa en la necesidad de estar conectados y relacionados socialmente a través de las redes sociales pero, al mismo tiempo, intentar preservar dicha información del conocimiento público, especialmente cuando dicha información con el paso del tiempo la consideramos perjudicial para nuestra imagen y puede incidir negativamente en nuestra consideración social y profesional. Así lo que en un momento determinado de nuestras vidas nos puede parecer inocuo o divertido, con el paso del tiempo, y en otro contexto personal o profesional, puede que se vuelva contra nosotros y no deseamos que sea conocido por nuestros conciudadanos.

Pero ¿tenemos una opción real para desvincularnos de las condiciones de privacidad que nos imponen las grandes compañías para hacer uso de sus servicios? Teóricamente sí, pero si ante los riesgos que presenta el tratamiento de nuestros datos personales optásemos por no aceptarlas no podríamos estar conectados a internet y viviríamos en un cierto ostracismo social, lo que nos obliga a confiar

nuestra protección a las normas internas y comunitarias destinadas a regular y limitar el uso de nuestros datos y eventualmente a reclamar la protección de nuestros derechos por vía civil o ante las autoridades públicas encargadas de su tutela.

Es aquí donde surge el llamado «derecho al olvido», que aparece como reacción frente a las nuevas tecnologías, especialmente para evitar que datos e informaciones referidas a nuestra persona puedan ser localizados fácilmente y de forma intemporal por cualquier usuario de la red con una enorme facilidad.

B. PRIVACIDAD VERSUS PUBLICIDAD Y TRANSPARENCIA

En otras muchas ocasiones, la información existente sobre las personas físicas es ajena a su voluntad. Son las Administraciones públicas la que introduce en la red información sobre las personas relacionada por la actividad desplegada por los ciudadanos con la Administración, información que cada vez es mayor. De modo que los jóvenes con una edad inferior a los 25 años y desde luego las generaciones futuras tendrán su vida reflejada en internet.

Y aquí se produce la segunda paradoja entre privacidad versus publicidad/ transparencia.

La publicidad y la transparencia son pilares básicos de la actuación pública al contribuir de forma decisiva a evitar la arbitrariedad y permitir un adecuado control por parte de los ciudadanos sobre la Administración pública y sobre la actuación de la justicia, que contribuye, sin duda, a mejorar la posibilidad de ejercer un mejor control por el ciudadano.

Casi todos los países de la Unión Europea tienen una ley que regula la transparencia de la actividad pública y trata de garantizar el acceso a la información de los ciudadanos (2), y suelen hacerlo en términos muy generosos por entender que la transparencia de la actividad pública es un valor democrático y contribuye a un mejor control de los poderes públicos y sus funcionarios. Por otra parte, la Carta Europea de Derechos Fundamentales configura la transparencia como un derecho fundamental en relación con la información contenida en las instituciones europeas (3), aunque en España no se ha configurado como tal.

El problema surge porque la transparencia puede entrar en conflicto con otros derechos, tales como la protección de los derechos al honor y la intimidad de las personas y muy singularmente con la protección de sus datos personales (4).

---

(2) En España la transparencia se reguló por la Ley 19/2013 de 9 de diciembre.

(3) El art. 42 de la Carta Europea de Derechos Fundamentales regula como un derecho fundamental el «Derecho de acceso a los documentos» afirmando que «Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión».

(4) El Tribunal de Justicia de la Unión Europea, también ha tenido ocasión de conocer esta confrontación entre el interés público consistente en dar publicidad a la asignación de fondos en relación con la protección de datos personales de los afectados en su Sentencia del TJUE de 8 de junio de 2010 (asunto C-55/08) y en la sentencia del TJUE 29 de junio de 2010 (Gran Sala) (Asunto C-139/07Comisión/Technische Glaswerke Ilmenau) en la que se trata el problema del acceso a información y documentos en un proceso contra el Estado por concesión de ayudas comunitarias contrarias al derecho comunitario, o en la sentencia de 29 de junio de 2010 (Asunto C-28/08 P. Comisión/Bavarian Lager) relacionada con un problema de acceso a documentos (principio de buena práctica administrativa) y protección de datos de carácter personal.

II. EL MEDIO TECNOLÓGICO EMPLEADO ¿CAMBIA LA RESPONSABILIDAD Y LA PROTECCIÓN QUE DEBE DISPENSARSE?

A la vista de los problemas que presenta este entorno tecnológico cabe preguntarse si la protección dispensada, y, por ende, sus límites cambian dependiendo del medio de difusión empleado. La pregunta nos la podríamos formular en los siguientes términos: ¿El medio técnico utilizado cambia el alcance y los límites de la protección?

Una primera aproximación permitiría entender que la protección debería ser la misma cualquiera que sea el medio empleado para difundirla. El punto de partida podría ser «no pueden imponerse mayores limitaciones en Internet de las que rigen en el mundo real y, por tanto, no puede considerarse ilegal en Internet lo que es legal fuera de la Red, pues de otro modo /.../ lo único que se consigue es la criminalización de la Red». Ello implica que el uso de un medio determinado carecería, en principio, de relevancia, de modo que el instrumento de difusión tendría un valor estrictamente accesorio.

Pero esta inicial apreciación puede y debe ser matizada:

1. En primer lugar por las propias características del medio empleado y de los agentes que en él actúan.

– La jurisprudencia viene reconociendo como un límite tradicional a los derechos de honor, intimidad y propia imagen, la existencia de un derecho de libertad de información, protección especialmente reforzada cuando es ejercida por los profesionales de la información (los «media» profesionales), en cuanto constituyen un elemento imprescindible para la creación de una sociedad democrática y de una opinión pública libre.

Sin embargo, en Internet un receptor de información puede convertirse en proveedor de información por sí mismo o a través del reenvío de la información realizado por un tercero, quebrándose la clásica relación de alteridad (emisor-receptor) que constituía la esencia de la comunicación hasta el momento.

La realidad actual es que los datos, la información y las opiniones que se incorporan a la red por los particulares es mucho mayor que la que incorporaran los medios de información «profesionales». Estos problemas no han tenido una respuesta clara en nuestra jurisprudencia que sigue anclada en afirmaciones generales referidas a un mundo de comunicación totalmente sobrepasado por la realidad actual de los medios de comunicación.

Por otra parte, la información que se introduce en internet no es autenticada por profesionales ni por un código deontológico y convierten a la red en un cúmulo de datos e información que operan al margen de los medios de comunicación profesionales.

Ello ha motivado que la generación en la red de noticias falsas que se convierten en virales y que tienen visos de credibilidad son difundidas sin un control por las empresas que servicios o proveedores de contenidos sin realizar una criba de autenticidad (por ej: en la reciente campaña electoral americana se difundió la noticia de que el Papa de Roma apoyaba la candidatura de Trump y la noticia se convir-

tió en viral). Ello ha motivado que empresas como Facebook o Google se hayan cuestionado su posición y responsabilidad en la difusión de estas noticias y la posibilidad de ejercer un cierto control de contenidos.

– Internet es un medio independiente en infraestructura y técnicamente compleja, que dota de un protagonismo especial a los «*proveedores de información*» (de servicio o de contenido), y que exige una mayor especificación jurídica a efectos de imputación de responsabilidades (distinción entre edición y distribución e intermediarios).

Con frecuencia las empresas que gestionan motores de búsqueda aducen que ellos no crean la información ni la alteran sino que simplemente la transmiten y la ponen a disposición del usuario de forma sencilla. Pero también esta afirmación puede ser cuestionada porque los algoritmos matemáticos utilizados por dichas compañías detectan, en atención a nuestras consultas y hábitos, nuestras preferencias y pueden seleccionar u ordenar la información en relación con criterios relacionados con ese interés, por lo que se corre el riesgo de que en nuestras búsquedas se nos proporcione una información o unos servicios que operen como cámara de resonancia que reafirme nuestras propias opiniones o gustos desechando o postergando aquellas más alejadas de nuestro pensamiento o forma de ser, con el riesgo de condicionar la información que nos llega por esta vía.

Debe destacarse también que internet es un medio descentralizado o abierto (con múltiples puntos geográficos de acceso), se incrementan las dificultades técnicas y se frustra gran parte de los intentos de un control efectivo –como regla general, las redes electrónicas no permiten la identificación del usuario o del emisor de determinada información– y que plantea enormes dificultades para establecer un control judicial, empezando por determinar el órgano judicial competente para su conocimiento y el sujeto obligado a repararlo, temas que trataré más adelante.

B. DISEÑO DE PERFILES PERSONALES

Internet permite acumular los datos e informaciones, en principio inocuos individualmente considerados, pero que apreciados en su conjunto pueden configurar perfiles de las personas, con una incidencia mucho mayor en la privacidad de las personas. De hecho, no es impensable que informaciones que por sí mismas no atentan contra la intimidad de las personas pero, apreciadas en su conjunto y relacionadas entre sí, nos proporcionen una información completa sobre los gustos, la vida y la actividad de las personas que puede incidir sobre la privacidad de las personas de forma mucho más peligrosa.

Datos e informaciones sobre la infancia, vida académica, profesional o laboral, hábitos de vida, uso del dinero por tarjetas, relaciones personales, gustos y aficiones, incluso sobre las creencias religiosas e ideologías pueden ser fácilmente obtenidos y tratados de forma ordenada con la informática. Las grandes compañías que los manejan pueden conocer así sus actividades, hechos o pautas de comportamiento que pertenecen a la esfera privada de las personas a su privacidad.

La posibilidad de realizar una búsqueda rápida y sencilla toda la información que existe en internet sobre una persona incrementa las posibilidades de crear perfiles de las personas y construir un «historial» de su vida y actividades o de su tra-

yectoria económica o profesional. Y este riesgo no solo existe respecto de personas con proyección pública o mediática sino que afecta a cualquier ciudadano que ve como se incluyen en internet una gran cantidad de datos o informaciones relacionados con su persona que afectan a aspectos cotidianos de su actividad diaria.

C. LA IMPORTANCIA DEL TIEMPO

Un tercer factor decisivo para ponderar la vulneración, es el tiempo transcurrido, factor que hasta hace poco no había sido suficientemente ponderado al tiempo de evaluar la lesión de este derecho.

La información que antes de la aparición de estas nuevas tecnologías tenía una difusión limitada territorial y temporalmente, y que al cabo del tiempo caía en el olvido, en estos momentos puede ser localizada fácilmente y, sobre todo, no se olvida, permanece en la red indefinidamente. Esto supone un peligro añadido y potencialmente muy grave para la privacidad de las personas, pues una información, aun lícita y exacta en su origen, por el transcurso del tiempo puede haber dejado de ser actual al haber sido superada por acontecimientos posteriores que la desvirtúan o minimizan y, sin embargo, cada vez que se teclea el nombre de una persona en un buscador vuelve a recordarse aquel acontecimiento o información relacionado con su persona.

D. LA AMPLITUD DE LA DIFUSIÓN

En la ponderación del derecho a la autodeterminación informativa y el derecho a la libertad de información y expresión se ha sostenido que es preciso atender a la naturaleza de la información que se facilita y la finalidad perseguida, pero también ha de contarse con el medio utilizado y al número de destinatarios posibles para poder evaluar la existencia de un interés general en difundir esa información, pues no podemos desdeñar que la información que se publica en internet puede ser consultada en cualquier momento por un número indeterminado de personas en muchos países por lo que debe exigirse un interés general más intenso en conocer y transmitir esa información ya que el crédito personal del afectado y la injerencia en su privacidad es mayor.

Por todo ello puede extraerse la conclusión de que os criterios de ponderación, los límites y, en definitiva la solución que se ofrezca no necesariamente debe ser la misma ante eventuales infracciones de la privacidad dentro y fuera de la red y dependiendo del agente causante de las mismas.

III. **ALGUNOS RETOS DE LA PROTECCIÓN DE DATOS EN INTERNET**

La protección de la privacidad, como concepto más amplio que el de intimidad o vida privada, aparece conectado con la protección de datos personales, de modo que la protección de los datos (de la privacidad) es algo más y distinto que la pro-

tección al honor, a la intimidad y a la propia imagen, pues no tiene por objeto establecer si una determinada información publicada lesiona o no el derecho al honor del afectado o es injuriosa o calumniosa, sino que plantea el poder de disposición del particular sobre sus datos personales.

La protección de este derecho fundamental, en cuanto tutela de relaciones en particulares, sigue siendo posible mediante el ejercicio de una acción civil, pero, al mismo tiempo, es posible acudir para su tutela a los organismos administrativos autónomos encargados de su protección (en España la Agencia Española de Protección de datos) bien para solicitar una tutela del derecho bien para pedir la iniciación de investigación que eventualmente concluya con una sanción administrativa, y en este caso, la tutela jurisdiccional se encomienda a los tribunales contencioso-administrativos.

La protección de datos y por ende la privacidad de las personas en internet plantea nuevos y constantes retos.

La amplitud del concepto «dato personal» (5), «fichero» y «tratamiento de datos», y su consideración como un derecho fundamental implica que su tutela se haya convertido en uno de los temas claves frente a los peligros que representa la sociedad digital y el tratamiento de la información y los datos de forma global e intemporal.

A. ÁMBITO TERRITORIAL DE APLICACIÓN

Internet y la actividad que se desarrolla en la red plantea un inicial problema consistente en determinar la normativa aplicable para regular las relaciones jurídicas que se producen y la jurisdicción competente para controlarlas. La territorialidad es consustancial al ejercicio de la jurisdicción e Internet constituye una realidad virtual en la que el espacio físico no existe.

En 1996 John P. Barlow colgaba en la Red la llamada «Declaración de Independencia del Ciberespacio» en la que proclamaba: «En el Ciberespacio no tenemos gobierno electo ni es probable que lo tengamos, de ahí que me dirija a ustedes, Gobiernos del Mundo Industrializado con no mayor autoridad que aquella con la que habla la propia libertad. Yo declaro que el espacio social global que estamos construyendo es por naturaleza independiente de las tiranías que ustedes pretenden imponernos. Ustedes no tienen ningún derecho moral para gobernarnos ni poseen método alguno de coerción que debamos temer con fundamento... Sus conceptos jurídicos de propiedad, libertad de expresión, derecho a la identidad, libertad de circulación y contexto no nos son aplicables. Se basan en la materia. Aquí, en el Ciberespacio no hay materia».

Tales afirmaciones son exageradas pero tienen un sustrato real: el ciberespacio es un ámbito virtual en el que los límites territoriales de las jurisdicciones nacionales y las competencias territoriales de los tribunales no son funcionales. Sin embar-

(5) Se ha considerado como datos personales el nombre y apellidos, la voz, la imagen de una persona, su números de identificación fiscal, DNI, cuentas bancarias, su historial clínico, el número de fax, las direcciones de email y las direcciones IP «pues proporciona información sobre una persona física identificada o «identificable».

go, los litigios de todo tipo a que puede dar lugar la utilización de la Red deben ser resueltos por órganos jurisdiccionales con base territorial.

Los principales problemas que plantea la protección de datos en este entorno global, dominado por empresas que se ubican en terceros Estados, pero que prestan servicios a ciudadanos de todo el mundo a través de internet, radica en la determinación de la normativa a la que quedan sujetas las reclamaciones que los usuarios planteen contra las mismas y consiguientemente los tribunales competentes para ejercicio de las reclamaciones en defensa de los derechos de los ciudadanos.

Ya en el asunto Google Spain se planteó este problema. La empresa Google sostenía que a los efectos de la aplicación de la normativa de protección de datos y consiguientemente al control administrativo y jurisdiccional de su actividad solo estaba sujeta a la jurisdicción norteamericana y a la normativa de protección de datos de EEUU, pues ni tenía un establecimiento en España, ya que Google Spain SL no realizaba actividad relacionada con el tratamiento de datos, ni recurría a medios ubicados en España.

El Tribunal de Justicia de la Unión Europea en la ya conocida sentencia de 13 de mayo de 2014 consideró que existía esa conexión que permitía aplicar la normativa de protección de datos de la Unión cuando una empresa matriz que tuviese su domicilio social fuera de la Unión Europea pero que «dispone de un establecimiento en un Estado miembro, está sometida a la normativa de la Unión si dicho establecimiento está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor», pues ambas actividades están indisolublemente asociadas.

El problema se ha vuelto a plantear en la STJUE de 1 de octubre de 2015 (C-230/14, Asunto Weltimmo) en el que se discutía la aplicación de la Ley de Protección de datos húngara a una empresa que tenía su domicilio en Eslovaquia. El Tribunal realizó una interpretación flexible del concepto «establecimiento», afirmando que debe acudirse tanto al grado de estabilidad de la instalación como la efectividad del desarrollo de actividades en ese Estado, tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios (especialmente en el caso de servicios prestados exclusivamente a través de Internet). Y que basta la existencia de cualquier actividad real y efectiva, aunque mínima, ejercida mediante una instalación estable, y como tal puede entenderse la gestión de varios sitios de Internet de anuncios de inmuebles situados en Hungría y redactados en húngaro.

Pero la solución puntual en estos casos no resuelve ni mucho menos todos los problemas. Las empresas que operan internet, utilizan soportes técnicos que pueden estar centralizados o dispersos en diferentes países y sus servidores pueden estar ubicados en lugares remotos y muchas veces secretos. Y pueden prescindir de crear un establecimiento estable.

Una protección eficaz de este derecho fundamental no puede depender del lugar donde la empresa decida asentar los medios técnicos. La utilización de soportes técnicos inmateriales, que permiten prestar los servicios desubicados del territorio al que van dirigidos y, en muchos casos, sin contar con medios residenciados en el mismo, complica una tutela eficaz de las eventuales lesiones de los derechos de la personalidad que se producen en el ciberespacio, especialmente en materia de protección de datos. Sin desconocer el peligro añadido que supondría la posibili-

dad de suprimir los establecimientos y medios que tuviere para impedir la aplicación de la normativa comunitaria o nacional, o cambiar el centro de gestión de recursos y medios, localizándolo en aquellos países que careciesen de una normativa de protección de datos o en los que sus normas fuesen más permisivas con la tutela de estos derechos.

Estas preocupaciones siguen vigentes en la actualidad, y posiblemente las lagunas detectadas hallan determinado el cambio de criterio en los puntos de conexión previstos en el proyecto de Reglamento de Protección de Datos que se está elaborando en la Unión Europea.

El Reglamento de la Unión, de 27 de abril de 2016, relativo a la protección de datos de las personas físicas, modifica y mejora los criterios de conexión. En su art. 3.2 establece que «El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que tenga lugar en la Unión.»

Este criterio de conexión es nuevo y resulta muy acertado, pues tal y como hemos señalado el problema con la actual tecnología radica en la desubicación de los medios y de los establecimientos en el tratamiento de datos, por lo que hasta ahora si la empresa tenía su sede fuera de la Unión y tampoco tenía en ella un establecimiento ni designaba un responsable, quedaba excluida del ámbito de aplicación de la normativa europea, aunque, en realidad, estuviese tratando datos de los ciudadanos de la Unión y el foco de conflicto de intereses estuviese situado en la Unión Europea.

Con la reforma prevista en el nuevo Reglamento se asume en gran medida el criterio de la ubicación del «centro de gravedad del conflicto» que se apuntaba en la cuestión prejudicial planteada por España en el caso Google Spain, pues indudablemente el centro de gravedad del conflicto y donde se puede realizar una tutela más eficaz de la indebida injerencia en los derechos fundamentales de un ciudadano residente en un Estado de la Unión cuyos datos han sido tratados en virtud de una relación de bienes o servicios o están siendo utilizados para realizar un control sobre él, es el lugar de residencia del afectado, prescindiendo del lugar donde se ubique la empresa o los medios que utilice para realizar dicho tratamiento.

La tutela judicial de la privacidad en el Reglamento de la Unión permite que todo interesado pueda presentar una reclamación ante la autoridad de control de cualquier Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción (art. 77.1) y contra la decisión o inactividad de la autoridad de control en materia de protección de datos se garantiza el recurso judicial (art. 78).

Mención aparte merece la regulación referida al derecho a un recurso judicial contra el responsable o encargado (art. 79 del Reglamento). Esta acción se puede ejercitar ante los órganos jurisdiccionales del Estado miembro en el que el responsable o encargado tenga un establecimiento o, alternativamente, donde el interesa-

do tenga su residencia habitual con la única excepción de que «el responsable sea una autoridad pública que actúa en el ejercicio de sus poderes públicos», supuesto en el que ha de presentarse en el Estado miembro donde se encuentre dicha autoridad. Esta previsión, por tanto, trata de facilitar el ejercicio de la tutela de estos derechos cuando el afectado por el tratamiento resida en un Estado miembro distinto de aquel donde el responsable o encargado tenga un establecimiento.

La existencia del foro alternativo conlleva el riesgo de la existencia de dos procesos independientes ante dos Estados miembros con la posibilidad de incurrir en decisiones contradictorias para lo cual el art. 81 de Reglamento prevé que el órgano judicial se ponga en contacto con el órgano jurisdiccional del otro Estado miembro para confirmar la existencia de procedimientos paralelos y, en su caso, suspender su procedimiento (art. 81 apartados segundo y tercero). El problema vendrá determinado por la dificultad de conocer la existencia de estos procedimientos paralelos en dos Estados miembros.

B. LA CREACIÓN DE PERFILES DE LOS USUARIOS

El segundo reto que presenta la tutela de la privacidad en internet es la creación de perfiles personales o de los hábitos y comportamientos de los ciudadanos.

El almacenamiento de los datos relativos a las páginas consultadas por los usuarios de internet proporciona una ingente información sobre los gustos, costumbres, aficiones e incluso vicios o debilidades de la persona. La posibilidad de almacenar esa información, tratarla y ordenarla por las grandes compañías proporciona a las empresas y a los estados una información muy valiosa sobre los ciudadanos, que puede ser tratada con fines comerciales privados o para identificar necesidades públicas de forma lícita, pero también puede ser utilizado para controlar y «dirigir», e incluso abiertamente a coaccionar y depurar, máxime si esta información puede ser cruzada con los datos que identifiquen al usuario.

Este problema está conectado con las llamadas direcciones «IP», que puede definirse como la secuencia numérica asignada a un dispositivo (un ordenador, Tablet o teléfono inteligente) que nos permite acceder a la red. El acceso a las páginas web registra la dirección IP del usuario, por lo que es posible conocer el titular de estos dispositivos que ha accedido a determinada información, a qué contenidos, desde donde y por cuanto tiempo, lo que permite obtener una gran información sobre el usuario.

Debe tomarse en consideración que la compañía proveedores de servicios (normalmente las compañías telefónicas) que adjudican estas direcciones IP pueden vincularla con los datos personales de los usuarios que ellos mismos han proporcionado para poder obtener la dirección IP y así poder operar en la red. El TJUE en su sentencia de 24 de noviembre de 2011 (C-70/10, Asunto Scarlet Extended») ya consideró que las direcciones IP estáticas son datos personales protegidos, ya que permiten identificar concretamente a los usuarios, si bien lo hizo en un contexto en el que la recogida y la identificación de las direcciones IP las realizaba el proveedor de acceso a la red y no un proveedor de contenidos.

El problema se ha planteado también respecto de las IP dinámicas (6) en relación con el registro que las instituciones públicas que tiene portales de internet abiertos al público y ofrecen información a los ciudadanos, almacén el acceso a los ficheros incluso una vez acabada la operación (conversan la dirección de IP desde la que se ha hecho la consulta y el nombre del fichero o página solicitada, los conceptos introducidos en los campos de búsqueda, la cantidad de datos trasmitidos). La cuestión se ha planteado a raíz de una cuestión prejudicial planteada por el Tribunal Supremo Civil y Penal alemán preguntando si una dirección «IP dinámica» es un dato personal para el proveedor de una servicio de Internet cuando la compañía de telecomunicaciones que ofrece el acceso a la red (el proveedor de acceso) maneja datos adicionales, que combinados con aquella dirección, permitan identificar a quien accede a la página web gestionada por el primero.

Las conclusiones del Abogado General Manuel Campos Sánchez-Bordona, presentadas el 12 de mayo de 2016, consideró que «las direcciones IP dinámicas, solo por facilitar información sobre la fecha y la hora en las que se ha accedido a una página web desde un ordenador (u otro dispositivo), manifiestan unas ciertas pautas de comportamiento de los usuarios de internet y, por lo tanto suponen una potencial injerencia en el derecho a la vida privada» (considerando 55). Es cierto que la fecha y hora de conexión y el mero hecho de disponer del código numérico no revela, directa ni inmediatamente, quién es la persona a la que pertenece el dispositivo que accede a la página web, no lo es menos que esa información junto con los datos adicionales de los que dispone la empresa o entidad que asigna las IP que dispone de los datos de identificación del usuario al que se le adjudica dicha IP, permite considerar que se trata de una información sobre una «persona identificable». El problema se centra en interpretar la expresión «medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona». El término «razonablemente» implica que el acceso a estos datos adicionales y la combinación con los que ya se dispone para terminar identificando al usuario no ocurrirá «cuando el contacto con esos terceros sea, de hecho, muy costoso en términos humanos y económicos, o prácticamente irrealizable o prohibido por la ley» (considerando 68), pero finalmente se concluye que ésta identificación es posible y, por tanto, «La dirección IP dinámica debe ser catalogada, para el proveedor de servicios de Internet, como un dato de carácter personal habida cuenta de la existencia de un tercero (el proveedor de acceso a la red) al que puede razonablemente dirigirse para conseguir otros datos adicionales que, entrecruzados con aquella, propicien la identificación de un usuario» (considerando 74), pues en caso contrario si las direcciones IP dinámicas no constituyeran un dato de carácter personal para el prestador de servicios, éste podrá conservarlas de manera indefinida y solicitar esa información adicional en un futuro, momento en el que se convertiría en dato personal con carácter retroactivo.

Aunque considera lícito el almacenamiento de las direcciones de IP y los restantes datos de la consulta tanto para la prestación del servicio, incluida la facturación, como para prevenir ataque y posibilitar acciones penales contra los «piratas».

(6) Las «IP dinámicas» son las que las compañías de manera temporal, para cada conexión a internet, y las cambian con ocasión de las conexiones posteriores. Dichas compañías llevan un registro en el que consta qué dirección IP han adjudicado, en cada momento, a un dispositivo.

La sentencia del Tribunal de Justicia (Sala Segunda) de 19 de octubre de 2016 (C-582/14 asunto Patrick Breyer), confirmando el criterio apuntado por el Abogado General, parte de que una dirección IP dinámica no constituye una información relativa a una persona física identificada (puesto que no revela directamente la identidad de la persona física propietaria del ordenador desde el que se realiza la consulta) pero, a continuación, se cuestiona sí puede calificarse de una información relativa a una «persona física identificable». Y a tal efecto, considera identificable al que pueden conocerse sus datos no solo directamente sino también indirectamente, entendiendo que para «calificar una información de datos personal no es necesario que dicha información permita, por sí sola, identificar al interesado» sino que basta el que se puedan utilizar los medios que razonablemente permitan identificar a dicha persona, sin que sea necesario que toda la información que permita identificar al interesado debe encontrarse en poder de una sola persona.

Entiende, siguiendo al Abogado General, que no es se consideran medios razonables cuando la identificación del interesado esté prohibida por la ley o sea prácticamente irrealizable porque, por ej, implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos, considerando que sí lo es cuando disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a internet de dicha persona.

IV. LA PROTECCIÓN DE LA PRIVACIDAD FRENTE A LAS AUTORIDADES Y FRENTE A PARTICULARES

Los potenciales peligros contra la privacidad se han planteado tanto frente a los Estados y las autoridades públicas como frente a los particulares.

A. PROTECCIÓN FRENTE A LAS AUTORIDADES

Un claro ejemplo de los peligros que representa en nuestros días una recopilación exhaustiva por las autoridades de todos los datos incluidos internet, lo representa la nueva política del gobierno chino sobre la privacidad de sus ciudadanos. La nueva ley, que aprobada por el parlamento chino que tiene como objetivo «luchar contra el terrorismo», obligará a todas las compañías tecnológicas que operen en China a facilitar el acceso a sus sistemas, bases de datos e información confidencial para que las fuerzas y cuerpos de seguridad chinos (incluyendo sus servicios secretos) puedan recopilar información que les permita, supuestamente, luchar contra el terrorismo. La obligación de proporcionar esa información a las autoridades chinas se hará aunque los servidores de estas compañías no se encuentren localizados dentro de China, ya que la ley obliga a cualquier compañía a facilitar la información requerida por la policía o el ejército, se encuentren donde se encuentren los datos. La Ley de Seguridad Cibernética, además, obligará a los servicios de mensajería instantánea y otras compañías de Internet a hacer que sus usuarios se registren con sus nombres reales y brinden su información personal; y no solo eso, sino también a censurar contenido considerado como «prohibido».

Y ello no ocurre tan solo en China. Los Estados pretenden tener acceso a la información sobre los usuarios en internet con la finalidad de prevenir y perseguir actividades delictivas o que eventualmente puedan afectar a la seguridad nacional. El problema se plantea cuando el acceso es indiscriminado y desproporcionado, pues la información obtenida puede convertirse en una potente arma que puede ser indebidamente utilizada contra los ciudadanos.

La STUE de 8 de abril de 2014 Digital Right Ireland abordó el problema de la conservación de datos relacionados con comunicaciones telefónicas y su puesta a disposición de las autoridades durante el tiempo establecido por la ley para prevenir y detectar delitos, investigarlos y enjuiciarlos, así como para garantizar la seguridad del Estado.

El TJUE sostuvo que aunque la conservación de datos para su eventual acceso por parte de las autoridades nacionales competentes responde efectivamente a un objetivo de interés general, pero no supera el juicio de proporcionalidad porque:

– la injerencia afecta prácticamente toda la población europea, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales;

– no establece ninguna relación entre los datos cuya conservación se exige y una amenaza para la seguridad pública y, en particular, la conservación no se limita a datos referentes a un período temporal o zona geográfica determinados o a un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, ni a personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos grave;

– no fija ningún criterio objetivo que permita delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que puedan considerarse suficientemente graves para justificar tal injerencia.

– porque, en relación con al acceso de las autoridades nacionales competentes a los datos y su utilización posterior, la normativa comunitaria no precisaba ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido;

– y finalmente, en lo que atañe al período de conservación de los datos (un período mínimo de seis meses), no establece ninguna distinción entre las categorías de datos previstas en función de su posible utilidad para el objetivo perseguido o de las personas afectadas.

Por todo ello, el Tribunal concluye que la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta. Por lo tanto, debe considerarse que esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario.

Otra sentencia relevante del Tribunal de Justicia de la Unión Europea es la dictada por la Gran Sala, de 6 de octubre de 2015 (Asunto C-362/14, Maximillian

Schrems contra Data Protection Commissioner) a raíz de una cuestión prejudicial planteada por la High Court de Irlanda, en relación con la transferencia de datos a EEUU de un usuario de Facebook. En ella, por lo que ahora nos interesa, se trata de los riesgos de una indebida utilización de nuestros datos por las autoridades o empresas radicadas en terceros estados. Diariamente autorizamos a empresas que operan a nivel internacional para que utilicen nuestros datos personales. La inscripción o registro en las redes sociales (Facebook, twiter, etc.) y las cada vez más frecuentes transacciones comerciales «on line» implican poner nuestros datos personales a disposición de empresas multinacionales radicadas en terceros Estados con un diferente nivel de protección en materia de protección de datos, y con estos datos se pueden crear perfiles de comportamiento y hábitos o incluso afectar a nuestra propia intimidad y seguridad personal, que si bien puede quedar protegida en el entorno de la Unión Europea, se corre el riesgo de una protección menor cuando se transfieren esos datos a un Tercer Estado cuyo nivel de protección no es «equivalente».

B. LA PROTECCIÓN DE DATOS FRENTE A LAS EMPRESAS PARTICULARES

Los datos personales no solo han de protegerse frente las autoridades públicas sino también frente a eventuales lesiones procedentes de particulares o de empresas privadas. Y ha de partirse de que la protección frente a las empresas privadas que operan en la red, aunque plantean un conflicto entre particulares, ambas partes (el ciudadano y las compañías de servicios o de contenidos) no se encuentra en un plano de igualdad, tal y como he mencionado anteriormente, dato que necesariamente ha de condicionar la ponderación de derechos e intereses a proteger.

La protección frente a particulares puede revestir distintas modalidades:

a) **Límite frente al ejercicio de acciones de terceros**

En muchas ocasiones, la protección de datos opera como límite oponible al ejercicio de acciones en las que se ejercitan derechos por un tercero. Este sería el caso del ejercicio de acciones destinadas a la tutela de derechos de propiedad intelectual ante la sospecha de una actividad ilícita en la que se solicita de la compañía de servicios que revele la identidad física del presunto infractor que actúa en internet.

La STJUE de 29 de enero de 2008 (C-275/06, Asunto Promusicae, apartados 54 y 55) consideró que el derecho comunitario no se opone a que los Estados miembros establezcan una obligación de transmitir a particulares datos personales para permitir ejercer acciones ante la jurisdicción civil contra infracciones del derecho de propiedad intelectual, pero tampoco obliga a los Estados miembros a imponer tal obligación.

Y en similares términos, la STJUE de 19 de abril de 2012 (C-461/10, Asunto Bonier Audio) se planteó si una empresa puede solicitar de un tribunal que éste dirija un requerimiento al operador del sistema a efectos de identificación de un usuario (nombre y dirección de un abonado a internet) que hace uso de una direc-

ción de IP a partir de la cual presuntamente se estaban realizado actividades contrarias a los derechos de propiedad intelectual (descargas ilícitas de libros). El Tribunal consideró que la normativa nacional que se dicte debe garantizar un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico de la Unión y respetar el principio de proporcionalidad. De modo que para «que pueda emitirse un requerimiento judicial de comunicar los datos en cuestión, la normativa nacional controvertida exige que existan indicios reales de vulneración de un derecho de propiedad intelectual sobre una obra, que los datos solicitados puedan facilitar la investigación de la vulneración del derecho de autor y que el fin perseguido por dicho requerimiento sea más importantes que el daño o perjuicio que se puedan causar a la persona afectada o a otros intereses contrapuestos».

b) **El derecho al olvido**

En otras ocasiones, el ciudadano esgrime de forma activa la protección de datos frente a terceros para recabar la tutela de su derecho a la cancelación. Es aquí donde surge el llamado «derecho al olvido», que podría ser definido como el legítimo interés de toda persona de no permanecer indefinidamente expuesto al daño que causa en su privacidad el conocimiento público y de forma indefinida de determinados datos personales o hechos que les afectan y le permiten su identificación y que no desean que sean conocidos.

Las razones por las que una persona física puede considerar que una información, imagen o noticia, incluso aquella que aparentemente pueda aparecer inocua, puede dañar su dignidad o tener una repercusión negativa en su esfera personal, social o profesional pueden ser muy variadas, y en muchas ocasiones tienen un marcado componente subjetivo. Los ejemplos pueden ser muy variados: fotografías o noticias comprometedoras de una juventud intensa, implicaciones en actividades ilegales o ilícitas que no se desean que sean conocidas varios años después, situaciones pasadas de insolvencia que han sido superadas, etc.

El interrogante que surge puede plantearse en términos generales sería ¿Es bueno que se olvide?, y por añadidura ¿puede reconocerse al individuo un control absoluto sobre todos sus datos que se publican?, ¿el ciudadano tiene el derecho a suprimir todos aquellas informaciones que incorporen sus datos personales o cuando entienda que esta «atenta o puede atentar» a su dignidad, entendida como un concepto amplio?

Ciertamente el derecho al olvido no es ajeno a los ordenamientos jurídicos actuales, pues está relacionado con instituciones como la prescripción de los delitos o la cancelación de antecedentes penales que tienen como finalidad permitir un cierto control sobre los datos oficiales que deben constar en los registros públicos sobre una persona y con la rehabilitación social, por entender que existe un derecho a que se olvide la existencia de determinados hechos del pasado que no deben ser recordados de forma permanente.

Aunque la sensibilidad sobre el público conocimiento y difusión de hechos pasados, incluso transcurrido un lapso temporal, no es la misma en todos los Estados. Así, en EEUU los ciudadanos tienen derecho a consultar las bases de datos a todos los niveles del estado en donde consten los antecedentes penales de sus con-

ciudadanos, aunque estén cancelados, por entender que esta información sobre los hechos pasados constituye un derecho que facilita la posibilidad de adoptar una decisión más acertada para entablar relaciones comerciales (por ej arrendarle un inmueble) o incluso para tomar decisiones personales o familiares (cuidado de sus hijos, elección de un colegio etc..). Otros ordenamientos, normalmente los continentales europeos, son más propicios a limitar estos datos del conocimiento público permitiendo un acceso más limitado y su eventual cancelación.

La sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014 (Asunto C-131/12, Google Spain, S.L., Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González), dando respuesta a una cuestión prejudicial planteada por la Sala de lo Contencioso-administrativo de la Audiencia Nacional del Reino de España, aborda este problema.

El Tribunal de Justicia reconoce el derecho de un particular a ejercer sus derechos a la rectificación, supresión o bloqueo de sus datos personales no solo cuando «los datos sean inexactos, sino en particular, de que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, de que no estén actualizados o de que se conserven durante un período superior al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos». Y añade que un tratamiento inicialmente lícito de datos exactos «puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Éste es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido» y en tales casos la información y los vínculos deben eliminarse a petición del interesado.

Ello implica el reconocimiento claro y explícito del «derecho al olvido» cuya esencia radica en la supresión de datos e informaciones que con el transcurso del tiempo han perdido la razón de ser que las justificaron en su momento y el afectado desea que no sean del conocimiento público. Y lo hace con independencia de que dichas noticias o informaciones le generen un perjuicio («la apreciación de la existencia de tal derecho no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado»).

La protección de la privacidad de los ciudadanos tendría las siguientes características:

– no es exigible que la información suministrada cause o no un perjuicio al interesado;

– no aparece vinculada a ilicitud de la información suministrada pues esta protección también opera frente a datos exactos cuyo conocimiento, por el tiempo transcurrido, ya no sean necesarios en relación con los fines para los que se recogieron o trataron;

– se establece una protección asimétrica en razón a los derechos invocables y los intereses que protegen los diferentes operadores en internet.

– se permite que el ejercicio del derecho de cancelación de los datos se ejercite frente al buscador con independencia de que no se solicite la cancelación de los datos frente al editor.

La regulación de este derecho y sus límites, ha sido aborda a nivel de la Unión Europea por el Reglamento del Parlamento Europeo y del Consejo, de 27 de abril

de 2016, en su art. 17 y bajo el título «Derecho de supresión («el derecho al olvido»)» reconoce el derecho del interesado a obtener del responsable del tratamiento de los datos personales que le concierna, el cual estará obligado a suprimir los datos cuando concurran alguna de las circunstancias siguientes: cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; cuando el interesado retira el consentimiento; cuando el interesado se oponga al tratamiento y no prevalezcan otros motivos; cuando los datos hayan sido tratados ilícitamente; cuando los datos deben suprimirse para el cumplimiento de una obligación legal, o los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de información de menores de 16 años.

Pero el reconocimiento de este derecho también está condicionado por la confrontación con otros derechos fundamentales, singularmente con los derechos de información y libertad de expresión.

V. CONFRONTACIÓN ENTRE LOS DERECHOS E INTERESES ENFRENTADOS

Resulta obvio recordar que tanto el derecho a la vida privada (en un sentido estricto) como el de la privacidad/protección de datos no son derechos absolutos. Los derechos fundamentales pueden ceder ante otros derechos e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido.

A. CRITERIOS GENERALES

La confrontación de los intereses en conflicto exige analizar las circunstancias en las que el afectado podrá ejercer su derecho, especialmente el supuesto previsto en el «los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados».

Considero que la determinación de cuando existe un interés en que determinados datos sean conocidos o mantenidos exige, desde una vertiente positiva, un análisis en donde se mezclan aspectos objetivos (relativos al contenido de la información y los datos que se publican) y subjetivos (relacionados con las circunstancias del afectado, y especialmente con su notoriedad pública), que han de conectarse con un juicio de proporcionalidad que exige determinar si la conservación o difusión de los datos sin el consentimiento de su titular o incluso en contra del mismo, es necesaria (si no existe una medida menos lesiva para cumplir el mismo fin) y es idónea (sirve para cumplir el fin propuesto).

Y desde una vertiente negativa es preciso tomar en consideración el factor tiempo. Será necesario ponderar la permanencia de ese interés en el tiempo, pues, aun cuando la utilización de los datos pudiera estar justificada en un principio, el paso del tiempo ha podido hacerlo desaparecer, especialmente cuando los datos ya no son necesarios en relación con los fines para los que fueron recogidos o trata-

dos. La actualidad de la información y de los datos que incorpora puede dejar de ser relevante, desapareciendo el interés público que justificaba su inicial publicación. Y es esa pérdida de actualidad la que resulta especialmente trascendente, dado que precisamente es el paso del tiempo y la voluntad del afectado de que determinados datos o informaciones no sigan siendo accesibles al conocimiento público, unido al hecho de la intemporalidad de los datos en internet, la que justifica el ejercicio del derecho al olvido.

B. COLISIÓN CON OTROS DERECHOS

Por otra parte, frente al derecho del afectado en preservar su privacidad se encuentran los derechos e intereses legítimos invocables por el responsable del tratamiento.

En principio, la aprobación del Reglamento de la Unión de 27 de abril de 2016 permite un tratamiento uniforme en la Unión Europea. Pero, decimos «en principio», porque la conciliación de la «privacidad» frente a la libertad de expresión e información (incluido el tratamiento con fines periodísticas y de expresión académica, artística o literaria), se encomienda a los Estados miembros (art. 85 del Reglamento), pero, al mismo tiempo, se permite que los Estados miembros puedan establecer exenciones o excepciones a gran parte de los preceptos del Reglamento «si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información» (art. 86.2 del Reglamento), lo que podría determinar unos criterios dispares en los diferentes Estados miembros en la confrontación de los derechos enfrentados.

Una de las excepciones que el Reglamento europeo establece a la imposibilidad de tratar los datos personales del afectado sin su consentimiento es que dicho tratamiento sea necesario «para ejercer el derecho a la libertad de expresión e información», lo cual ya venía siendo un criterio utilizado por la jurisprudencia de los diferentes Estados miembros, si bien analizando esta ponderación en atención a las circunstancias concurrentes en cada caso concreto.

Hechas estas precisiones conviene delimitar que alcance y límites tiene este derecho dependiendo del destinatario de la petición.

a) **El derecho al olvido frente a los responsables de la página web**

El Tribunal de Justicia declaró en la sentencia Lindqvist que «la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento [de datos personales]». El Tribunal de Justicia concluyó que «la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva». De esta sentencia se deduce que el editor de páginas web que contienen datos personales es responsable del tratamiento de datos personales. El editor está sometido, por tanto, a todas las obligaciones que la normativa de protección de datos impone a los responsables del tratamiento.

Este normalmente invocará su derecho a la libertad de expresión e información para tratar los datos de carácter personal. Y esta misma colisión, especialmente intensa en relación con el derecho a la libertad de información, se producirá cuando se ejercite el derecho de supresión frente a un medio de comunicación convencional. Debe aclararse, en este punto, que también los particulares, y no solo los periodistas profesionales, pueden estar amparados por la libertad de información tal y como se ha encargado de destacar nuestra jurisprudencia (7).

Pero cuando el derecho al olvido se ejercite frente a las Administraciones Públicas los problemas se gravan, al entrar en juego intereses públicos o fines públicos legítimos necesitados de protección, tales como la transparencia de la actividad pública, el principio de publicidad de sus actuaciones, la seguridad jurídica, la necesidad de preservar la concurrencia y participación en contratos o asuntos públicos, o simplemente el cumplimiento de obligaciones legales, que está contemplado también como otra de las excepciones en el art. 17.3.b) del Reglamento.

Son los responsables del tratamiento de la información en origen, los responsables de la publicación, los que técnicamente tiene la posibilidad retirar una información de su página o modificarla, o de incluir en sus páginas web códigos de exclusión que restringen el indexado y el archivo de la misma. Y son ellos los que fundamentalmente puedan discutir frente al afectado que pretende ejercer su derecho de cancelación u oposición, la licitud del dato, la existencia de consentimiento del afectado, la actualidad y proporcionalidad de la información y finalmente la invocación de otros derechos que puedan entrar en colisión con los del afectado que pretende su cancelación.

Por ello, cuando se ejercita el derecho de cancelación/supresión de datos frente al editor de los mismos, inevitablemente se produce una confrontación entre los derechos del afectado a ejercer un control sobre el tratamiento y difusión de sus datos personales y el interés perseguido en su difusión y los derechos que asisten al que los ha introducido.

La necesaria ponderación de los derechos e intereses en conflicto, deberá de hacerse caso por caso y atendiendo a las circunstancias concurrentes.

b) **El derecho al olvido frente los buscadores en Internet**

Los buscadores, indexan una información y la difunden de forma muy sencilla a nivel mundial, sin que ellos hayan generado esa información de origen ni puedan modificarla o alterarla.

Los buscadores tienen una importancia capital en la sociedad actual, al permitir una fácil y rápida localización de la ingente cantidad de información que existe en internet, contribuyendo de forma decisiva a que la misma sea accesible de forma inmediata a un gran número de usuarios en el mundo y, consecuentemente, al desarrollo de la sociedad de la información y a la creación de una opinión pública mejor informada. No cabe desconocer tampoco la importancia que esta herramienta tiene para los titulares de las páginas web en las que se aloja dicha información, pues si

(7) Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, Sección 1.ª, del 11 de abril del 2012 (rec. 410/2010).

la difusión de sus contenidos se restringe se vería afectado también su derecho a transmitir información por internet o comercializar sus productos.

La supresión o limitación de los motores de búsqueda podría incidir también en el correcto funcionamiento de los servicios públicos y los mecanismos previstos en la ley para cumplir los fines que le han sido encomendados, piénsese que en el supuesto que nos ocupa se estaría restringiendo la publicidad de las actuaciones desarrolladas por las Administraciones públicas no solo para hacer efectivo el principio de transparencia sino también para que los interesados tengan conocimiento de su actuación y puedan participar en las mismas (por ej: piénsese en la convocatoria de una subasta pública, o en la publicidad en la convocatoria de una licitación pública).

Pero los afectados aprecian que el peligro real procede, en muchas ocasiones, no tanto del origen de la información como de su difusión por medio de estos buscadores, dado que son ellos los que permite una difusión global e ilimitada de la información de forma sencilla y la recopilación, utilizando un simple término de búsqueda (como puede ser el nombre de una persona) de toda la información relacionada con la misma, propiciando la elaboración de perfiles personales.

Esta preocupación ha motivado que muchos ciudadanos hayan solicitado la tutela para que los buscadores (básicamente Google) elimine u oculte sus datos y dejen de incluirse en los resultados de búsqueda sus datos personales relacionados con una noticia o un acontecimiento determinado. En definitiva, no desean que determinadas informaciones, publicadas en páginas web de terceros que contienen sus datos personales y permiten relacionarles con la misma, sean localizadas, indexadas y sean puestas a disposición de los internautas de forma indefinida.

La STJUE de 13 de mayo de 2014 afirmó al respecto que «la ponderación de los intereses en conflicto que ha de llevarse a cabo... puede divergir en función de que se trate de un tratamiento llevado a cabo por un gestor de un motor de búsqueda o por el editor de esta página web, dado que, por un lado, los intereses legítimos que justifican estos tratamientos pueden ser diferentes, y, por otro, las consecuencias de estos tratamientos sobre el interesado, y, en particular, sobre su vida privada, no son necesariamente las mismas», porque si bien el editor de páginas web que contienen datos personales puede oponer el legítimo ejercicio del derecho de información con fines exclusivamente periodísticos, no es el caso en el supuesto del tratamiento que lleva a cabo el gestor de un motor de búsqueda. Es más, dicha sentencia añade «… en la medida en que la inclusión, en la lista de resultados obtenida tras una búsqueda llevada a cabo a partir del nombre de una persona, de una página web y de información contenida en ella relativa a esta persona facilita sensiblemente la accesibilidad de dicha información a cualquier internauta que lleve a cabo una búsqueda sobre el interesado y puede desempeñar un papel decisivo para la difusión de esta información, puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web».

Por ello el Tribunal de Justicia de la Unión Europea en su sentencia de 13 de mayo de 2014 proporcionó algunas pautas para realizar dicha ponderación:

– La decisión de cancelación o supresión de tales datos frente al buscador no presupone que los mismos sean eliminados con carácter previo o simultáneamente de la página web en la que han sido publicados, por lo que la supresión de los datos

dependerá de los derechos que invoque la persona o entidad frente a la que se ejercita, pues no tendrán la misma intensidad ni idéntica protección.

– El derecho de cancelación de los datos de un particular prevalece frente al interés económico del gestor del motor de búsqueda.

– En relación con el interés de los internautas en tener acceso a la información en cuestión, el derecho a la privacidad prevalece, con carácter general, sobre el mencionado interés de los internautas, no obstante dependerá de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública.

C. ALGUNOS PRONUNCIAMIENTOS JUDICIALES RELEVANTES

Existen numerosos pronunciamientos de los tribunales que han ponderado el derecho al olvido frente a los intereses y/o derechos invocados por el responsable del tratamiento. Me centraré tan solo en algunos de ellos, sin perjuicio de recoger las pautas de ponderación seguidas por los tribunales de lo contencioso-administrativo cuando se ha ejercitado el derecho al olvido.

a) **La Sala Primera del Tribunal Supremo, en su STS de 15 de octubre de 2015 (rec. 2772/2013)**

Abordó una demanda en la que se reclamaba el derecho al olvido contra Google Spain y otras compañías en relación con una información publicada en un periódico sobre un indulto por un delito cometido en 1981 que afectada a su intimidad personal y familiar, a su imagen y honor. La actuación que motivó la demanda no fue la publicación de la noticia en la edición en papel del periódico, sino el tratamiento de los datos personales derivado de la inclusión de los nombres y apellidos en el código fuente de la página web de la hemeroteca digital de un periódico en que se digitalizó tal noticia con un tratamiento que permite su indexación por los motores de búsqueda de Internet.

Según el alto tribunal, la vinculación entre los datos personales de una persona y una información lesiva para su honor e intimidad en una consulta por Internet va perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico. Por ello, el derecho a la protección de datos personales justifica que, a petición de los afectados, los responsables de las hemerotecas digitales deban adoptar medidas tecnológicas impedir que en sus páginas la información obsoleta y gravemente perjudicial pueda ser indexada por los buscadores de Internet.

Sin embargo, la Sala rechaza la procedencia de eliminar los nombres y apellidos de la información recogida en la hemeroteca, o que los datos personales contenidos en la información no puedan ser indexados por el motor de búsqueda interno de la hemeroteca.

Especialmente relevante resulta, a mi juicio, la ponderación de los intereses en conflicto realizada por la Sentencia de la Sala Primera (Civil) de 5 de abril de 2016

(rec. 3269/2014). La sentencia partiendo de la doctrina sentada por la STEDH de 18 de septiembre de 2014 (caso Brunet contra Francia) y la fijada en la sentencia del TJUE de 13 de mayo de 2014 (caso Google Spain) realizó una ponderación de los intereses enfrentados llegando a la conclusión de que la mención de los datos personales del demandante en la resolución oficial que concede el indulto no puede considerarse contrario al honor o intimidad de la persona indultada que lo debe soportar «porque así lo exige el derecho de información de una sociedad democrática». Pero el tratamiento de sus datos que era lícito inicialmente, con el paso del tiempo ha dejado de serlo, por lo que el hecho de que sus datos aparezcan conectados con el indulto en los resultados de búsqueda de internet resulta desproporcionado en relación al interés público que ampara el tratamiento de estos datos, «cuando el demandante no es una persona de relevancia pública, ni los hechos presentan un interés histórico». De modo que si bien el derecho a la información y el control de la actividad gubernamental justifica que esos datos puedan ser accesibles para una búsqueda específica en la página web oficial del organismo público donde se publican oficialmente los indultos, no está justificado que aparezca en los resultados de un motor de búsqueda.

Finalmente, la sentencia realiza una interesante consideración sobre los límites del llamado «derecho al olvido» afirmando que éste «no ampara que cada uno construya su pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos» ni que los que se exponen públicamente puedan exigir que se construya un »currículum» a su gusto eliminando de internet las informaciones negativas pues «de admitirse esta tesis, se perturbaría gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país». Pero dicho derecho sí ampara, cuando no se tenga la consideración de personaje público, la posibilidad de oponerse a un tratamiento de sus datos personales que permita localizar esa información utilizando como palabras clave en el buscador sus datos personales (nombre y apellidos) pues ello hace permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, «distorsionando gravemente la percepción que los demás ciudadanos tienen sobre su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad».

b) **Sentencias de los tribunales contencioso-administrativos (dictadas tras la sentencia del TJUE, asunto Google Spain)**

Las sentencias dictadas en el orden contencioso-administrativo sobre esta materia proceden en su mayor parte de la Audiencia Nacional, dada las dificultades que presentaba el acceso de estas materias al Tribunal Supremo por vía del recurso de casación, dificultades que previsiblemente podrán ser remedidas con el nuevo diseño del recurso de casación que entrará en vigor el próximo mes de julio de 2016.

En ellas se plantearon supuestos muy variados pero a grandes rasgos los criterios de ponderación han sido los siguientes (8):

– El criterio general ha sido la supresión del motor de búsqueda de internet de los datos personales vinculados a un hecho o noticia cuando debido al tiempo transcurrido, la naturaleza de la noticia, su interés público y la falta de notoriedad del sujeto, tales datos no se consideran necesarios en relación con los fines para los que se recogieron o trataron.

– Los datos no se suprimen de la página web de origen donde se publicó la información, especialmente si aparecen contenidos en un periódico o registro público. La libertad de información se encuentra satisfecha por su subsistencia de la información en la fuente, permitiendo incluso que permanezca en la base de datos interna del periódico, tan solo se impide que el motor de búsqueda pueda indexarla.

En la sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 103/2010) se trataba de la publicidad de la concesión de un indulto. El afectado ejercitó su derecho de

(8) En tal sentido pueden mencionarse las siguientes sentencias:

SAN de 29 de diciembre de 2014 (rec. 725/2010). En esta sentencia se resuelve el caso que dio lugar al planteamiento de la cuestión prejudicial ante el TJUE. El nombre del recurrente aparecía en los listados de búsqueda vinculado a una información referida a unos anuncios publicados en dos páginas web del periódico «La Vanguardia» de marzo de 1998 en las que se anunciaba una subasta inmobiliaria por deudas a la Seguridad Social del reclamante, que ya habían dejado de tener relevancia con el paso del tiempo.

SAN, Sala de lo Contencioso-Administrativo, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 781/200). Datos personales publicados en periódicos digitales referidos a una condena penal por hechos ocurridos en el 2002.

SAN, Sala de lo Contencioso-Administrativo, Sección 1, de 29 de diciembre de 2014 (Recurso: 240/2011). Datos personales (nombre y apellidos) publicados en una página WEB vinculados a una resolución sancionadora publicada en un Boletín Oficial hace diez años

SAN, Sala de lo Contencioso-Administrativo, Sección 1, de 29 de diciembre de 2014 (Recurso: 109/2010). Falta de relevancia del personaje público, información sobre una acusación penal publicada hace 26 años.

SAN, Sala de lo Contencioso-Administrativo, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 179/2012). Noticia aparecida en un periódico digital en 1985 en la que se hacía referencia a su detención en relación con una actividad de consumo de drogas y al hecho de estar sujeta a un tratamiento de desintoxicación.

SAN, Sala Contencioso-Administrativo, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 212/2009). El afectado, cirujano plástico, ejercitó el derecho de oposición al tratamiento de sus datos personales, pues al introducir su nombre en el buscador de «Google» aparecía la referencia a una página web del periódico «El País» de 1991, que informaba sobre una querella que presentó una paciente contra aquel por una operación, habiendo sido absuelto.

SAN, Sala Contencioso-Administrativo, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 104/2010). El afectado ejercitó, en abril de 2009, ante Google Spain, S.L, el derecho de cancelación de sus datos personales en relación con determinados datos indexados por el buscador Google, refiriéndose en concreto a una información que aparece en la versión digital del diario «El País.com», de 1993, en la que aparece, junto con otras personas, y se le cita de forma tangencial como implicado en un alijo de drogas. La sentencia toma en consideración el carácter sensible de la información para el afectado y el tiempo transcurrido, más de 20 años, desde la publicación inicial de la citada información.

SAN, Sala Contencioso-Administrativo, Sección 1.ª, de 29 de diciembre de 2014 (Recurso: 130/2012). Información que relacionaba a un Catedrático con un delito de acoso sexual del que fue absuelto

oposición al tratamiento de sus datos personales, instando la desaparición de la lista de resultados del buscador Google de la referencia a varias páginas web que incluían información relativa al BOE en el que se publicaba el Real Decreto que le concedió el indulto relativo a la condena impuesta por la comisión de un delito contra la salud pública por hechos cometidos en el año 1981, al considerar que resultaba lesiva para su intimidad, dificultándole rehacer su vida.

La sentencia, tras analizar la naturaleza jurídica del indulto con cita de varias sentencias del Tribunal Supremo, consideró que siendo lícita la publicidad de la inserción en el Boletín Oficial del Estado del Real Decreto de indulto por la carga que pesa sobre el indultado de soportar dicha publicidad, afirmando «Sin duda, tan relevante y trascendente institución en un Estado de Derecho debe verse sometida en su excepcional ejercicio al escrutinio público, mediante su debida publicidad, cuya potenciación por los buscadores de internet no debe reputarse, en principio, una desproporcionada carga para el favorecido por el indulto».

Ahora bien, el Tribunal manteniendo la legítima publicidad del indulto en la página oficial del boletín suprime la posibilidad de localizarla en los motores de búsqueda utilizando el nombre y apellidos del interesado por entender que: se trata de una información sensible para el afectado, que afecta a su vida privada y al derecho a la protección de datos personales de aquel; la antigüedad de tal información, que se remonta a quince años atrás, y de los hechos delictivos a que se refiere, acaecidos hace ya unos treinta y tres años; la ausencia de circunstancia personal alguna del afectado que determinara una especial relevancia del interés público de esa información.

Existen otros pronunciamientos que deniegan el derecho de cancelación ejercitado frente al buscador, la mayoría de los supuestos se refieren a denuncias en los que los datos suministrados por los afectados resultan insuficientes para determinar la naturaleza de la información que se pretende suprimir o no mencionan cuales son las páginas en las que se contiene la información ni el contenido de la misma, por lo que el Tribunal considera que no tiene datos para realizar la ponderación de los intereses en conflicto (9).

c) **Un caso interesante de ponderación: derecho al olvido/publicidad de los registros públicos de sociedades**

Acaba de plantearse una nueva cuestión prejudicial por el Tribunal Supremo de Casación Italiano en torno al alcance del derecho al olvido, en relación con la posibilidad de cancelar, anonimizar o bloquear los datos personales inscritos en el registro de sociedades. El problema que se planteaba era el siguiente: El Sr. Manni era administrador único de sociedad de construcción a la que se adjudicó un contrato para la construcción de un complejo turístico. El Sr. Manni demandó ante los tribunales a la cámara de comercio de Lecce, alegando que los inmuebles de dicho complejo no se vendían porque en el registro de sociedades constaba que él había sido administrador único y liquidador de otra sociedad, declarada en concurso de

(9) Este es el caso de las sentencias de la Audiencia Nacional de 29 de diciembre de 2014 (Recurso: 220/2011), de 29 de diciembre de 2014 (rec. 661/2009), de 29 de diciembre de 2014 (Recurso: 661/2009), de 29 de diciembre de 2014 (Recurso: 25/2013) y de 29 de diciembre de 2014 (Recurso: 657/2009).

acreedores en 1992 y que había sido cancelada del registro de sociedades, a raíz de un procedimiento de liquidación en el 2005. Datos que habían sido tratados por empresas de información profesionales. El Sr Manni solicitó que se ordenase a la Cámara de Comercio que cancelase o anonimizase o bloquease los datos que vinculaban su nombre al concurso de acreedores de dicha sociedad de la que fue administrador y que se le indemnizasen los perjuicios sufridos por la vulneración de su reputación.

El Tribunal de instancia italiano estimó su pretensión al considerar que difícilmente puede afirmarse que sea necesaria y útil la indicación del nombre del administrador único de la sociedad en el momento del concurso», debido a que «se trata de hechos producidos hace más de una década y pese a la cancelación de la inscripción registral de la sociedad [...] desde hace más de dos años». Según este Tribunal, la «"memoria histórica" de la existencia de la sociedad y de las dificultades que atravesó [...] también puede reflejarse en una amplia medida mediante datos anónimos». En efecto, las inscripciones que vinculan el nombre de una persona física a una fase crítica de la vida de la empresa (como el concurso de acreedores) no pueden ser indefinidas, a falta de un interés general específico en su conservación y divulgación». Se interpuso recurso de casación y el Tribunal Supremo de Casación italiano planteo cuestión prejudicial de interpretación. Partiendo del principio de que los datos personales no se conserven durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente, se pregunta si se opone a este principio un sistema de publicidad que opera el registro de sociedades italiano en la medida en que exige que cualquier persona, sin límite temporal, pueda conocer los datos de las personas físicas que constan en ese registro. La ponderación planteaba como posibilidades alternativas a la publicidad ilimitada si los datos transcurrido un determinado periodo de tiempo pueden ser consultados por destinatarios concretos en virtud de una apreciación caso por caso del responsable de esos datos o se podrían anonimizar la información.

Las conclusiones del Abogado General Sr. Ives Bot, presentadas el 8 de septiembre de 2016 (Asunto C-398/15. Cámara de Comercio de Lecce contra Salvatore Manni) tras destacar la importancia que tiene la inscripción y publicación en estos registros de la información relativa a las sociedades en aras a garantizar la seguridad jurídica necesaria para la protección de los acreedores y terceros, las operaciones comerciales y el buen funcionamiento del mercado, realiza una ponderación entre el interés público representado por la libre circulación de los datos en aras a la seguridad jurídica y la protección de datos del afectado.

El Abogado General se decanta por considerar que la garantía de la función esencial del registro de sociedades y el libre acceso, incluso intemporal, a los datos registrados debe prevalecer por las siguientes razones:

– La publicidad legal versa sobre un número limitado de datos, proporcionando una información mínima para identificar a las personas físicas que se ocultan tras la máscara de la personalidad jurídica de que están revestidas las sociedades.

– La publicidad de la información inscrita en los registros de sociedades sigue siendo necesaria para la protección de los intereses de tercero, incluso en los casos en que las sociedades hayan puesto fin a su actividad hace años, pues pueden subsistir derechos o relaciones jurídicas relativos a la sociedad o sea necesario saber quién estaba facultado para representar a la sociedad en un época concreta a los

efectos de comprobar la legalidad de un acto efectuado varios años antes o para que los terceros puedan ejercitar una acción contra los miembros de los órganos societarios o contra los liquidadores de la sociedad.

– No es posible anonimizar esa información, pues la función del registro de sociedades y el objetivo de protección de terceros hace necesaria la recopilación y conservación de datos nominativos. Y puede resultar útil a terceros compradores de inmuebles saber si la persona que dirige esta sociedad ya estaba al frente de otras sociedades en el pasado y cuál fue la trayectoria de estas sociedades

– No debe olvidarse que los datos personales de las personas físicas que operan en este registro se produce porque ellas han decidido ejercer su actividad por medio de una sociedad con personalidad jurídico. Y quien desee participar en los intercambios económicos a través de una sociedad mercantil debe estar dispuesto a hacer pública determinada información como contrapartida al ejercicio de la actividad en la forma de una sociedad que reporta de otros beneficios, incluido actuar con personalidad jurídica propia.

Y añade que el hecho de que una sociedad haya quedado sujeta a un procedimiento concursal no constituye de suyo una indicación que vulnere la reputación o el honor del administrado que la ha representado, pues la declaración de concurso puede deberse a circunstancias exteriores ajenas a la mala gestión de la sociedad.

– También rechaza la posibilidad, propuesta por la Comisión, consistente en limitar, tras un cierto periodo contado desde el cese de las actividades de la sociedad, de limitar la información inscrita en el registro de sociedades a un grupo restringido de terceros que justifiquen un interés legítimo. Y ello por entender que bajo el concepto de terceros interesados que pretende proteger la publicidad de estos registros societarios, se comprenden no solo los acreedores de la sociedad sino también, de forma más general, todas las personas que deseen obtener información sobre esta sociedad. Además se dejaría a la libre apreciación de las autoridades encargadas de la llevanza de los registros de sociedades el momento en el que se pasa de una publicidad absoluta a una publicidad selectiva, y la propia constatación de a quienes se reconoce el interés legítimo, con los riesgos de divergencias en la apreciación entre las autoridades encargadas de la llevanza de los registros de sociedades. Y finalmente porque la comprobación de la existencia de un interés legítimo del solicitante entrañaría una carga administrativa desmesurada, en tiempo y coste, difícilmente asumible por el registro y la posibilidad de que personas de otros países tuvieran dificultades de poder demostrar su interés en obtener la información que figura en el registro de sociedades, con el consiguiente efecto de disminución de su confianza en estos registros.

Madrid a 18 de noviembre de 2016