"Derechos humanos, internet y TICs", en Rey Martínez, Fernando (dir.), Los derechos humanos en España, un balance crítico, Tirant lo Blanch, Valencia, 2015, págs. 418-480

(versión previa pruebas de imprenta, acuda al original publicado)

Lorenzo Cotino Hueso (www.cotino.es), Profesor titular acreditado como Catedrático de Derecho Constitucional de la Universidad de Valencia[1]

[1] www.cotino.es (ahí puede accederse al texto completo de muchas publicaciones). El presente estudio se realiza en el marco del Proyecto MINECO "Régimen jurídico constitucional del Gobierno 2.0-Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos" (DER2012-37844), del que es investigador principal.

I. Internet, derechos y libertades y movimientos sociales en internet

1. Algunas definiciones

Se puede definir Internet como una red informática mundial descentralizada que conecta computadoras u ordenadores así como a los usuarios de dicha red[2]. Pese a que sus orígenes datan de 1969, su verdadera e incesante eclosión se da desde los años 90 con la World Wide Web (WWW, o "la Web") que hizo sencillo el acceso a recursos de texto y multimedia. Desde 2004 y en especial en los últimos tiempos, la red gira en torno a la noción de la llamada "web 2. 0[3]" o web social participativa. Más que las diferentes tecnologías o mecanismos (*Wiki, Youtube, Facebook, Twitter, blogs, posts,* etc.) se trata de un fenómeno social, basado en diferentes ideas fuerza[4] y actitudes: compartir, comunicación, participación, la web como plataforma, conversaciones, simplicidad, contenido generado por el usuario, periodismo ciudadano, filtrado colaborativo, reputación / confianza, redes sociales, remezclar, *software* social, movilidad, *creative commons,* computación social, recomendaciones, transparencia, inteligencia colectiva, etc. Frente a la web 1. 0 donde los usuarios se limitaban a la visualización pasiva de información que se les proporciona, un sitio Web 2. 0 destaca por la interactuación del usuario con otros, aportar o modificar contenidos, más que consumidores de información los usuarios activos son *prosumers*[5] de la misma[6].

2. Las dos facetas en el nexo Internet y derechos humanos

El acceso mismo a la red se perfila como contenido de uno o varios derechos humanos. En muy buena medida, las nuevas tecnologías de la información y la comunicación (en adelante TIC) son un medio espléndido para el ejercicio de las libertades públicas, esencialmente a partir de las libertad de expresión e información. El

---

[2] Definición por la *RAE*: "Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación. http://buscon. rae. es/drae/

Definición en *Wikipedia* (2011) "conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. http://es. wikipedia. org/wiki/Internet

[3] Definición en *Wikipedia* (2011) "El término Web 2. 0 (2004–actualidad) está comúnmente asociado con un fenómeno social, basado en la interacción que se logra a partir de diferentes aplicaciones en la web, que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario o D. C. U. y la colaboración en la World Wide Web. Ejemplos de la Web 2. 0 son las comunidades web, los servicios web, las aplicaciones Web, los servicios de red social, los servicios de alojamiento de videos, las wikis, blogs, mashups y folcsonomías. Un sitio Web 2. 0 permite a sus usuarios interactuar con otros usuarios o cambiar contenido del sitio web, en contraste a sitios web no-interactivos donde los usuarios se limitan a la visualización pasiva de información que se les proporciona. http://es. wikipedia. org/wiki/Web_2. 0

[4] Resulta muy recomendable seguir estas ideas fuerza en el "Mapa Visual de la Web 2. 0" http://internality. com/web20/ (ult. Visita 2011)

[5] Definición en Wikipedia (2011): "La palabra prosumidor, o también conocida como prosumer, es un acrónimo formado por la fusión original de las palabras en inglés producer (productor) y consumer (consumidor). Igualmente, se le asocia a la fusión de las palabras en inglés professional (profesional) y consumer (consumidor). http://es. wikipedia. org/wiki/Prosumidor

[6] Bowman y Willis: *We Media. How audiences are shaping the future of news and information,* Thinking Paper of The Media Center, 2005. Fumero, Antonio y Roca, Genís y Sáez Vacas, Fernando (2007): *Web 2. 0*, Fundación Orange, Madrid.

Tribunal Supremo federal de EEUU en el asunto ACLU vs Reno de 1997[7], en una antológica sentencia se aplicó a internet la protección de la libertad de expresión en su estándar más elevado, similar a la prensa escrita, El ejercicio en la red de estas libertades informativas queda en muchas ocasiones conectado con el de otras libertades como la religiosa, de asociación y partidos políticos, sindicación, libertad de empresa, etc. Conocer los países que censuran Internet en el mundo[8], según diversos informes[9] es un buen termómetro para determinar el grado de democraticidad de los Estados. Así, se consideran "enemigos" de Internet a Arabia Saudita, Birmania, China, Corea del Norte, Cuba, Egipto, Irán, Uzbekistán, Siria, Túnez, Turkmenistán y Vietnam, situándose bajo observación a Bahrein, Belarús, Corea del Sur, Emiratos Árabes Unidos, Eritrea, Malasia, Sri Lanka, Tailandia o Zimbabue. No obstante, países indudablemente democráticos como Australia o España han sido criticados en alguno de estos informes.

Como se señala en la interesante Declaración conjunta sobre libertad de expresión e internet de 2011 por altas instituciones internacionales de libertad de expresión, incluyendo la ONU y la OEA[10] (nº 6, a): "El acceso a Internet también es necesario para asegurar el respeto de otros derechos, como el derecho a la educación, la atención de la salud y el trabajo, el derecho de reunión y asociación, y el derecho a elecciones libres." En especial con la web 2. 0 también los derechos de participación o políticos así como los derechos de los administrados (transparencia, buena administración), quedan potenciados por las TIC hacia continuas vías dentro de lo que generalmente se denomina *egovernment*, democracia electrónica o, últimamente, *open government*. Por cuanto a los diversos derechos sociales prestacionales, las tics tienen un enorme potencial para el derecho a la educación y el derecho de acceso a la cultura, por ejemplo. Asimismo, las TIC son instrumento indispensable para la prestación de servicios públicos electrónicos por el gobierno y administración electrónicos. En razón de lo dicho, a los poderes públicos en general les corresponde no poner trabas al ejercicio de las libertades y derechos de participación política en la red al tiempo de potenciar la prestación de servicios electrónicos por las administraciones.

Del lado contrario, en el ciberespacio se vulneran de manera muchas veces masiva otros derechos y libertades, especialmente los derechos de la personalidad (vida, integridad, honor y, en especial, la privacidad, intimidad y protección de datos, etc.) así como la propiedad intelectual.

3. Movimientos libertarios y sociales en internet y su proyección jurídica especialmente en propiedad intelectual

Hay que desterrar una visión romántica y utópica de la red como un espacio, por sí mismo, de libertad. Una serie de factores llevaron a una comprensión libertaria y anárquica que ha dominado el mundo activista de internet[11]: la sensación psicológica de

---

[7] Texto e información en http://en. wikipedia. org/wiki/Reno_v. _American_Civil_Liberties_Union

[8] Reporteros Sin Fronteras: *Enemigos de Internet 2014*, informe anual, acceso en http://www. rsf-es. org/grandes-citas/dia-contra-censura-en-internet/

[9] Destaca el informe ante el Senado de los EEUU y las comparecencias de altos cargos de *Google* en 2010 (ult. Acceso 2011) http://judiciary. senate. gov/pdf/10-03-02Wong'sTestimony. pdf

En cualquier caso, según los parámetros que se sigan, se llega a afirmar que el 95% de los países del mundo establecen algún tipo de control y filtro de contenidos en internet. Así, véase el Mapa *Internet Censorship Around the Globe*, http://www. whoishostingthis. com/blog/2014/02/20/internet-censorship/ referido por la Asociación de Internautas, http://www. internautas. org/html/8177. html

[10] http://www. oas. org/es/cidh/expresion/showarticle. asp?artID=849&lID=2

[11] A este respecto, de manera más amplia mi trabajo "Nuevas tecnologías, desafíos y posibilidades para la libertad de expresión", publicación de la Ponencia en las III Jornadas de Derecho constitucional

libertad ante la falta de factores espaciales y contextuales, la quiebra de la identidad, el fácil anonimato o la grave dificultad que existía para controlar y perseguir los ilícitos en la red. En EEUU en el estudio de la libertad de expresión e internet destacaron firmas jurídicas como Sunstein, Balkin, Ribstein o Wu[12]. Lessig con *El Código*[13], así como en obras posteriores[14] convenció de que frente a la apariencia de internet libertario de 1995 "El ciberespacio tiene el potencial de ser el espacio más plena y extensamente regulado que hayamos conocido jamás en cualquier lugar y en cualquier momento de nuestra historia. Tiene el potencial de ser la antítesis de un espacio de libertad. Y, a menos que comprendamos este potencial, a menos que veamos cómo podría desarrollarse, es probable que no nos enteremos de esta transición de la libertad al control.[15] La clave, como expuso este autor, reside en el *código*, esto es, el conjunto de *software*, *hardware* y la configuración neutral de la red. Las amenazas a la libertad proceden de la acción de los grandes productores de estos elementos en connivencia con los Estados que tienen capacidad real de acción.

Sobre estas ideas, el movimiento libertario de la red se ha reconvertido en los defensores de *Linux*[16], del código abierto, del *Open Source* y el código libre[17]. Se trata de un verdadero movimiento social creciente y potente. Aunque cobra también expresión en partidos políticos, esta línea de acción es discreta. Así, cabe tener en cuenta los Partidos Piratas presentes en 60 países u otros partidos que se presentan con más o menos éxito a las elecciones con postulados muy vinculados a la cultura colaborativa y de internet (por ejemplo en 2014, Red ciudadana. Partido X, etc.). Diversos postulados como el acceso libre a internet y la rebaja de la propiedad intelectual se aprecian con claridad en el Movimiento Cinco Estrellas italiano. Desde la

---

"Constitución y libertad de expresión", Fundación Giménez Abad-Cortes de Aragón- UNED, Barbastro (Huesca) 7-8 de noviembre de 2008, disponible en http://goo. gl/cBkEa

[12] Sunstein, Cass R. : *República. com. Internet, democracia y libertad*, Paidós, Madrid, 2003. En inglés, *Republic. com*, Princeton University Press, 2001; Balkin, Jack M. : "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society". *New York University Law Review*, Volume 79, april 2004, n. 1, págs. 1-58, disponible en http://ssrn. com/abstract=470842 o Ribstein, Larry Edward: "Initial Reflections on the Law and Economics of Blogging" (April 4, 2005). *U Illinois Law & Economics Research Paper* No. LE05-008. http://ssrn. com/abstract=700961 También de este autor, en "*Bloggers* and Their First Amendment Protection, " vol. 57, no. 3 Otoño 2003 issue of "The Neiman Reports, " The Neiman Foundation for Journalism at Harvard University. http://www. nieman. harvard. edu/reports/03-3NRfall/95-96V57N3. pdf ; Wu, Tim: *Who Controls the Internet*, Oxford U. Press 2006, entre otros. En Reino Unido, Lipschultz, J. H. : *Free expression in the age of the internet*, Westview Press, Boulder-Oxford, 2000 o recientemente, Packard, A. , *Digital Media Law*, Willey-Blackwell, Oxford, 2010.

[13] La posición de este autor en forma extensa y razonada puede seguirse en Lessig, Lawrence, *El código y otras leyes del ciberespacio*, (Alberola Blázquez, Ernesto, trad.), Taurus, Madrid, 2001. De forma sinóptica, "Las leyes del ciberespacio", en *Cuadernos Ciberespacio y Sociedad* Nº 3, Marzo 1999 (trad. Javier Villate), del original en: cyber. harvard. edu/works/lessig/laws_cyberspace. pdf (3 abril 1998) Dispuesto para su acceso en http://goo. gl/Pgq2Pb

Asimismo, Lessig, Lawrence: *Cultura Libre. Cómo los grandes medios usan la tecnología y las leyes para encerrar la cultura y controlar la creatividad*, traducción de Antonio Córdoba/Elástico, 2004, http://www. elastico. net/archives/001222. html

[14] Se puede acceder al texto completo de muchas de ellas en http://es. wikipedia. org/wiki/Lawrence_Lessig

[15] Cita de Lessig, Lawrence: "Las leyes del ciberespacio"… cit.

[16] Popular sistema operativo *abierto* (*Windows* lo es cerrado) a partir de Linus Torvalds en Finlandia, quien se integró en el Proyecto GNU de la *Free Software Foundation*, presidida por Richard Stallman.

[17] De una manera puede afirmarse que se trata de programación que permite al usuario adentrarse en él para usarlo, estudiarlo, adaptarlo, distribuirlo y modificarlo y mejorarlo libremente. La idea es de free como libre, no como gratis.

perspectiva de los hechos, los usuarios descargan masivamente contenidos protegidos y se multiplican los medios para facilitar tales descargas. El Gobierno de EEUU elabora anualmente la famosa lista 301[18] sobre la persecución que se hace en cada país frente a los ataques a la propiedad intelectual, especialmente a través de internet. España estuvo en esta lista negra desde 2008 hasta 2011, si bien las medidas como la llamada Ley Sinde y después el Decreto Wert, por referencia a los respectivos ministros socialista y popular, permitieron que España saliera de esta lista negra.

Estos moviemientos tienen expresiones fácticas como determinados delitos de hacking llevados a cabo por comunidades o grupos ciberactivistas, como por ejemplo *Anonymous*. Más allá de estas conductas, desde estos movimientos sedefienden las licencias de uso por la que los autores renuncian a sus derechos de propiedad intelectual de forma condicionada a través Licencias GNU[19] o las *creative commons* (diseñadas por Lessig)[20]. Del otro lado, en razón de este choque libertad de expresión – propiedad intelectual, no es fortuito que las grandes batallas jurídicas por la libertad de expresión en la red se libren en EEUU –y a menor escala en otros lugares como España o Francia- entre activistas y grandes medios de comunicación y contenidos o entidades de defensa y gestión de la propiedad intelectual. En este contexto, no tuvieron éxito ante el TS de Estados Unidos la pugna de los internautas contra la *Digital Millennium Copyright Act* de 1998 o la *Sonny Bono Copyright Term Extension Act* de 1998 en el caso *Eldred vs. Ashcroft* sentencia de 15 de enero de 2003)[21]. Se trató de un supuesto defendido por el propio Lessig ante el TS, que no obstante, consideró que la *Digital Millenium Copyright Act* no vulneraba la libertad de expresión.

En Europa quizá el hito más destacable fue la Decisión nº 2009-580 de 10 de junio de 2009 [22] del Consejo Constitucional francés por la que se declaró inconstitucional la llamada Ley Hadopi I, Ley que favorece la difusión y la protección de la creación en Internet y permitía la sanción administrativa de corte de acceso a internet. Ahí se dijo algo obvio: el acceso y uso de Internet está protegido por la libertad de expresión e información y la sanción del corte de acceso a este servicio debe ser decretada por un Juez. La reacción fue crear un procedimiento penal con garantías judiciales en la Ley Hadopi II. También es llamativo el caso alemán, donde una ley que permitía el control de contenidos en internet, aprobada en 2009 nunca ha llegado a aplicarse [23]. En Colombia, la responsabilidad por los contenidos ilícitos quedó desregulada tras el fracaso de la llamada Ley Lleras[24].

---

[18] Oficina para la Defensa de los Intereses Comerciales de Estados Unidos (USTR), *Informe anual 'Special 301* Acceso en http://www. iipa. com/special301. html

[19] De la Fundación para el Software Libre, www. gnu. org.

[20] www. creativecommons. org.

[21] Al respecto, cabe seguir toda la descripción de la *lucha* ante el Tribunal Supremo por Lessig en Sobre este tema en particular Lessig, Lawrence: *Cultura Libre. ... cit.*

[22] Puede seguirse una descripción completa por mí realizada en http://goo. gl/hDgH4j

[23] El 18 de Junio de 2009 fue expedida por el Parlamento Federal alemán la ley para dificultar el acceso a contenidos de pornografía infantil en las redes de comunicación. Esta ley tenía un periodo de prueba hasta finales de 2012, si bien se dictó el 5 de abril una orden de no aplicación externa y finalmente fue derogada sin aplicarse. Al respecto, Sänger, Raffael, "El bloqueo de páginas web en el Derecho alemán, a través del ejemplo de la ley para dificultar el acceso a páginas web", en Corredoira y Alfonso, Loreto y Cotino Hueso, Lorenzo, (eds.) *Libertad de expresión e información en Internet, cit.*

[24] La fuerte reacción a la llamada ley Lleras (Proyecto de ley 241 de 2011 "Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en internet") conllevó una sentencia de inconstitucionalidad formal y, finalmente, a que la materia del control de contenidos en aquel país quedase finalmente sin regulación alguna.

La literatura científica sobre la materia en España[25] es relativamente discreta en comparación con la siempre más rentable atención del fenómeno de la protección de datos. En España los "internautas" (en su sentido de activistas del referido movimiento en la red) suelen celebrar como victorias éxitos jurídicos como la no persecución por el Ministerio Fiscal ni de páginas web de enlaces ni a los usuarios de las mismas (Circular 1/2006 de la Fiscalía General del Estado) [26], o la no consideración judicial de la lesión de la propiedad intelectual en la mayoría de casos de páginas de enlaces como los casos *Sharemula*, *Elitedivx, Rincón de Jesús*, *Indicedonkey, Estrenosdivx, Cinetube*, a los que han sucedido muchos más[27]. O la batalla jurídica frente al canon impuesto a los soportes digitales, declarado parcialmente ilegal en 2010 por el TJUE[28] y que fue eliminado en 2011. También se consideraron como éxitos las dificultades que impone el TJUE para acceder a datos de tráfico de internet para perseguir ilícitos civiles (caso *Promusicae*[29]) o la prohibición de imponer controles automáticos de contenidos a los servicios de internet para proteger la propiedad intelectual.

En España, estas medidas normativas de protección de la propiedad intelectual se intensificaron bajo la presión de EEUU (como se puso de manifiesto a través de los cables revelados por *Wikileaks*)[30]. Se trató de la políticamente convulsa "ley Sinde" (por la entonces ministra de cultura socialista Sinde), que fue rechazada por el Senado y posteriormente modificada para lograr el apoyo de partidos de la oposición. Con la "ley Sinde" y a través de diversas reformas legales se creó un órgano administrativo (la Sección 2ª de Propiedad intelectual) que tras un procedimiento puede resolver el cierre o bloqueo de una página web por permitir el acceso ilegal a contenidos protegidos por propiedad intelectual. Puede incluso señalarse que el movimiento 15-m tuvo su germen en las reacciones en internet y las redes sociales articuladas en contra de esta ley[31]. Las reacciones sociales frente a esta legislación obligaron a introducir hasta dos garantías judiciales para velar por la libertad de expresión o por la privacidad en estos procedimientos, poniendo aún más en cuestión la efectividad práctica de estas medidas[32]. En 2011 se aprobó tal "ley Sinde", si bien el gobierno socialista que se sabía

[25] En España, además de los trabajos de quien suscribe, hay que destacar los trabajos iniciales de Fernández Esteban, los numerosos de Boix Palop, el clásico de Villate, así como los de José Julio Fernández, Loreto Corredoira, García Morales y Villaverde Menéndez entre otros.

[26] Circular 1/2006 de la General del Estado, que dice: "las conductas relacionadas con la utilización de nuevas tecnologías, para la comunicación u obtención de obras protegidas, tales como las de "colocar en la Red o bajar de Internet" o las de intercambio de archivos través del sistema "P2P", sin perjuicio de poder constituir un ilícito civil, frente al que los titulares podrán ejercitar las correspondientes acciones en dicha vía, no tienen, en principio, los requisitos para su incriminación penal si no concurre en ellas un ánimo de lucro comercial.

[27] Pueden seguirse numerosas de estas resoluciones en http://www. bufetalmeida. com/51/sentencias-propiedad-intelectual

[28] Acceso completo en http://goo. gl/ek1Zy1

[29] Sentencia del Tribunal de Justicia (Gran Sala), de 29 de enero de 2008, asunto C275/06, Productores de Música de España (Promusicae), Telefónica de España, S. A. U. , que concluye que las normas comunitarias "no obligan a los Estados miembros a imponer, […] el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Esto es, que sólo en procedimientos penales cabría imponerse la revelación de los datos de tráfico.

[30] Así puede seguirse por ejemplo en *El* País (3. 2. 2010), "EE UU ejecutó un plan para conseguir una ley antidescargas", acceso en http://goo. gl/oByKpG

[31] El movimiento internauta *No les votes*, nació en respuesta a la Ley Sinde y estuvo en el origen de las primeras movilizaciones. Al respecto, entre otros muchos "Así nació el 15-m" en *ABC* de 22. 5. 2011, http://goo. gl/2xdOpy

[32] Desde 2009 se inició la polémica sobre la protección de la libertad de expresión frente al cierre de página web por un órgano administrativo, lo cual llevó a que se introdujera el procedimiento especial

saliente, no se atrevió a aprobar el necesario procedimiento reglamentario. Una de las primeras medidas Gobierno popular[33] a final de 2011 fue el desarrollo reglamentario de esta ley al tiempo de suprimirse el también polémico canon digital. Estas normas lograron atemperar las críticas y presiones de Estados Unidos y sacaron a España de la referida lista 301. No obstante, la efectividad práctica o simbólica contra la piratería es más que relativa[34].

Desde 2012 existen anteproyectos e iniciativas de reforma. De un lado, del Código penal (proyecto de ley de septiembre de 2013) para perseguir penalmente a las webs de enlaces. Del otro lado, la llamada "ley Lassalle" de reforma de ley de propiedad intelectual (proyecto de ley de febrero de 2014), entre otras cosas, persigue restringir mucho las posibilidades de difundir "copias privadas" y deja clara la ilegalidad de cualquier difusión de obras protegidas en internet, al tiempo que se refuerza mucho las posibilidades de persecución, sanción y cierre efectivo de webs que faciliten enlaces a obras protegidas.

Del lado contrario, se ha criticado y a mi juicio no sin razón, la corriente jurisprudencial iniciada precisamente con la condena a la Asociación de Internautas frente a la SGAE[35], que tiende a responsabilizar a los intermediarios por los contenidos ilícitos de terceros que difunden o alojan por no extremar precauciones frente a los mismos. Como se verá, esta corriente confluye con la del TEDH.

II. El acceso a Internet como nuevo derecho fundamental y sus garantías. La no discriminación en el acceso a los servicios públicos electrónicos

de protección de derechos fundamentales para que un juez pudiera autorizar la resolución administrativa que declaraba el cierre de una web en razón del procedimiento. Pese a toda la polémica suscitada, hasta el momento de cerrar estas páginas en 2014, sólo se conoce una ocasión en la que se ha seguido este procedimiento judicial de garantía. Se trata de una resolución judicial de la Audiencia Nacional en 2014 respecto del cierre de www. goear. es. Y la justicia ha fallado en contra del cierre de la web. Ver http://goo. gl/fg81yn

Para lograr el apoyo del Partido Popular y Convergència i Uniò (que inicialmente votaron en contra de la ley) se introdujo otra posible intervención judicial para velar por la privacidad en la investigación de las páginas web de enlaces (nuevo párrafo 2º, artículo 8 Ley 34/2002, de 11 de julio).

[33] Se trata esencialmente del Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual. Al mismo momento se suprimió el canon digital a través de la Disp. 10ª del Real Decreto-ley 20/2011, de 30 de diciembre.

[34] Según una respuesta del Gobierno a pregunta parlamentaria en enero de 2014 la Sección segunda de propiedad intelectual ha resuelto 316 de las 394 solicitudes presentadas suponiendo la retirada de contenidos 85 páginas, así como el cese de actividades de 15 de ellas. Son cientos las webs de enlaces y millones los enlaces que apuntan continuamente a contenidos protegidos por la propiedad intelectual.

[35] SSTS de la Sala 1ª Civil 773/2009, de 9/12/2009 (caso *Putasgae-Asociación de internautas*); STS 316/2010, de 18/05/2010 (caso *Quejasonline*); STS 72/2011, de 10/02/2011 (caso *Alasbarricadas*); STS 172/2012, de 3/04/2012 (caso *Megakini*, sobre art. 15); STS 742/2012 de 4/12/2012 de 4 de diciembre de 2012, (caso *Merodeando*, sobre el art. 17); STS 128/2013 de 26/2/2013 (caso *foro de El Economista*) o STS 144/2013 de 4/3/2013 (caso *Operación Malaya en Google*). El TS en 2013 señala que "la entidad demandada, como titular de la página web y creadora del foro de debate abierto, debió extremar las precauciones y ejercer un mayor control sobre las opiniones y comentarios alojados, cuyas connotaciones despectivas y peyorativas para el demandante no podían pasarle inadvertidas" (FJ 4º).

1. El acceso a internet y la dimensión prestacional del nuevo derecho fundamental de acceso a la red

Al menos en las sociedades occidentales, internet se ha convertido en algo "esencial para la vida", tal y como afirmó el TS alemán el 24 de enero de 2013[36]. Y los datos no hacen más que confirmar esta tendencia. Aunque en general el acceso ronda el 70%, en 2013 en España[37] unos 19 millones de españoles "viven conectados" a internet y consultan el móvil unas 150 veces al día. El 53, 8% de la población se conecta a diario, siendo el 86% de los jóvenes entre 16 a 24 años. Veinticinco millones de españoles acceden a Internet, y las redes sociales forman parte de la vida del 64, 1% de los usuarios (del 95% de los jóvenes entre 16 a 24 años). Por cuanto a los usos administrativos, el 45% de la ciudadanía interactuó con las Administraciones Públicas a través de internet.

En términos comparativos relativos a 2012, los conectados a internet en España son el 67, 2% (38. 7% en 2006[38]), con 17, 5 millones de usuarios de Facebook, ocupando un lugar medio en la Unión Europea frente a países como Holanda (93%) o Noruega (96, 9%).

A finales del 2012 en el mundo alrededor de 2. 500 millones de personas estaban en línea (incremento del 10% anual), 241 millones más que el año anterior[39]. La media de acceso en Europa, según esos datos es de 63% y de Norte América 78%. En 2013 se estima que casi el 40% de la población mundial estaba conectada a Internet. El porcentaje de personas que utilizan Internet en los países desarrollados alcanzó a finales del 2012 el 73, 4%. En términos absolutos, casi la mitad de los conectados a internet en el mundo son en Asia Pacífico, siendo 1. 133 millones en 2012[40].

Pues bien, no todas las personas quieren o pueden conectarse a internet y hoy por hoy la red reproduce, incluso intensifica, las pautas de marginalidad social no virtuales. Es necesario mostrar atención jurídica a la "informarginalidad", "muro", "telón" o, más habitual, "brecha digital" tanto social o territorial y su obvia conexión con la implantación de la democracia y participación electrónicas. Los sectores más marginados son precisamente los más necesitados de representación y de que el interés general se conforme sobre la base de sus necesidades. Y, sin embargo, estos sectores son los que menos acceden a la red o lo hacen con menor eficacia. De ahí que, al igual que en la implantación de servicios públicos a través de internet, ha de tenerse especial cautela con la no discriminación.

Cada vez tiene más acogida la afirmación de un derecho fundamental de acceso a internet (*ius comunicationis*). Así, a partir del artículo 19 de la Declaración Universal de Derechos Humanos interpretado por Naciones Unidas en la *Declaración de Ginebra* de 2003 y la *Declaración de Principios* Túnez de 2005 que afirmaron el "derecho de acceso como acceso universal". Más recientemente destacan dos importantes documentos y declaraciones internacionales. La antecitada Declaración conjunta sobre

---

[36] Se trata de la sentencia de la Sala Civil de 24 de Enero 2013 - III ZR 98/12, a los efectos de determinar la compensación que corresponde por la interrupción del servicio de internet, que es "esencial para la vida". Acceso al texto en http://juris. bundesgerichtshof. de/cgi-bin/rechtsprechung/list. py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288

[37] Telefónica: *Informe anual 2013 La Sociedad de la Información en España*, (14ª edición). Acceso en http://www. fundacion. telefonica. com/es/arte_cultura/publicaciones/sie/sie2013. htm

[38] Datos de junio 2012, http://www. internetworldstats. com/stats. htm

[39] Telefónica: *Informe anual 2013,* cit. págs. 34 y ss. con referencias a Eurostat-ONTSI ("Indicadores Destacados de Sociedad de la Información"- Septiembre 2013).

[40] Datos de ITU Statistics 2012 (http://www. itu. int/ict/statistics).

libertad de expresión e internet de 2011 destaca el su apartado 6 cuando afirma la "obligación positiva de facilitar el acceso universal a Internet". A partir de esta obligación general dimanan una serie de obligaciones concretas, unos mínimos de acción: "establecer mecanismos regulatorios ", creación de "puntos de acceso público", asegurar "el acceso equitativo a Internet para personas con discapacidad y los sectores menos favorecidos" y para todo ello, "adoptar planes de acción detallados".

También en 2011 destaca el Informe del Relator Especial a la Asamblea de Naciones Unidas de 16 de mayo de 2011 sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue (uno de los autores de la anterior declaración). Ahí se proclama el "derecho de todas las personas a buscar, recibir y difundir información e ideas de todo tipo por Internet. Y respecto del acceso a internet se formula la obligación de (nº 85) "elaborar una política eficaz y concreta en consulta con personas de todos los sectores de la sociedad, entre ellos el sector privado, y con los ministerios gubernamentales competentes, a fin de que Internet resulte ampliamente disponible, accesible y asequible para todos los sectores de la población. En la Unión Europea el acceso a Internet se garantizó especialmente merced al artículo 3. 1º de la Directiva 2002/22/CE que exige la garantía a un acceso de calidad y a un precio asequible, lo cual se ha ido recogiendo en las diversas normas nacionales de comunicaciones. En Finlandia, la reforma de la Ley del Mercado de las Comunicaciones de 2009 reconoció el "derecho básico" al acceso a Internet de una banda ancha de 1 MB como mínimo y de 100 Mb en 2015. También como hito mencionable, el 30 de julio 2010 un fallo de la Corte Suprema de Costa Rica declaró que internet es la "herramienta básica para facilitar el ejercicio de los derechos fundamentales y la participación democrática y el control ciudadano, la educación, la libertad de pensamiento y de expresión, el acceso a la información y los servicios públicos en línea, el derecho a comunicarse con gobierno electrónico y transparencia administrativa, entre otros. Esto incluye el derecho fundamental de acceso a estas tecnologías, en particular, el derecho de acceso a la Internet o la World Wide Web".

En España, este derecho de acceso se recogió en la histórica declaración de derechos de las Conclusiones de la Comisión Especial de Redes Informáticas del Senado de España[41], de 1999. Años más tarde este derecho tuvo clara acogida en el Estatuto de la Comunidad Valenciana en su artículo 19. 2º: *"Queda garantizado el derecho de acceso de los valencianos a las nuevas tecnologías y a que La Generalitat desarrolle políticas activas que impulsen la formación, las infraestructuras y su utilización.* Otros estatutos vinieron a emular este derecho. Más que derechos subjetivos exigibles, éstas y otras proclamaciones pueden tener cierto valor simbólico o impulsor de políticas de fomento de internet de universalización del acceso a internet, de extensión territorial o social de servicios, etc. Y bien es cierto que este peso jurídico puede en su caso servir para justificar la restricción otros derechos subjetivos en conflicto.

2. Garantías frente al cierre de webs o al corte de acceso o filtrado de contenidos en internet

El naciente derecho fundamental de acceso a internet incluye también garantías frente al corte de suministro o de acceso a la información. Así, la varias veces citada Declaración conjunta sobre libertad de expresión e internet de 2011, aun sin valor jurídico en su apartado 6 dispone:

[41] Acceso en http://www. internautas. org/documentos/decla_dere. htm

"b. La interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional. Lo mismo se aplica a las medidas de reducción de la velocidad de navegación de Internet o de partes de este.

c. La negación del derecho de acceso a Internet, a modo de sanción, constituye una medida extrema que solo podría estar justificada cuando no existan otras medidas menos restrictivas y siempre que haya sido ordenada por la justicia, teniendo en cuenta su impacto para el ejercicio de los derechos humanos.

En cualquier caso, no hace falta acudir a un nuevo derecho fundamental, puesto una medida de restricción del acceso a las TIC debe ser considerada como limitación a la libertad de expresión y de emitir y recibir información con las garantías legales y judiciales que ello comporta. En este sentido, cabe destacar la Decisión nº 2009-580 de 10 de junio de 2009 del Consejo Constitucional francés respecto de la ya mencionada Ley Hadopi I. El máximo intérprete de la Constitución gala afirmó con rotundidad que la libertad de expresión incluye el derecho de acceder a los servicios de internet, dado "su desarrollo generalizado" y "la importancia de estos servicios para la participación en la vida democrática y la expresión de ideas y opiniones" (nº 12). Sobre esta base, una autoridad administrativa y no judicial no puede aplicar sanciones de corte de suministro de internet, pues suponen una restricción de la libertad de expresión, que sólo lo puede hacer un juez.

Asimismo, no puede ordenarse a los prestadores que bloqueen contenidos sin discriminar entre los que son lícitos y los ilícitos y para que se adopten medidas de bloqueo es necesaria una regulación legal que dé previsibilidad, certeza y garantías suficientes en la materia. En este sentido, la STEDH de 18 de diciembre de 2012 en el asunto Ahmet Yıldırım c. Turquía ha sido la primera de este alto tribunal que aborda la libertad de expresión en internet. Se entiende que viola la libertad de expresión la imposición –judicial- de medidas de bloqueo de acceso a contenidos en internet que no discriminaron contenidos del sitio de internet implicado en un proceso penal y los de otros sitios del servicio *Google* sites con contenidos al margen de dicho proceso. El TEDH aprovecha la ocasión para fijar algunos parámetros de la regulación del bloqueo de contenidos en internet (aps. 64 y ss.).

En marzo de 2014 el presidente turco Recep Tayyip Erdogan ordenó bloquear Twitter en su país y días después Youtube, porque no filtraron unos contenidos concretos que consideraba ilegales. Esta carrera bloqueadora fue detenida judicialmente por la justifica ordinaria y por el Tribunal Constitucional turco.

Además de lo indicado, no puede imponerse a los prestadores o intermediarios que establezcan controles o filtrados técnicos de contenidos en internet sin distinguir entre contenidos lícitos o ilícitos. Las sentencias del TJUE de 24 de noviembre de 2011, Asunto C-70/2010, Scarlet Extended vs SABAM y Asunto C-360/10 SABAM vs Netlog de 16 de febrero de 2012 no permiten que judicialmente se impongan controles y filtrados técnicos y preventivos a prestadores de servicios y redes sociales para evitar la comisión de ilícitos de propiedad intelectual y protección de datos. El TJUE considera que deben prevalecer la libertad de expresión y la protección de los usuarios que serían controlados y rastreados, así como la libertad de empresa frente a la imposición de estos controles "dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito". Sin perjuicio de lo

anterior, en razón de sentencia del TJUE de 27 de marzo de 2014[42], sí que es posible que un juez solicite a un proveedor de acceso a Internet que bloquee el acceso de sus clientes a un sitio web que vulnera los derechos de autor. Se afirma cuanto menos que las medidas de bloqueo de acceso a los usuarios "no priven inútilmente a los usuarios de Internet de la posibilidad de acceder de forma lícita a la información disponible" (nº 63) y que "tanto los internautas como también el proveedor de acceso a Internet deben poder hacer valer sus derechos ante el juez" (nº 54). No obstante, no es necesario probar que los usuarios del servicio acceden efectivamente a los contenidos ilegales.

En España al menos en dos ocasiones se han adoptado medidas individualizadas judiciales para impedir el acceso a internet, en ambos casos fruto de cierto activismo judicial sin un marco legal claro. Así, la sentencia del Juzgado de lo Penal nº 2 de Huelva de 17 de octubre de 2012, respecto de un condenado por delito sexual en la red impuso a los proveedores de acceso a internet de todo el país la prohibición de facilitar al condenado acceso a Internet. En otro marco, la Audiencia Provincial de Barcelona en su sentencia 470/2013 de la Secc. 15ª, de 18 de diciembre de 2013, ordenó al operador de telecomunicaciones suspender "de inmediato y de forma definitiva la prestación del servicio de acceso a Internet" a uno de sus usuarios. La base legal (arts. 138 y 139. 1. h) de la Ley de Propiedad Intelectual es discutible y no había sido antes aplicada.

Respecto del bloqueo o cierre de una página web en España, la ley de internet, Ley 34/2002 en su artículo 8 no deja clara la cuestión de si es necesaria la autoridad judicial:

"En todos los casos en los que la Constitución y las Leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo, en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información.

Y lo cierto es que hasta 2010 ninguna ley expresaba la garantía judicial para cerrar una web. En 2010, como medida contra la piratería informática la Ley de economía sostenible estableció un sistema para decretar por una entidad administrativa el cierre de webs que enlacen a contenidos ilícitos, en la llamada ley Sinde. Sin embargo, se le añadió una intervención judicial: "Acordada la medida por la Comisión, se solicitará del Juzgado competente la autorización para su ejecución, referida a la posible afectación a los derechos y libertades garantizados en el artículo 20 de la Constitución. (art. 122 bis Ley 29/1998). Es interesante destacar que en el trámite de aprobación, el Consejo de Estado y el Consejo General del Poder Judicial dieron por hecho que la Constitución impone la garantía judicial para impedir el acceso a una página web[43].

Frente a esta cuestión más polémica, ha pasado desapercibido que una Administración, la Agencia de protección de datos no tiene problema en decretar sanciones muy relevantes por difusión ilícita de datos personales en webs, esto es, por informar sobre otras personas. Es más, en la instrucción de procedimientos relativos a una página web o los contenidos de una red social, la Agencia puede requerir la cesación de la difusión de datos personales, o inmovilizar directamente, en otras palabras, puede bloquear el acceso o cerrar una web (art. 49 LOPD). Se hace impensable que esto pudiera hacerlo una Administración respecto de los medios

[42] Sentencia TJUE de 27 de marzo de 2014 asunto C 314/12 UPC Telekabel Wien GmbH / Constantin Film Verleih GmbH y Wega Filmproduktionsgesellschaft mb.

[43] Con facilidad puede seguirse en http://www.cotino.net/2010/03/consejo-de-estado-ley-de-economia-sostenible-y-cierre-de-webs/

clásicos de comunicación. El Tribunal Constitucional español en modo alguno ha dejado claros los términos en que un control administrativo de contenidos es posible[44], pese a que parece que se está generalizando en la red.

A mi juicio, no todo es libertad de expresión e información en internet y, por tanto, no toda restricción de acceso a contenidos de la red requerirá de la garantía judicial. La clave reside básicamente en el interés o relevancia pública de la información, que es lo que ha de hacer más intensa la protección de la misma, y no ya el sujeto que transmite tal información (medios de comunicación clásicos). Así las cosas, en terrenos más distantes del ejercicio de la libertad de expresión e información, como por ejemplo, en la oferta de bienes y servicios a través de internet y el consumo, no hay que excluir las resoluciones administrativas que puedan afectar a contendidos en internet siempre con la previsión legal exigible y la siempre posible revisión judicial.

3. La no discriminación en la implantación de la Administración electrónica y las obligaciones de relacionarse exclusivamente por medios electrónicos

Desde el punto de vista jurídico, desde el principio de igualdad debe garantizarse que la implantación de servicios electrónicos por las Administraciones públicas no genere discriminaciones. Ahora bien, el avance de las nuevas tecnologías siempre va a dotar de más posibilidades a quien accede a las mismas que a quien no quiere o no puede hacerlo. El ciudadano conectado, lógicamente, siempre contará con más y mejor información. Considerar *per se* esto discriminatorio frenaría, de forma absurda, el avance de la sociedad de la información y conocimiento. En general, dotar de ventajas al internauta no debe considerarse discriminatorio, siempre que ello no implique una clara desventaja, incluso castigo a quien no está conectado. El tratamiento jurídico no es en modo alguno sencillo y es preciso ir al caso concreto. Por ejemplo, cabe preguntarse si sería discriminatorio que la devolución del IRPF se practique antes, como así parece ser, a quienes presentan su declaración vía electrónica. La mayor agilidad en la tramitación del procedimiento puede justificar este tipo de tratos favorables. También cabe cuestionarse si una tasa puede ser menor cuando el ciudadano reciba un servicio electrónico que tenga menos costes para la Administración que cuando lo presta en *papel.*

A mi juicio, las discriminaciones más relevantes pueden generarse por obligar a la ciudadanía a relacionarse exclusivamente por medios electrónicos con la Administración. A ello da cobertura el artículo 27. 6º de la ya Ley 11/2007 que regula la e-administración:

"6. Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

Cabe tener en cuenta que respecto de la relación electrónica con la Administración hay un claro mandato de garantías de acceso a todos a las TIC (art. 8):

"1. Las Administraciones Públicas deberán habilitar diferentes canales o medios para la prestación de los servicios electrónicos, garantizando en todo caso el acceso a

[44] Se dan algunas directrices en la STC 52/1995, de 23 febrero (FJ 4º, que sea una ley formal la que autorice al poder público y que la resolución sea motivada.). Por el contrario la STC 187/1999, de 25 octubre (caso "La máquina de la verdad"), hace dudar de cualquier control no judicial de contenidos (FJ 6º).

los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

Pues bien, el artículo 27. 6º impone que sea un reglamento el que imponga la obligación de relacionarse electrónicamente con la Administración. Cabe recordar que las bases de un concurso, contratación o beca, por ejemplo, no tienen naturaleza reglamentaria aunque se adopten a través de Decretos u Órdenes. Asimismo, la norma reglamentaria que imponga la relación electrónica debe determinar suficientemente la tipología de procedimientos que son obligatorios para la ciudadanía, así como los colectivos que quedan sujetos a la obligación, evitando fórmulas genéricas.

El tema es más sensible de lo que pueda parecer, puesto que hoy día millones de pequeñas empresas o empresarios autónomos, o comunidades de propietarios quedan obligados a que se les notifiquen electrónicamente, por ejemplo, las multas de tráfico o comunicaciones con Hacienda, respectivamente. La sentencia 59/2010 de 29 enero del TSJ Castilla y León anuló la imposición de la relación electrónica a una empresa de la construcción. Se entiende que sobre la base de un derecho reconocido a la relación electrónica (art. 6 Ley 11/2007), la posibilidad de imponer la interactuación es excepcional y por tanto debe ser interpretada de forma restrictiva. Ni la norma estatal ni las normas autonómicas o locales tampoco ofrecen muchas luces ni garantías sobre la obligatoriedad de medios electrónicos[45].

Así pues, quien apruebe la norma reglamentaria que establezca la obligación de medios electrónicos debe efectuar una constatación probada de que ello no implica riesgos de exclusión. Y considero que esta garantía debería darse también para la tan generalizada práctica de obligar a utilizar una plantilla en internet para generar y completar una solicitud, sin perjuicio de que luego pueda presentarse el escrito en papel en la Administración presencial.

III. Algunos retos de la privacidad, el secreto de las comunicaciones y la protección de datos en el entorno digital

1. Nuevos derechos y redefinición de los ya clásicos para el entorno digital. La conflictiva cuestión de los datos de tráfico y de geolocalización

Si bien internet facilita el ejercicio de las libertades públicas, del lado contrario, los medios informáticos potencian también los peligros respecto de los derechos de la personalidad. Así, la intimidad, la protección de datos, el secreto de las comunicaciones, el honor e incluso la integridad física y, especialmente la moral, quedan exponencialmente en peligro. Precisamente, el derecho de protección de datos personales, "nace" en los años ochenta para intentar dar especial respuesta a los particulares peligros informáticos. Y desde entonces se ha ido constitucionalizando expresa o implícitamente en un proceso que en España culminó con la sentencia 292/2000, auténtico certificado de nacimiento de un derecho fundamental en nuestro país. Para la protección específica de este derecho se han generalizado autoridades administrativas independientes, lo cual incluso se ha constitucionalizado (art. 8. 3º Carta

[45] A salvo del futuro Decreto de e-administración de la Comunidad Valenciana que sí que incluye previsiones específicas y novedosas al respecto, quizá únicamente cabe mencionar la Ordenanza de Administración electrónica de Zaragoza sí que incluye algunas concreciones. Pese a que facilita mucho la imposición de medios electrónicos a cualquier solicitante de subvenciones o asociaciones, su apartado 2º incluye una garantía formal que puede evitar tal discriminación con la obligación de "informar con carácter previo a los afectados a través de sus colegios o asociaciones profesionales y otorgar un plazo de adaptación adecuado, antes de implantar plenamente la obligatoriedad del uso de medios electrónicos.

UE[46]). Es más, estas autoridades independientes de protección de datos hoy día y por lo general rebasan su ámbito de actuación para adentrarse en la privacidad en general. Además, en muchas ocasiones –por ejemplo Alemania, Gran Bretaña o recientemente Andalucía- la ley les atribuye funciones relativas a otro derecho fundamental emergente cual es el acceso a la información pública. Además del derecho de protección de datos personales, en Alemania incluso se ha reconocido otro nuevo derecho, como el derecho fundamental frente al registro oculto en línea. Así sucedió en la sentencia del Tribunal Constitucional Federal alemán de 27 de febrero de 2008[47].

Más allá de la emergencia de nuevos derechos, la informática e internet han forzado también la reinterpretación de derechos ya clásicos y obligan a su readecuación a los nuevos contextos. Como punto de partida, derechos clásicos, como el derecho a la intimidad y la protección de datos pasan a afectar casi "por defecto" a todas las cuestiones de control laboral, policial o judicial de los datos y comunicaciones de ordenadores, *tablets*, *smartphones*, etc. Asimismo, el secreto de las comunicaciones adquiere nuevas dimensiones y genera complejas cuestiones. Así, resulta especialmente difícil el tratamiento de los llamados datos de tráfico y geolocalización que generan las comunicaciones de telefonía móvil y el rastro de la navegación en la red. Desde el ataque terrorista del 11-S en general (2001) y tras el 11-M en Madrid (2004) y el 7-J en Londres (2005) en Europa, surgieron normativas que obligan a la retención masiva de estos datos para la investigación por los cuerpos y agencias de seguridad e inteligencia. Así, en la Unión Europea se adoptó la Directiva 2006/24/CE de retención de datos de las comunicaciones. En este punto, cabe tener en cuenta la ya histórica STJUE (Gran Sala) de 8 de abril de 2014[48] que declara esta Directiva es contraria a la intimidad, vida privada y protección de datos.

Por lo que respecta a España, es compleja la cuestión del grado de afectación de la sentencia respecto de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Cabe recordar que aunque prácticamente a nadie le ha importado, esta ley ya era dudosamente constitucional formalmente por no tratarse de una ley orgánica. A este respecto, la sentencia del TJUE evidencia que se trata de una restricción directa de derechos fundamentales que en razón de nuestro derecho interno debiera ser regulada por ley orgánica. Asimismo, en razón de la STJUE se hace más clara la inconstitucionalidad de esta ley interna española por la falta de precisión de los tipos de delitos (los "graves", art. 1. 1º) respecto de los cuales es posible acceder a los datos de tráfico y geolocalización retenidos[49]. No parecen presentar tantos problemas las cuestiones sobre la garantía jurisdiccional –dado que la Ley 25/2007 reguló la intervención judicial. Tampoco en España parece polémico el límite del tiempo de conservación de los datos retenidos –dado que el legislador eligió el periodo de 12 meses, que parece que entra en la razonabilidad del TJUE. En cualquier caso, sería del todo deseable en España una revisión legislativa tras la sentencia. Respecto de los datos de tráfico y geolocalización, de tanta importancia para la investigación, cabe también

[46] "Artículo 8. Protección de datos de carácter personal: […] 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

[47] Acceso completo en inglés en http://goo. gl/Yb8cH6

[48] Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros (C-594/12) / Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irlanda y el Attorney General.

[49] De todo interés teórico y práctico la Circular de la Fiscalía General del Estado 1/2013, de 11 de enero de, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas.

tener en cuenta la importante Convención internacional sobre el Cibercrimen, de 2001[50], del ámbito del Consejo de Europa. Dicha convención facilita la posibilidad de acceder a los diversos datos contra la comisión de delitos.

2. La readecuación del secreto de las comunicaciones a las comunicaciones electrónicas y la imperiosa necesidad de la acción legislativa

En cuestión de controlo de las comunicaciones se hace plamaria la necesidad de mejorar nuestra muy deficiente legislación procesal. Cabe remitir a los excelentes y numerosos trabajos de Juan José González López. Especialmente ha destacado este autor quien, desde antiguo, alerta tanto de las carencias existentes al tiempo de hacer propuestas de actualización de nuestro Derecho procesal y policial que, de momento, caen en saco roto.

Entre los temas de especial interés, desde las SSTEDH del Caso Malone de 1984 y Caso Valenzuela de 1998, queda claro que los datos relativos a las circunstancias de la comunicación (tiempo, modo y lugar de ésta) sí que están amparados por el secreto. Ello sería aplicable a los datos de tráfico y de geolocalización, lo cual conlleva la exigencia de las garantías judiciales pertinentes. Del otro lado, y a mi juicio de mayor importancia, no está en modo alguno claro si las comunicaciones ya realizadas quedan protegidas por este derecho. De así ser, las comunicaciones ya finalizadas quedarías simplemente amparadas por las más débiles garantías del derecho a la intimidad, que no incluyen -de natural- la previa garantía judicial. La primera opción, esto es, que el secreto de las comunicaciones sí que protege las comunicaciones ya realizadas, parece que es la seguida en SSTEDH de 3 de abril de 2007 (caso Copland vs. Reino Unido, asunto 62617/00), de 16 de octubre de 2007 (caso Wieser y Bicos Beiligungen GMBH vs. Austria, asunto 74336/01); de 22 de mayo de 2008 (caso Ililla Stefanov vs. Bulgaria, asunto 65755/01) de 10 de marzo de 2009 (caso Bykov vs. Rusia, asunto 4378/02). No obstante, esta línea viene a chocar con el Tribunal Constitucional español hasta la fecha, así por ejemplo en STC 70/2002: "la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos", de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en el proceso de comunicación (precisión que también se recoge en la STC 56/2003). Este parecer ha sido reiterado, aunque si se me permite, con la *boca pequeña*, en sentencias de 2013 a las que luego se alude. Para hacerse cargo de la importancia de la cuestión, se trata al fin y al cabo de saber si es necesaria la garantía judicial para acceder a las decenas de miles de correos –ya enviados y recibidos- en mi cuenta de *Gmail*.

En un sentido semejante, nuestra legislación procesal también *hace aguas*, como ha denunciado por ejemplo la STC 207/2011, de 7 de noviembre, respecto de los requisitos y garantías respecto del acceso administrativo o policial a un ordenador sin intervención judicial. Ello lleva a situaciones complejas. Así, sí que es posible intervenir un teléfono móvil de un alumno para acceder a su perfil de redes sociales, por parte del Director de un instituto sin autorización judicial[51]. De igual modo, la Guardia Civil también puede acceder a la agenda del teléfono móvil sin intervención judicial (STC

[50] Convención ratificada por España el 20 de mayo de 2010, BOE 17 de septiembre http://conventions. coe. int/Treaty/en/Treaties/html/185-SPA. htm

[51] Cuestión analizada bajo el régimen jurídico de la protección de datos por la SAN, Secc. 1ª de 26 de septiembre de 2013, recurso 481/2012. La sentencia ratifica la consideración de la Agencia Española de Protección de Datos y que había motivos de interés público y por tanto de interés legítimo para la inspección realizada por el centro educativo sin consentimiento de los padres.

142/2012, de 2 de julio), pero no puede acceder sin dicha intervención judicial al listado de las últimas llamadas realizadas en una actuación en caliente (STC 230/2007, de 5 de noviembre). Los ejemplos ilustran la imperiosa necesidad de un marco normativo que dé seguridad jurídica tanto a la ciudadanía cuanto a las Fuerzas y Cuerpos de Seguridad.

3. De la "expectativa razonable de confidencialidad" al control laboral absoluto del uso de medios informáticos

En los últimos años destacan la doctrina fijada en la STC 241/2012, de 17 de diciembre y en la STC 170/2013, de 7 de octubre de 2013. De las mismas resulta especialmente llamativo el concepto de "expectativa razonable de confidencialidad" que tenga el usuario de las comunicaciones en razón del contexto tecnológico y jurídico. Si se cuenta con tal expectativa de confidencialidad, sí que se predica el secreto de las comunicaciones y, por tanto, las garantías que lleva aparejadas. De una parte, este concepto permite la proyección a muy variables contextos de comunicación hoy posibles. Así, no podrá predicarse razonablemente el secreto de las comunicaciones respecto de las que se realizan en un foro de internet en abierto, o en una red social en la que se cuentan por cientos los "amigos" o "seguidores", o cuando se remite un correo electrónico o un *Whatsapp* a decenas o centenas de remitentes. Pero sí que habría tal razonable expectativa de confidencialidad respecto de un sistema de mensajería privada integrado en una red social (por ejemplo, el correo o mensajes privados de *Facebook* o en un foro o chat privado), una conversación en *Skype* o en un *Whatsapp* dirigido a un contacto.

El concepto de "expectativa razonable de confidencialidad" permite además una importante contextualización jurídica, esto es, la confidencialidad ya no se hace depender de la tecnología utilizada, sino del marco jurídico en el que se produce la misma. Así, para la STC 241/2012, de 17 de diciembre, aunque se utilice un sistema cerrado de mensajería, el usuario no puede esperar razonable confidencialidad si el programa (como el antiguo *Messenger*, o por ejemplo el *Whatssap*) ha sido instalado en un ordenador en contra de las normas del empresario que vedaban al trabajador la instalación de programas. En consecuencia, la prueba obtenida al controlar el uso del sistema de mensajería sí que se consideró admisible constitucionalmente. De igual modo, para la STC 170/2013, de 7 de octubre de 2013, decae la expectativa de confidencialidad del correo electrónico de la empresa cuando éste es utilizado por el trabajador para fines personales siendo que las normas aplicables prohibían el uso privado del correo. Así las cosas, se confirma y complementa la doctrina unificada por el TS en su sentencia de 26 de septiembre de 2007. En razón de la jurisprudencia, la prueba obtenida a través del control empresarial respecto del uso laboral de medios informáticos será válida siempre que el trabajador haya conocido la posibilidad de dicho control o, en su caso, existan normas –también conocidas- que establezcan prohibiciones de usos o previsiones del referido control empresarial. A mi juicio, ciertamente, esta doctrina lleva a permitir un control o monitoreo absoluto por parte el empresario de corte anglosajón, simplemente al mínimo precio de haber informado previamente al trabajador del posible control. El legislador bien podría intervenir y establecer algunos límites y garantías frente a un control total que despoje de un mínimo de intimidad y secreto de las comunicaciones en el ámbito laboral.

Y lo que es a mi juicio más criticable, esta situación contrasta y se hace casi incoherente con soluciones como la de la STC 29/2013, de 11 de febrero. En este caso, se estima contraria al derecho de protección de datos personales y por tanto nula la prueba obtenida por una cámara de videovigilancia cuya finalidad era la seguridad y que cumplía con los requisitos legales, entre otros, quedar debidamente anunciada y ser

conocida por el trabajador. Las imágenes captadas se hicieron servir en contra de un trabajador que incumplía sus deberes, si bien se consideró que la finalidad de seguridad era incompatible con la del control laboral. A mi juicio, estas corrientes jurisprudenciales chirrían y deben se moduladas y matizadas merced a la fuerza democrática del legislador.

4. Las mayoría de las cesiones de datos entre Administraciones pasan a ser inconstitucionales en razón de la STC 17/2013

La STC 17/2013, de 31 enero ha pasado a ser la referencia constitucional ineludible por cuanto a la comunicación de datos entre administraciones públicas.

En razón de esta sentencia, se requiere ley expresa que prevea la cesión misma de los datos, la finalidad de dicha cesión y la competencia concreta de la administración que ha de recibir los datos y que legitima dicho uso. Asimismo, la regulación legal debe cumplir con garantías constitucionales de calidad, esto es, estableciendo una serie de condiciones o garantías para cumplir con la necesaria proporcionalidad de la medida. Por ello, la regulación debe hacerse con un nivel de garantías superior al que se impone para autorizar el acceso a datos concretos y particulares de otra Administración. Cuanto menos cabe pensar que por ley debe regularse quién es la Administración cedente, qué datos concretos puede ceder, la finalidad de tal comunicación y garantías que deben darse tanto en el procedimiento de solicitud y cesión de los datos cuanto garantías en la trazabilidad de tales datos ante los riesgos concretos que puedan darse por cuanto al desvío de las finalidades legítimas.

A mi juicio, esta sentencia, y con mayor claridad si cabe la coetánea STC 29/2013, caen en la corriente del *eleopedecentrismo*[52], esto es, hacer de la LOPD centro del universo jurídico, y atribuir un nivel de garantías muy elevado y destacado entre los demás derechos fundamentales. El nivel de garantías para las comunicaciones de datos que fija el TC es más garantista de lo que pudiera parecer. Tanto que podría poner en situación de inconstitucionalidad a buena parte de las leyes que hoy día autorizan comunicaciones de datos sin consentimiento. Sin embargo, las posibilidades de regulación del flujo de datos entre administraciones podrían ser mucho más generosas y flexibles, como en otros países de la Unión Europea y al amparo del ordenamiento europeo.

Pues bien, lo cierto es que pese a esta sentencia, la cuestión sigue en *standby* y no parece que ni la doctrina, la AGPD, ni el legislador se muestren preocupados por las consecuencias que podrían derivarse. Se trata de un ámbito más donde la acción del legislador sería decisiva.

5. Del mito del consentimiento del titular de los datos y la nueva regulación de la protección de datos en Europa. Hacia un sistema de obligaciones objetivas más paternalista

El derecho de protección de datos personales ha girado estructuralmente hasta la fecha en el consentimiento del titular de los datos personales, pues teóricamente el

[52] Desde hace años me sumo a una corriente –minoritaria- que critica la sobredimensión del derecho de protección de datos personales y la percepción de todo el fenómeno jurídico a través de esta ley. Este fenómeno se percibe obviamente entre los que trabajan los ámbitos de privacidad y nuevas tecnologías si bien se produce por una vis expansiva de la regulación y comprensión de este derecho por el legislador y los tribunales. El término se acuña por escrito por PACHECO, ALFONSO, "La Sentencia 29/2013 de la Sala Primera del Tribunal Constitucional: ¿fin a las grabaciones ocultas por parte de la empresa? El eleopedecentrismo al poder", en www. privacidadlogica. es, 21. 3. 2013.

titular de los datos debe consentir el tratamiento de datos y tutelar bajo su voluntad sus derechos ARCO (acceso, rectificación, cancelación y oposición). No obstante, por diversos motivos esta columna vertebral de la protección de datos quebró hace tiempo.

En primer lugar, porque son legión las excepciones legales a la necesidad de consentimiento informado para la recogida o para la cesión de datos. Hoy día las excepciones legales al consentimiento plagan ya nuestro ordenamiento de un modo disperso y asistemático. Más que de una restricción a un derecho fundamental parecen ya casi una cláusula de estilo de muchas leyes, sin que en la mayoría de los casos la norma integre los presupuestos constitucionales del límite al derecho por cuanto a la justificación, razonabilidad y proporcionalidad de la restricción. La general remisión a la ley del artículo 6 o del artículo 11 LOPD parece cubrir esta práctica.

En segundo lugar, no hay que olvidar la STJUE de 24 de noviembre de 2011 que resolvió la cuestión prejudicial planteada por el TS español en los asuntos C-468/10 y C-469/10 y la consecuente STS de 8 de febrero que derogó el art. 10. 2. b) del Real Decreto 1720/2007 que aprueba el Reglamento de la LOPD. Dicha sentencia europea vino a hacer temblar los cimientos de la protección de datos en España por cuanto es posible no exigir el consentimiento del afectado si el tratamiento se justifica en el interés legítimo del responsable del tratamiento. Lejos de un fuerte terremoto, lo que ha habido es un goteo de sentencias que consideran que existe un interés legítimo que permite el tratamiento de datos sin consentimiento, pero no de una manera generalizada. A mi juicio, se está a la espera del Reglamento Europeo para que la cuestión quede más definida, en lo que hoy es una gran incertidumbre.

En tercer lugar, y a mi juicio como cuestión de calado frente a la importancia del consentimiento, hay que estar con Oliver y Muñoz[53], cuando señalan que es un hecho la banalización del consentimiento como mecanismo de tutela del derecho. No es realista en modo alguno creer que existe un efectivo control de la información personal a través del consentimiento y los derechos que lo complementan. Es más, el ideal del consentimiento informado choca en la práctica con la función que está cumpliendo hoy día, que no es otra cosa que permitir la renuncia misma a la autodeterminación informativa. El consentimiento se torna en una *carta blanca* al descontrol del flujo de los datos personales. El consentimiento acaba configurándose como un simbolismo que conlleva, a la postre, al fracaso de la privacidad pretendida y a la inoperancia del sistema de protección. Es más, siguiendo a estos autores, el consentimiento se hace inservible e inoperante con la mayor complejidad del contexto tecnológico, la *web 3. 0* y el *big data*. Así, por ejemplo, con los sistemas de inteligencia artificial y decisiones automatizadas, no es posible consentir dado que no siempre es posible prever la decisión automatizada que se adoptará. En la misma dirección, con los sistemas repartidos y troceamiento de la información propios del *big data* no es posible conocer la ubicación de los datos y tratamiento efectivo de los datos, con lo que es bien difícil predicar un control de los mismos por el usuario.

En este contexto, cabe hacer somera referencia al Reglamento Europeo de Protección de Datos aprobado el 12 de marzo de 2014 por el Parlamento Europeo y sólo pendiente de su aprobación final por el Consejo. Se trata de una norma que está gestándose hace tres años y ha sido sometida tremendas presiones desde los más diversos sectores, como los grandes prestadores de servicios norteamericanos a través

[53] Oliver A. Daniel y Muñoz José Félix, "El mito del consentimiento, o por qué un sistema individualista de protección de datos (ya) no sirve para (casi) nada", en Valero Torrijos, Julián: *La protección de los datos personales en Internet ante la innovación tecnológica, Aranzadi*, Cizur Menor, 2014. Puede seguirse una exposición oral (desde el minuto 2' en http://www. sicarm. es/servlet/vsicarm. servlets. Videos?METHOD=FLASH&video=umu03)

de Estados miembros como Irlanda o Reino Unido. Esta norma tendrá vigencia directa en los estados miembros y va a generar una compleja situación jurídica al momento de su aprobación. De un lado, requerirá de un muy importante desarrollo técnico normativo a cargo de la Comisión Europea, en tanto en cuanto la norma así lo dispone en decenas de ocasiones. De otro lado y presumiblemente, el reglamento europeo y la referida normativa de desarrollo convivirá por largo tiempo con la también exhaustiva normativa nacional. Se trata, no olvidemos de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y el extenso Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

Pues bien, no procede aquí una glosa de tan prolijo reglamento europeo, si bien cabe afirmar que sigue girando en torno al consentimiento del individuo y las reglas llamadas "principios" de la protección de datos. No obstante, la nueva norma europea gira también sobre el principio general de la responsabilidad: el que trata los datos, responde. En este punto, cabe subrayar el viraje hacia cierto paternalismo en la protección de datos superador de la garantía subjetiva sobre la base del consentimiento del titular de los datos. Así, se configuran concretas obligaciones objetivas para los responsables de ficheros:

- Se generaliza la obligación del responsable de notificar a la Agencia y comunicar al titular de los datos las brechas de seguridad y violaciones de protección de datos. Esta obligación en parte ya fue introducida para el sector de las telecomunicaciones por la Directiva 2009/136/CE, transpuesta por el Real Decreto-ley 13/2012, de 30 de marzo.

- La privacidad por diseño o por defecto, que impone implementar las medidas y procedimientos técnicos y organizativos apropiados. En este aspecto, la normativa técnica de desarrollo va a definir una miríada de obligaciones objetivas a cumplir por los responsables de ficheros. Ello va a complementar la insuficiente garantía del consentimiento.

Será obligatorio en las organizaciones de nombrar un delegado de protección de datos (DPO, *Data Proteccion Officer*), con responsabilidad e independencia.

- Los PIA, informes de impacto de privacidad, esto es, evaluaciones preventivas del impacto del tratamiento de los datos personales obligatorios para el responsable de ficheros en determinados casos. (En marzo de 2014 la AEPD publicó el Borrador de su Guía para la Evaluación de Impacto en la Protección de Datos Personales).

6. Google y el derecho al olvido tras la STJUE de 13 de mayo de 2014

La STJUE (Gran Sala) de 13 de mayo de 2014 en el asunto C-131/12, en el procedimiento entre *Google* Spain, S. L. , *Google* Inc. vs. la Agencia Española de Protección de Datos (AEPD) y Mario Costeja González[54] ha sido una de las sentencias más esperadas y relevantes en materia de protección de datos. En la misma el TJUE afirma:

1º: *Google* realiza y es responsable de un "tratamiento de datos personales" en el sentido de la Directiva cuando indexa contenidos de la web y los ofrece como resultados, pese a que no controle la información de origen de las páginas web que indexa (ap. 34).

[54] Cuando un internauta introducía el nombre del Sr. Costeja González en el motor de búsqueda de *Google* obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, respectivamente, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre. La AGPD consideró que *Google* debía desindexar la información relativa al Sr. Costeja. No cuestionó que la hemeroteca de la Vanguardia siguiese facilitando estos contenidos en la web.

2º: A *Google* le es de aplicación la normativa de la Unión Europea y por tanto está sometido a la legislación sobre protección de datos española (aps. 50 y ss.), cuanto menos, si tiene una oficina comercial en el país.

3º Ni el interés económico de *Google* ni el general interés de los usuarios a acceder información de otros justifica suficientemente la grave afección a la privacidad y protección de datos que implica el buscador de *Google* (ap. 97, ídem en 81 o 99). Sólo será admisible que *Google* arroje resultados relativos a las personas en determinados supuestos en razón "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" (ap. 81).

4º La ciudadanía puede dirigirse a *Google* para solicitar la desindexación sin que sea necesario haber acudido previamente a solicitar la retirada de contenidos en la web de origen. Es más, la información puede ser legítima en la web de origen pero no en *Google* (ap. 87). Así las cosas, será *Google* primero y las autoridades de protección de datos o los tribunales después quienes deberán llevar a cabo la ponderación concreta de si procede la desindexación solicitada.

5º "cada tratamiento de datos personales debe ser legítimo […] durante todo el período en el que se efectúa. (ap. 95). Por ello, en razón del tiempo deberán desindexarse informaciones inicialmente lícitas.

A mi juicio la sentencia es criticable, de un lado, porque no confiere una protección especial al buscador *Google* en razón de su papel esencial para el acceso a la información en el mundo. No se tiene en cuenta el efecto que puede producirse de modo global por imponer límites o condiciones severas a este buscador. No parece preocupar que sus consecuencias sean una sensible merma de contenidos accesibles efectivamente en internet. Y, sobre todo, que esta merma de contenidos sea resultado de aplicar de criterios privados, esto es, tanto el interés privado del sujeto sobre el que versan los contenidos cuanto el interés privado de *Google* de retirar contenidos que sean problemáticos. Del otro lado, la sentencia es criticable porque son varios los "olvidos", que abren la puerta a una gran incertidumbre en elementos clave. Y es que aplicar la sentencia hasta sus últimas consecuencias implicaría que sólo podrían aparecer en *Google* quienes hubieran dado previamente su consentimiento. Asimismo, es necesaria la definición de quiénes quedan obligados por el derecho al olvido. No en vano, no son pocos los prestadores de servicios que sobre la base de información de internet tratan datos personales en el sentido afirmado en la sentencia, por cuanto "recogen", "extraen", "registran", "organizan", "conservan", "comunican" y "facilitan el acceso". Asimismo, la sentencia sitúa el centro de gravedad futuro en las medidas que adopte la propia compañía. Sin embargo, el acceso de contenidos de internet en la Unión Europea no debería quedar en manos de una compañía privada sin una definición por parte del legislador. Y es que a mi juicio no deberían ser los tribunales, sino el legislador europeo y en su caso el nacional quien habrían de concretar su alcance y tomar decisiones que pueden ser clave para internet.

Al momento de cerrar estas páginas, no se conoce el alcance que puede tener esta sentencia. En junio de 2014 *Google* dispuso una web para España[55] para poder ejercer el derecho al olvido y creó un Comité consultivo internacional de siete miembros reconocidos (entre ellos un español)[56] para valorar el alcance de esta sentencia y su

[55] En español, en junio de 2014 la web disponible en http://goo. gl/GZ6XNA

[56] Dicho comité se compone el expresidente de *Google*, Eric Schmidt, el director de Wikipedia, Jimmy Wales, el exdirector de la AEPD José Luis Piñar; Frank La Rue, relator especial de la ONU para la protección del derecho a la libertad de expresión; Luciano Floridi, profesor de Filosofía y Ética de la Universidad de Oxford, y Peggy Valcke, de la Universidad de Lovaina.

aplicación. Asimismo ha convocado el 9 de septiembre de 2014 en España y en otras fechas en otros países a diversos expertos, como a quien suscribe, para consultas sobre cómo aplicar la referida sentencia. Habrá que estar a la espera.

IV. La libertad de expresión e información de todos los usuarios de la red y algunas cuestiones clave por resolver

1. El necesario punto de partida: la Constitución protege la difusión de opiniones e informaciones por cualquier sujeto a través de cualquier canal, modo o medio

Como he sostenido en otros lugares desde hace tiempo[57], las libertades informativas se reconocen a toda persona (aunque no sea empresa de comunicación o periodista) que emita información veraz o exprese opiniones, así como a la colectividad que las recibe. Antes de internet estas afirmaciones, si se me permite, *salían gratis*. Así el TS de EEUU diría que "la libertad de la prensa es el derecho de un solo panfleto. . . al igual que el de la más importante publicación metropolitana"[58]. La sentencia Engels del TEDH, de 8 de junio de 1976 afirmó que "Está claro que la libertad de expresión garantizada por el artículo 10 [del CEDH que reconoce la libertad de expresión] es aplicable a todas las personas" (Apartado 100). Afortunadamente para la libertad de expresión en el mundo, en 1997 el TS de EEUU asentó con claridad la premisa de que Internet es un canal de comunicación que queda protegido por la libertad de expresión e información (*ACLU vs Reno* de 1997). Este mismo punto de partida se ha reconocido sin valor jurídico normativo en diversas declaraciones internacionales "Los Estados miembros no han de colocar restricciones a los contenidos en Internet que vayan más allá de las aplicadas a otros medios de difusión de contenidos. (principio nº 1 de la "Declaración sobre la libertad de comunicación en internet", del Consejo de Europa de 28 de mayo de 2003[59]). Más recientemente, la ya citada Declaración conjunta sobre libertad de expresión e internet de 2011 acoge de forma contundente este punto de partida: "La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen,

---

[57] Me permito recordar algunos de mis trabajos especialmente como coordinador, publicados en la materia, entre otros, "Algunas claves para el análisis constitucional futuro de las libertades públicas ante las nuevas tecnologías (con especial atención al fenómeno de los "*blogs*")", en AA. VV. *Estudios jurídicos sobre la sociedad de la información y nuevas tecnologías,* Facultad de Derecho de Burgos, Burgos, 2005, págs. 51-76. También, "Nuestros jueces y tribunales ante internet y la libertad de expresión: el estado de la cuestión", en Cotino Hueso, Lorenzo (Coord.), *Libertad en internet…,* cit. así como el estudio introductorio a la obra.Nuevas tecnologías, desafíos y posibilidades para la libertad de expresión", publicación de la Ponencia en las III Jornadas de Derecho constitucional "Constitución y libertad de expresión", Fundación Giménez Abad-Cortes de Aragón- UNED, Barbastro (Huesca) 7-8 de noviembre de 2008, disponible en http://goo. gl/cBkEa

He coordinado obras monográficas como Cotino Hueso, Lorenzo (Coord.), *Libertades, democracia y gobierno electrónicos*, Comares (Colección Sociedad de la Información, nº 9), Granada, 2006: *Libertad en internet. La red y las libertades de expresión e información,* Tirant lo Blanch, Valencia, 2007; *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías,* PUV (Publicaciones de la Universidad de Valencia), Valencia, 2011, Corredoira y Alfonso, Loreto y Cotino Hueso Lorenzo (eds.) *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, 2013.

[58] Así, el Tribunal Supremo de Estados Unidos, en el caso *Branzburg v. Hayes* de 29 de junio de 1972, ("liberty of the press is the right of the lonely pamphleteer … as much as of the large metropolitan publisher.)

[59] Aprobada por el Comité de Ministros en el marco de la 840ª Reunión.

entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad". (I, principio general a).

En esta línea, el TJCE en 2008[60] afirmó que la importancia de la libertad de expresión impone interpretar ampliamente la noción de "periodismo" hacia "toda persona que ejerza una actividad periodística" (nº 58). Se señala que difundir información con ánimo de lucro no excluye que se trate de fines periodísticos, "el soporte en el que se transmiten los datos, clásico como el papel o las ondas de radio, o electrónico como Internet, no es determinante para apreciar si se trata de una actividad "con fines exclusivamente periodísticos" (nº 60), de manera que las "actividades periodísticas" "No están reservadas a las empresas de medios de comunicación y pueden ejercerse con ánimo de lucro. (n. 61)

Es, pues, capital que el punto de partida sea el reconocimiento de las libertades informativas a todo contenido veraz de interés público, aunque éste sea transmitido en internet y pese a que no sea a través de periodistas o habituales medios de comunicación social. Ahora bien, esta extensión de la libertad de expresión e información a quien genere ideas o información de interés público en internet no empece que vaya acompañada de las exigencias de veracidad y diligencia de la información, así como del análisis de si tal información efectivamente tiene interés público y relevancia que le lleve a gozar de una especial protección.

Cabe alertar que desde sectores políticos y jurídicos como desde los medios de comunicación clásicos se pretende reservar sólo para estos últimos una libertad de expresión, información y de prensa reforzada y con garantías específicas (privilegios) que no se extiendan en general a internet[61]. Se trata de cierta inercia sociológica y jurídica en nuestros tribunales de reservar, más o menos veladamente, las libertades informativas para los medios de comunicación, digámoslo así, clásicos[62]. Así, el TS ratificó una sanción de la AEPD por la difusión de información sobre Guardias Civiles condenados por torturas en una web de la Asociación contra la tortura, considerando tales contenidos estaban excluidos de la libre expresión e información[63]. En concreto, afirma el Tribunal Supremo que "*la libertad de información "alcanza su máximo nivel*

---

[60] STJCE (Gran Sala) de 16 de diciembre de 2008, cuestión prejudicial asunto C 73/07. En especial ver los apartados 56 a 61.

[61] Así llamó la atención inicialmente en Estados Unidos, entre otros, Sunstein, Cass R. , *República. com. Internet, democracia y libertad*, Paidós, Madrid, 2003. En inglés, *Republic. com*, Princeton University Press, 2001; Balkin, Jack M. , "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society". *New York University Law Review*, Volume 79, april 2004, n. 1, págs. 1-58, disponible en http://ssrn. com/abstract=470842 o Ribstein, Larry Edward, "Initial Reflections on the Law and Economics of Blogging" (April 4, 2005). *U Illinois Law & Economics Research Paper* No. LE05-008. http://ssrn. com/abstract=700961 También de este autor, en "*Bloggers* and Their First Amendment Protection, " vol. 57, no. 3 Otoño 2003 issue of "The Neiman Reports, " The Neiman Foundation for Journalism at Harvard University. http://www. nieman. harvard. edu/reports/03-3NRfall/95-96V57N3. pdf ; WU, Tim, *Who Controls the Internet*, Oxford U. Press 2006, entre otros. En Reino Unido, Lipschultz, J. H. , *Free expression in the age of the internet*, Westview Press, Boulder-Oxford, 2000 o recientemente, Packard, A. , *Digital Media Law*, Willey-Blackwell, Oxford, 2010.

[62] Este criterio, que se vislumbra en la STC 136/2004, de 13 de septiembre, FJ 5º recordando la doctrina de del vehículo utilizado para difundir la información, en particular si éste es un medio de comunicación social (STC 107/1988, de 8 de junio, y 15/1993, de 18 de enero; STC 54/2004, de 15 de abril, FJ 3).

[63] Se trata de STS de 26 de junio de dos mil ocho, recurso: 6818/2003. Asociación contra la tortura contra las Resoluciones del Director de la Agencia de Protección de 4 de septiembre y 3 de octubre de 2000.

cuando la libertad es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública, que es la prensa" (FJ 6º).

Esta tendencia negativa encontró su máxima expresión en una muy desafortunada resolución de la APD, que llegó a fundamentar una sanción en que:

"Las páginas web del imputado no pueden ser consideradas medios de comunicación social sin que quepa invocar el ejercicio y prevalencia del derecho de libertad de información que derivaría en una prevalencia general que aboliría de facto al protección de datos personales. Y que desvirtuaría el equilibrio entre derechos sostenido sobre el derecho de la sociedad a ser informada a través de los medios de comunicación y el de los ciudadanos a la autodeterminación informativa y privacidad sostenido sobre el derecho de protección de datos.[64].

En otras palabras: un ciudadano no puede atreverse a alegar la libertad de expresión. Eso es cosa de medios de comunicación. Esta resolución fue anulada por la Audiencia Nacional en 2012[65] por lesión de la libertad de expresión; no obstante, son varias las resoluciones con esta tendencia de la AGPD[66]. Reservar de manera excluyente la protección más intensa de las libertades a los medios de comunicación clásicos es un punto de partida que amordaza la libertad de expresión e información en la red bajo la *espada de Damocles* de severísimas sanciones administrativas o penales.

Este punto de partida puede ayudar a resolver algunas de las cuestiones clave en materia de libertad en la red que a continuación se apuntan.

2. Cuestiones clave por resolver en materia de libertad en la red

En el apartado II (" El acceso a Internet como nuevo derecho fundamental y sus garantías") se ha prestado atención a las garantías frente al corte de internet y la restricción de acceso a sus contenidos en razón de la libertad de expresión. Ahí cabe remitirse. En cualquier caso, hay otras cuestiones constitucionales clave a mi juicio en materia de libertad en la red.

Cabe preguntarse si el secreto profesional o derecho a no revelar las fuentes de información se reserva a los profesionales del periodismo –clásico- o se generaliza a quienes informen con interés público en internet. La cuestión no deja de ser especialmente importante teniendo en cuenta las posibilidades de filtraciones masivas, de informaciones de indudable interés público, a través de medios como *Wikileaks* y muchos similares que surgen o surgirán en el futuro. La tendencia en Estados Unidos es la extensión del secreto profesional a todo informador a través de internet. Así en el Caso Apple y Dan Gillmore primero por un juez de Santa Clara, marzo 2005, y de forma más clara en la Corte Estatal de Apelaciones de San José en mayo de 2006-. También en el caso John Doe nº1 v. Cahill, de octubre de 2005, en Delaware. La sentencia de la Corte del Noveno Circuito el 17 de enero de 2014 en el caso Obsidian Finance Group, LLC v. Cox revoca la sentencia inicial de 2011 y sigue la línea de tratar de forma igual a los medios y a los ciudadanos que ejercen la libertad de expresión[67].

---

[64] Resolución 211/2010, PS 439/2009, CITA denunciada por la U. Politécnica de Madrid por difusión de enlaces y vídeos externos en crítica por competencia desleal de algunos profesores.

[65] Así en la sentencia de 11 de abril de 2012 en el P. A. 03078/2010.

[66] Así lo analizo en Cotino Hueso, Lorenzo: "Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)" en Troncoso Reijada, Antonio (dir.) *Comentario a la Ley Orgánica de Protección de Datos Personales*, Thomsom-Civitas, Cizur Menor, 2010, págs. 289-315 (acceso completo en internet).

[67] http://en. wikipedia. org/wiki/Obsidian_Finance_Group,_LLC_v._Cox

Una cuestión de especial incidencia en la red que he analizado ampliamente en otro lugar[68] y no resuelta en Europa es si cuando se alojan contenidos ilícitos por atentar contra la privacidad, la propiedad intelectual, etc. dado que no se conoce el autor de los mismos, si se puede atribuir responsabilidad al intermediario o prestador de servicios, como pueda ser una red social (*Facebook*), un alojador de vídeos (*Youtube*), de comentarios (periódicos, *blogs*, foros), de contenidos (*Wikipedia*), servidor de enlaces (*Google*), etc. La amenaza de atribuir esta responsabilidad jurídica civil e incluso penal al intermediario o pretador de servicios por tales contenidos ilícitos puede generar un efecto amenazante (*chilling effect*), contrario a la libertad de expresión. En Europa, a partir de la Directiva 2000/31/CE sobre el comercio electrónico, el esquema general es que el prestador de servicios de Internet no tiene un deber de vigilar los contenidos que transmite ni es responsable de los mismos si son ilícitos. Sin embargo, este esquema ha quedado completamente quebrado y superado por muchos tribunales en Europa y no hay acuerdo alguno para reformar la Directiva, pese a que se coincide en que ha quedado totalmente desfasada. Por ejemplo, el Tribunal Supremo español en diciembre de 2009[69] hizo responsable a la Asociación de Internautas por los contenidos ilícitos que insertó en su sitio una plataforma contraria a los derechos de autor, aunque también en otros casos no ha hecho responsable a una web de quejas. Habrá que esperar alguna decisión a nivel europeo, si bien en una línea bien peligrosa el TEDH en el caso Delfi vs Estonia de 10 de octubre de 2013 –pendiente de decisión final por la Gran Sala-condena a un medio digital por no vigilar y filtrar los contenidos de los usuarios lectores del mismo. El TEDH parte al menos de que atribuir la responsabilidad al intermediario es una restricción de la libertad de expresión. Si bien, el TEDH admite un marco legal, como el europeo, no muy definido para la determinación de quién responde por los contenidos de internet. Esto es así a diferencia de las más severas exigencias de legalidad para bloquear contenidos en internet en la STEDH de 2012 Ahmet Yıldırım c. Turquía. La línea seguida en el caso Delfi, obligaría a vigilar todos los contenidos 2. 0 por los intermediarios, algo casi materialmente imposible.

Por el contrario, en EEUU el régimen general de responsabilidad de los prestadores e intermediarios[70] que se aplica es de la Sección 230 de la Ley de Decencia en las Comunicaciones. Se confiere un "puerto seguro" ("safe harbour") a los proveedores de "servicios interactivos" por el discurso y contenidos ilícitos de sus usuarios. Se blinda así tanto a los grandes operadores y prestadores por los contenidos ilícitos que intermedian, incluso si se niegan retirar el contenido a petición del afectado [71] o aunque no sean diligentes en la identificación de usuarios o generen espacios que

[68] Sobre el tema, especialmente, Cotino Hueso, Lorenzo: "Libertades informativas y responsabilidad de los prestadores de servicios en la red" ponencia en el XI Congreso de la Asociación Constitucionalistas de España, (ACE), 21 y 22 de febrero de 2013, Barcelona, "La tutela judicial de los derechos fundamentales". Acceso en http://goo. gl/mD8idC

[69] Una valoración personal del caso con acceso al mismo en http://www. cotino. net/2009/12/otra-sentencia-contra-la-libertad-de-expresion-del-ts-caso-putasgae/

[70] Cabe señalar que en EEUU hay otros regímenes de responsabilidad de prestadores e intermediarios en ámbitos penales y, sobre todo destaca el sistema de responsabilidad por ilícitos de propiedad intelectual establecido por la "*Digital Millennium Copyright Act"* (*DMCA*, aprobada en octubre de 1998).

[71] La respuesta inicial y general se da en Zeran vs. AOL, 129 F.3d 327, 328 (4th Cir. 1997), a la que siguen otras muchas entre las que destacan Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1103–05 (9th Cir. 2009); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007). Al respecto, entre otros muchos cabe seguir Wu, Felix T. "Collateral Censorship and the Limits of Intermediary Immunity", en *Notre Dame Law Review*, Vol. 87, No. 1, p. 293, 2011, Cardozo Legal Studies Research Paper No. 354 (acceso en SSRN) así como lo más reciente en Gellis Catherine R., "Intermediary

facilitan los contenidos conflictivos. Es más, el "puerto seguro" protege también como "servicios interactivos" a los usuarios de servicios que difunden y redifunden información de terceros. Tal protección se da incluso aunque conozcan, seleccionen o promocionen la línea o idea de tales contenidos de terceros[72]. A diferencia de Europa, la jurisprudencia norteamericana prácticamente no tiene fisuras al respecto. Blindando a los prestadores e intermediarios se pretende evitar la "censura colateral" ("Collateral censorship")[73] y efecto amenazante ("chilling effect")[74] que supone otra opción: incertidumbre por la legalidad de los contenidos, altos costes de defensa y la amenaza de la importante sanción o indemnización que pueda darse[75].

Pues bien, en esta línea marcha la ya citada Declaración de libertad de expresión en internet de 2011 (punto 2 a y b) y no la brecha abierta en el modelo europeo.

Otra cuestión clave es la de la posible "censura" en internet por parte de empresas privadas, contraria al pluralismo en la red. Encontrar contenidos en más de 10 billones de páginas web puede ser peor que encontrar una aguja en un pajar. Estar presente entre los primeros resultados de *Google* o aparecer adecuadamente en Youtube, Wordpress o en las redes sociales, por ejemplo, es garantía de visibilidad en la red. Afortunadamente los criterios de visibilidad en estos buscadores y prestadores de servicios parecen ser bastante "democráticos" (popularidad en la red por otros internautas, enlaces que desde otras páginas llevan a la página y actualización de contenidos). En todo caso, se trata de empresas privadas que pueden, en principio, hacer lo que quieran, incluso "censurar" a quien quieran en sus buscadores. Se trata obviamente de una "censura" en sentido impropio al acometerse por sujetos privados. Pues bien, considero que las empresas privadas también pueden cometer una lesión de la libertad de expresión si los criterios de filtrado de contenidos fuesen discriminatorios o políticos[76]. Es más, el interés público podría justificar una actuación legislativa que impusiese a tales buscadores o intermediarios no utilizar criterios políticos o discriminatorios para omitir resultados de búsqueda y, en todo caso, hacer públicos todos los criterios que pueden servir para restringir resultados.

Liability for User-Generated Content. 2012 State of the Law Regarding Internet", *The Business Lawyer*; Vol. 68, November 2012, págs. 289-295. Acceso en SSRN.

[72] Entre otras muchas cabe señalar Carafano v. Metrosplash.com 339 F.3d 1119 (9th Cir. 2003) O la decisión de 20 de noviembre de 2006, del TS de California en el caso Barrett v. Rosenthal, 146 P.3d 510, 519 (Cal. 2006), entre otros muchos.

[73] La expresión la emplea Wu, con remisión a Balkin, J.M. *Free Speech and Hostile Environments*, 99 COLUM. L. REV. 2295, 2298 (1999).

[74] Referencia básica del "Chilling effect" es Schauer Frederick*, Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 686–87 (1978), pág. 689, cito por Seltzer, Wendy, "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects if the DMCA on The First Amendment", en *Harvard Journal of Law & Technology*, Volume 24, Number 1 Fall 2010 (acceso en SSRN), pág. 179.

[75] Seilzer, *Ibídem*, pág. 194.

[76] En esta línea, se vulnera la libre expresión dificultando materialmente la distribución de publicaciones, tanto por un sujeto público (En el interesante caso por el cual la entidad de Correos procedió a no distribuir revistas de una empresa calificadas de pornográficas, sentencia 52/1995, de 23 febrero) como incluso, por un sujeto privado. Así, en un caso alemán resuelto por el Tribunal Constitucional Federal, *BverfGE* 25, 256, caso *Blinkfüer* de boicot de distribución de una publicación en Berlín, donde se señaló "El ejercicio de una presión económica, que genera en el implicado graves perjuicios, y que tiene como finalidad impedir la difusión de opiniones y noticias, que se encuentran protegidas constitucionalmente, viola la igualdad de oportunidades en el proceso de formación de la opinión, y contradice el sentido y esencia del derecho fundamental de la libertad de opinión, que tiene por objeto garantizar la controversia ideológica. Se sigue por Schwabe, Jürgen, *Cincuenta años de jurisprudencia del Tribunal Constitucional Federal Alemán*, (prólogo de Jan Woischnik y traducción de Marcela Anzola Gil), Gustavo Ibáñez, Konrad Adenauer Stiflung, Bogotá, 2003, págs. 162 y ss.

3. La necesidad de que el legislador asuma su papel para proteger las libertades informativas y otros derechos fundamentales en internet

El conjunto normativo hace auténticas aguas a la hora de fijar no pocos elementos esenciales del ejercicio de la libertad de expresión e información por los grandes y pequeños prestadores de servicios en internet, así como cientos de millones de usuarios de internet en todo el mundo. Según se vio respecto de los datos de acceso a internet, *sólo* se trata de la actividad cotidiana de unos cuatrocientos millones de europeos y unos treinta y cinco millones de personas en España, además de todo el entramado empresarial y social que implican los prestadores de servicios e intermediarios europeos o extranjeros.

La necesaria regulación legal no debe caer en la tendencia, habitual en Europa y España, de que la protección de datos –y sus severas consecuencias penales y sancionadoras- absorba el tratamiento jurídico. Y es que la difusión de datos en internet no sólo es un tratamiento a efectos de normativa de datos, sino que, al mismo tiempo en muchos casos, es el ejercicio de la libertad de expresión e información. Ni el futuro Reglamento europeo de protección de datos ni legislación española prácticamente contemplan el posible conflicto protección de datos y libertad de expresión.

Si bien los grandes prestadores de servicios e intermediarios de internet deben contar con una especial protección constitucional, ello no debe traducirse en la habitual desregularización de la prensa que se ha dado históricamente en España. Es posible delimitar jurídicamente obligaciones concretas para los grandes prestadores que equilibren el desarrollo de la sociedad de la información con los derechos personales. Es preciso imponer la existencia de medios ágiles y efectivos para los usuarios de contenidos, imponer protocolos de actuación así como aclarar las subsidiarias vías administrativas o judiciales respecto del control de contenidos en internet. Asimismo se puede fijar la revisión periódica o automática de contenidos integrados por terceros en plataformas de internet así como fijar con la industria la configuración por defecto de los servicios de la sociedad de la información, la identificación más o menos robusta de los usuarios según los tipos de servicios o contenidos, la necesidad de plantillas efectivas y garantistas de comunicación de ilícitos y, en su caso, de solicitud de retirada de contenidos. Ello vendrá de la mano con el desarrollo del futuro reglamento de protección de datos de la Unión Europea

Asimismo, no está de más proclamar legalmente que toda la información y expresión de interés o relevancia pública en internet goza de protección constitucional, aunque no proceda de un clásico "medio de comunicación social"; pueden resultar útiles algunas pautas para determinar qué información tiene interés público con independencia de su origen, así como establecer concreciones sobre algunos requisitos o garantías de la veracidad y diligencia tanto respecto de los contenidos, como de quiénes son sus autores (necesidades de identificación de quienes introducen contenidos en la red). Es preciso que los prestadores de servicios e intermediarios que tengan que hacer efectivo el derecho al olvido tengan algunas guías y criterios para efectuar una ponderación de la procedencia de la retirada o desindexación de contenidos. Sería idóneo que tales criterios vengan fijados por una ley o normativa similar europea y no se dejen a la autorregulación y a la práctica que adopten *Google* y otros.

Cabe afirmar y perfilar las garantías del ejercicio de las libertades en internet por usuarios e intermediarios y el alcance concreto de algunas de ellas, como el derecho a no revelar las fuentes, o el derecho de réplica y el derecho de rectificación. También, falta una meridiana claridad respecto de las facultades administrativas de control de contenidos en internet, las posibilidades de ponderación de derechos en estos supuestos.

Igualmente, dado que los poderes públicos cada día generan más de contenidos en la red, hay que regular la difusión de contenidos en los boletines y tablones oficiales, ámbito inexistente en la legislación que precisaría el reconocimiento de facultades a los organismos para analizar y en su caso bloquear publicaciones que generen innecesario impacto en la privacidad, la regulación de la imposición de medidas como robot. txt proporcionadas, la existencia jurídica misma de la figura de la desindexación, la fijación del ejercicio concreto del derecho al olvido: quién, cómo, ante quién, vía de recurso o alegaciones, etc. Hoy día campa la más negativa discrecionalidad al respecto sin sustento jurídico.

No hay que temer la especialización o sectorialización del régimen jurídico. Internet es como la calle y no todo lo que puede haber en la vía pública merece una regulación idéntica, sino una adecuación y contextualización. A la vista de la experiencia y sin perjuicio del dinamismo de la red, es bien posible describir funcionalidades y servicios para aplicarles regímenes jurídicos singulares. Baste apuntar que la normativa hoy día desconoce que existen buscadores, redes sociales, lugares de comercio masivo, grandes centros de consejos y opiniones para los usuarios, lugares que facilitan el acceso a contenidos concretos, servicios de almacenamiento masivo por usuarios, etc.

En el ámbito de la responsabilidad por contenidos es posible fijar algunos criterios generales como puedan serlo la voluntariedad y conocimiento más o menos directo en la confección del servicio o web y sus posibles usos, o del contenido ilícito concreto, la estructura más o menos automatizada de una agregación, sindicación o redifusión de contenidos, más o menos selectiva de los mismos; la diligencia en la selección de contenidos o en la confección técnica de la selección; la significación y magnitud de los contenidos conflictivos en el marco de la cantidad de los contenidos seleccionados; la participación real en la generación de contenidos los mismos; los indicios que llevan a pensar en el conocimiento material de los contenidos y su posibilidad de control; el hecho de que esos contenidos estén más o menos difundidos en otros sitios; el nivel de acceso y relevancia en la red de quien los difunde; el contexto y naturaleza propio del sitio web, servicio y aplicación en el marco de los usos de internet (no es lo mismo insultar en una cantina a las dos de la madrugada que en mitad de una clase de la universidad); la posibilidad de respuesta del afectado en el medio que es la red y las garantías reales que tiene el afectado de proteger sus intereses en cada ámbito.

V. El "gobierno abierto". Carencias y necesidades de su regulación

1. La convergencia de la democracia, participación, transparencia y Administración electrónica en el "Gobierno Abierto"

La Recomendación CM / Rec (2009) 1 del Comité de Ministros a los Estados miembros sobre la democracia electrónica (e-democracia)[77] denomina democracia o participación electrónicas al "apoyo y fortalecimiento de la democracia, las instituciones democráticas y los procesos democráticos por medio de las TIC", "una oportunidad para permitir y facilitar el suministro de información y deliberación, fomentar la participación ciudadana con el fin de ampliar el debate político, y favorecer un mejor y

[77] Acceso completo a una versión traducida automatizadamente en español en http://documentostics. com/component/option, com_docman/task, doc_download/gid, 1495/Itemid, 3/

Acceso completo al texto original en inglés en http://www. coe. int/t/dgap/democracy/activities/ggis/cahde/2009/RecCM2009_1_and_Accomp_Docs/Recommendation%20CM_Rec_2009_1E_FINAL_PDF. pdf

más legítima adopción de decisiones políticas. (Principio nº 9 del Anexo). No se trata, pues de acabar con la concepción predominante de democracia parlamentaria y suplantarla por otras. La conexión del gobierno con la democracia electrónicas se detecta desde los orígenes. Así, las definiciones iniciales de e-gobierno incluyen estas ideas: "es el uso de las tecnologías de información y comunicaciones que realizan los órganos de la administración para mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos" (Proyecto de Reforma y Modernización del Estado. Gobierno electrónico en Chile hoy[78], 2003 y OEA[79]).

Estas ideas se subrayan hoy día bajo las nuevas denominaciones de gobierno 2. 0 como en la Declaración Ministerial sobre administración electrónica aprobada por unanimidad en Malmö, Suecia, el 18 de noviembre 2009[80]. Así se insiste desde entonces en la necesidad de centrar la e-administración en la ciudadanía mediante servicios flexibles y personalizados, productos de información basados en la demanda (*user-centry*); la usabilidad de las aplicaciones de e-administración, la necesidad de involucrar a la sociedad y que ésta evalúe los servicios públicos electrónicos. De igual modo se invita a que los particulares estimulen y colaboren en la prestación de tales servicios.

En todo caso, el protagonismo y el impulso han venido dados con la noción *Open Government* introducida por Obama[81] en un famoso discurso de diciembre de 2009 donde afirmaba

"Mi administración está comprometida a crear un nivel sin precedentes de apertura en el gobierno. Vamos a trabajar juntos para asegurar la confianza pública y establecer un sistema de transparencia, participación pública y colaboración. La apertura va a fortalecer nuestra democracia y promover la eficiencia y la eficacia en el gobierno.

La noción de gobierno abierto cuenta incluso con una definición legal desde la Ley Foral 11/2012, de 21 de junio, de la Transparencia y del Gobierno Abierto de Navarra[82]. Los elementos básicos del concepto de gobierno abierto[83] son más

[78] http://goo. gl/S8sOlz

[79] *Guía de Mecanismos para la Promoción de la Transparencia y la Integridad en las Américas* en http://www. oas. org/es/sap/dgpe/guia_egov. asp

[80] Acceso completo en http://goo. gl/epZ75y

[81] El documento de referencia de Gobierno Abierto es el Memorando de Obama sobre "Transparencia y Open Government" de 8. 12. 2009, donde se señala que el gobierno debe ser transparente, participativo y colaborativo. Al mismo se accede en http://goo. gl/aTB8P

Del mismo surge una Directiva algo más concreta a cumplir por las agencias. El texto completo de la Directiva en http://1. usa. gov/arNG2A

[82] Artículo 3. b): "forma de funcionamiento de la Administración Pública capaz de entablar una permanente conversación con los ciudadanos y ciudadanas con el fin de escuchar lo que dicen y solicitan, que toma sus decisiones centrándose en sus necesidades y preferencias, que facilita la participación y la colaboración de la ciudadanía en la definición de sus políticas y en el ejercicio de sus funciones, que proporciona información y comunica aquello que decide y hace de forma transparente, que se somete a criterios de calidad y de mejora continua, y que está preparado para rendir cuentas y asumir su responsabilidad ante los ciudadanos y ciudadanas a los que ha de servir".

[83] La mejor fijación conceptual se da a mi juicio en el trabajo de Villoria. El autor subraya cuatro elementos básicos: 1. El gobierno promotor de bienestar a través de la capacidad regulatoria; 2. El gobierno transparente que rinde cuentas; 3. El gobierno participativo y promotor de civismo y 4. El gobierno eficiente, colaborador y generador de conocimiento. Villoria Mendieta, Manuel: "El gobierno abierto como subsistema de políticas: una evaluación desde el institucionalismo discursivo", en Hofmann, Ramírez Alujas y Bojórquez Perenieto (2012), págs. 69-101, 2012. Disponible en la red. De gran claridad en la misma obra Campos Domínguez, Eva y Corojan, Ana: "Estado del arte del Gobierno abierto: promesas y expectativas", págs. 119-136.

transparencia, reutilización de la información, participación pública y colaboración y todo ello merced a internet y la web 2. 0. A mi juicio lo más original y reciente del concepto es la colaboración, la usabilidad, el uso de redes sociales, todo bajo la filosofía de la web 2. 0 como pauta. Y estos principios proyectados en las organizaciones políticas y administrativas imponen la primacía del conocimiento frente a la jerarquía, la flexibilidad y el logro de objetivos colectivos frente a la individualidad y la burocracia, entre otros.

Además, el gobierno abierto incluye la prestación de datos abiertos. Ello implica un *giro de tuerca* a las ya tradicionales exigencias de reutilización de la información pública. Cabe recordar que se trata de algo estimulado desde hace décadas en Estados Unidos y que en la Unión Europea culminó con la Directiva 2003/98/CE, de 17 de noviembre de 2003 relativa a la reutilización de la información del sector público, transpuesta en España por la Ley 37/2007, de 16 de noviembre. Aunque se trate de liberar información pública, no se trata propiamente de transparencia, si no de la información pública como materia prima y valor económico fundamental. Con los datos abiertos ahora el énfasis se da en que las instituciones no sólo tienen que permitir, sino facilitar activamente dicha información pública para ser reutilízala por el sector privado. Es más, la norma ha sido recientemente modificada por la Directiva 2013/37/UE, de 26 de junio, que genera la obligación de que se dispense la información pública en formato electrónico legible por máquinas (art. 5) en el llamado internet 3. 0 o internet de las cosas. Esta última modificación de la Directiva debe ser transpuesta por España. Y más allá de que la ley recoja este texto de la Directiva, lo importante es que los datos abiertos legibles por máquinas efectivamente se implanten y los poderes públicos promuevan, en efecto, el cumplimiento de esta obligación. Asimismo, cabe también regular órganos o mecanismos de colaboración con la sociedad civil y el sector de la infomediación interesado en la reutilización. En este sentido, es posible dotar normativamente de cierta seguridad y estabilidad a las políticas de datos abiertos para facilitar inversiones por el sector privado y no quedar a expensas de la moda por los poderes públicos.

El "Open Gov" ha tenido un gran eco. En 2010 ocho países fundaron inicialmente la Alianza para el Gobierno abierto www. opengovpartnership. org a la que se sumó España en 2011 y que en 2014 ya cuenta con 83 países comprometidos a perseguir políticas de gobierno abierto estandarizadas a través de la presentación de informes y compromisos. El Ministerio de la Presidencia español presentó su primer informe a inicios de 2014[84] teniendo en cuenta a expertos (a través del Instituto Ortega y Gasset). Bien es cierto que dada la "apertura" del concepto, en dicho informe se reúne toda una amalgama de acciones que difícilmente puede decirse que obedecen a una política gubernamental definida y bajo una estructura. En cualquier caso, en España la emergencia de las políticas de "gobierno abierto" es evidente, especialmente en el nivel autonómico y local donde aparecen desde normativas de gobierno abierto hasta concejalías con este nombre[85]. Cuestión diferente es la voluntad real, profundidad y sostenimiento en el tiempo de tales políticas.

Hay que evitar que se tome el "gobierno abierto" como una simple moda pasajera en manos de frívolos y oportunistas gestores y consultores políticos. Para ello estimo fundamental la –buena- acción del Derecho para *fijar, limpiar y dar esplendor* al gobierno abierto. Es necesario asumir compromisos normativos que obliguen a los poderes públicos y fijen y organicen los cambios.

[84] Toda la información en http://www. opengovpartnership. org/country/spain

[85] Así, la Concejalía de Gobierno Abierto de Quart, Valencia.

2. Algunos errores y aciertos de los que aprender

Pese a que toda institución se apunte a la moda de ponerse un 2. 0 detrás o un "open" delante, lo cierto es que poco —y poco bueno— hay regulado que genere verdaderos derechos exigibles con garantías y obligaciones concretas. En los estatutos de autonomía desde 2006 se reciben principios y derechos emergentes de la órbita del "gobierno abierto": acceso a internet, buena administración, calidad de los servicios públicos, participación, acceso a la información y transparencia. El reconocimiento estatutario[86] tiene un claro papel simbólico e impulsor de políticas en estas materias, así como de formación de una cultura jurídica. Sin embargo y por lo general, cuando los Estatutos han reconocido estos nuevos derechos tampoco han colaborado a asentar la normatividad y exigibilidad de estos derechos emergentes, al no concretarlos normativamente. Y a ello hay que sumar la conocida doctrina establecida en la STC 247/2007, de 12 de diciembre que limita el alcance jurídico que tiene el reconocimiento de derechos en estatutos de Autonomía.

En materia de acceso a la información, las normas autonómicas o locales tradicionalmente proclaman principios, reiteran derechos o reenvían a la anterior normativa estatal[87], sin mayores aportaciones. Se avanzó algo en la Ley 4/2006, de 30 de junio, de transparencia y de buenas prácticas en la Administración pública gallega, sin contenidos jurídicos muy concretos. Más tarde, desde el anteproyecto o el proyecto de la ley estatal de transparencia en 2012 comenzaron a surgir interesantes regulaciones de gobierno abierto[88]. Estas leyes regulan la transparencia, fortaleciendo sobre todo las obligaciones de información activa o el ejercicio del acceso a la información, asimismo abordan también mecanismos de participación ciudadana de modo más o menos laxa. También se incluyen cuestiones de calidad de las Administraciones. Así, la mencionada

---

[86] La bibliografía es abundante, especialmente Castillo Blanco, F. A. : "Derechos y principios relacionados con la buena administración y la calidad de los servicios", en Balaguer Callejón, F. y otros (coords.) (2008): *Reformas estatutarias y declaraciones de derechos*, Junta de Andalucía, Instituto Andaluz de Administración Pública, Sevilla, 2008 págs. 351-373. Un análisis exhaustivo del ámbito autonómico —no sólo de la C. Valenciana— lo he realizado en mis estudios en Garrido Mayol, V. (dir.): *Comentarios al Estatuto de Autonomía de la Comunitat Valenciana*, Tirant lo Blanch, 2013 "Artículo 9. Derechos de buena administración, transparencia, participación, uso de lenguas y otros mandatos al legislador valenciano, págs. 237-260; "Artículo 19. Desarrollo equitativo, territorialmente equilibrado y sostenible y derecho de acceso a las nuevas tecnologías", págs. 375-393 y "Artículo 49. 3º. 16ª La competencia autonómica en el régimen de las nuevas tecnologías relacionadas con la sociedad de la información y del conocimiento", págs. 1713-1719.

[87] Por ejemplo, la Ley 8/2010, de 23 de junio, de Régimen Local valenciana que incluye un Capítulo sobre "Información y participación ciudadana" (arts. 137-143), en la que las únicas aportaciones de cierta concreción lo son respecto a la iniciativa y consulta popular local. De igual modo, son jurídicamente vacuos los derechos de acceso a la información en la Ley 11/2008, de Participación valenciana. También se aprecia este fenómeno en la regulación genérica, de principios que se da en leyes de administración como la Ley 4/2011, de 31 de marzo, de la Buena Administración y del Buen Gobierno de las Illes Balears o la Ley 9/2007, de 22 de octubre, de Administración de la Junta de Andalucía.

[88] El mejor análisis de tales regulaciones se debe a Castel Gayán, S. : "Gobierno abierto en el Estado autonómico: régimen jurídico *y estrategias", en Transparencia, participación ciudadana y administración pública en el siglo XXI,* ", en Bermejo Latre, José Luis y Castel Gayán, Sergio (eds.) *Transparencia, participación ciudadana y administración pública en el siglo XXI,* monografía XIV de la Revista Aragonesa de Administración Pública, IAAP, Zaragoza, 2013, Bermejo Latre, J. L. y Castel Gayán, S. (eds.), monografía XIV … *ob. cit.* págs. 159-202

A este respecto, especialmente Cotino Hueso, Lorenzo: "Derecho y "Gobierno Abierto". La regulación de la transparencia y la participación y de su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones públicas. Propuestas concretas", en Bermejo Latre, José Luis y Castel Gayán, Sergio (eds.) *Transparencia*, cit. págs. 51-96.

Ley Foral 11/2012, de 21 de junio, de la Transparencia y del Gobierno Abierto de Navarra y la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura y la más reciente Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía. También hay anteproyectos en Aragón o País Vasco y se han anunciado leyes en Comunidad Valenciana o Castilla y León, entre otras.

Cabe esperar que se supere la inercia de regular el gobierno abierto con fórmulas de las que no se derivan contenidos propiamente jurídicos y exigibles a los poderes públicos. Más allá del Derecho, todo suele quedar en manos del liderazgo y voluntad política. Ello es negativo internamente para la Administración, para los servidores públicos y para los altos directivos, por cuanto no se genera verdadera cultura de gobierno abierto, que queda como una cuestión departamental y no transversal, además sometida al libre decisionismo del Consejero, Director General o Concejal responsable de transparencia, participación y TIC de turno. Con normas así, finalmente tampoco se toman en serio el gobierno abierto los juristas y la doctrina, al no ver referentes de regulación serios que acaben de dar forma a derechos y principios.

No cabe duda de que la situación normativa ha ido mejorando con la legislación estatal y las secuelas autonómicas. Ya específicamente por cuanto a la regulación de las TIC cabe esperar el paso *del "podrán" al "deberán"* en materia de transparencia o participación a través de TIC. Cabe recordar que éste fue el lema de la avanzada Ley 11/2007 de e-Administración. Ejemplos de que la transparencia y participación a través de las TIC pueden ser reguladas de forma concreta y con garantías lo brinda la regulación de la transparencia y buen gobierno corporativo empresarial en la Ley 26/2003, de 17 de julio, con el fin de reforzar la transparencia de las sociedades anónimas cotizadas y toda su importante normativa de desarrollo[89]. De igual modo, también como contraste con la situación normativa en España y referente a partir del cual aprender, destaca el ya mencionado Reglamento (UE) nº 211/2011, sobre la iniciativa ciudadana europea. Como he expuesto en otros lugares[90], más allá de la importancia real de esta más que discreta institución participativa, estimo que es muy destacable esta regulación porque supone un *giro copernicano*. Frente a esta situación, el mencionado Reglamento parte de que el medio natural de la institución participativa son las TIC y toda la regulación gira alrededor de ello y, es más, se ponen los instrumentos y software libre para su desarrollo.

La mayoría de normas españolas, como la Ley 19/2013, de 9 de diciembre, de transparencia, respecto del ejercicio electrónico del derecho, simplemente se limitan a introducir como "cuña" que el derecho "se podrá ejercer por medios electrónicos". Ello evidencia que lo electrónico es algo ajeno y secundario y conlleva a que en la realidad no pueda ejercerse en la práctica el derecho en cuestión a través de medios electrónicos por la falta de regulación. En España y en teoría, se puede ejercer electrónicamente el derecho de petición (Ley orgánica 4/2001, art. 4). También el artículo 6 y 10 de la Ley 11/2007 garantiza que se puedan formular peticiones en la sede electrónica. La Ley Orgánica 3/1984 que regula la Iniciativa Legislativa Popular, gracias a su reforma por

[89] En especial, cabe tener en cuenta la Orden ECO/3722/2003, de 26 de diciembre, sobre el informe anual de gobierno corporativo y otros instrumentos de información de las sociedades anónimas cotizadas y otras entidades y la Circular 1/2004, de 17 de marzo, de la Comisión Nacional del Mercado de Valores, sobre el informe anual de gobierno corporativo de las sociedades anónimas cotizadas y otras entidades emisoras de valores admitidos a negociación en mercados secundarios oficiales de valores, y otros instrumentos de información de las sociedades anónimas cotizadas

[90] Puede seguirse Cotino Hueso, L. : " El Reglamento de la Iniciativa Ciudadana Europea de 2011. Su especial regulación de la recogida de apoyos vía internet y de la protección de datos de los ciudadanos", en *Revista de Derecho Político*, nº 81, 2011. Págs. 323-378.

Ley Orgánica 4/2006, de 26 de mayo, permite recoger firmas para promover cambios legislativos a través de Internet y de medios electrónicos, eso sí, exigiendo firma electrónica (art. 7. 4º). Asimismo, técnicamente, son necesarios sistemas que permitan la recogida de firmas de forma fiable, que sean auditados por las entidades de control. Pues bien, en por Acuerdo de 28 de enero de 2010 la Junta electoral Central en España homologó por primera vez una plataforma de recogida de firmas. Lo cierto es que el fracaso de su uso es bien evidente, con experiencias "desastrosas" como www. mifirma. com[91]

3. Necesidades de regulación en el ámbito del gobierno abierto, la participación y la información pública en internet

Las regulaciones que se produzcan podrían ser en general de naturaleza estatal, autonómica, local o normativa propia de instituciones corporativas autónomas.

Aunque la participación y la transparencia tienen aspectos vinculados a derechos fundamentales (arts. 23 CE y 20 CE) su regulación se vincula con el 105 CE (ver STC 119/1995). Así, en general, la regulación no afectaría a la dimensión subjetiva de estos derechos fundamentales o se trataría de regular elementos conexos o relativos al ejercicio del derecho del artículo 23 CE y no al "desarrollo" del mismo. Además, los nuevos Estatutos con sus aparentes derechos, principios y algunos títulos competenciales en temas de participación, transparencia, buena Administración, etc. refuerzan su posibilidad de regular estas materias. Por cuanto a la forma que habría de revestir la normativa, en los más de los casos tan siquiera sería precisa una norma de rango legal.

En el ámbito de la participación y las TIC cabe tener en cuenta que no hay que emplear necesariamente las TIC en todas y cada una de las fases del proceso participativo. Asimismo, hay que evitar requerir una identificación plena de la ciudadanía. En este punto no hay que desconocer que pese a más de 30 millones de e-DNI expedidos son pocos los que saben o consiguen utilizarlo. Asimismo, la protección de datos y la privacidad no pueden pasar a ser excusas o barreras frente a la transparencia y la participación electrónicas, sin perjuicio de la necesidad de cumplir con dicha normativa.

Procede regular elementos concretos para posibilitar el ejercicio electrónico de los derechos de participación y transparencia que habitualmente se proclaman. También es muy recomendable la regulación de los modos de contacto electrónico de la ciudadanía con la administración fuera de un procedimiento, como el correo y las redes sociales. Asimismo, cabe regular de forma concreta la existencia de un punto en la web institucional que centralice la información (portal de transparencia de la Ley 19/2013) así como la participación electrónica a la ciudadanía. Lo suyo es la integración de los contenidos de participación y datos abiertos. En el ámbito de la participación, es de todo interés fortalecer el marco jurídico de los órganos colegiados electrónicos, simplemente previstos en la Ley 11/2007, y cuya actuación reviste especial importancia en materia participativa.

De igual modo, respecto de la regulación de los sujetos que participan por la sociedad civil, las normas deben tener en cuenta que cada vez es más habitual la

[91] Así, Javier Peña e Ignacio Alamillo Domingo: "La identidad digital en procesos de democracia electrónica. La desastrosa experiencia de la firma electrónica basada en certificados, en mifirma. com", en Balcells, J. y otros (coords.): *Internet, Derecho y Política. Una década de transformaciones*. Actas del X Congreso Internacional, Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 3-4 Julio, 2014. Barcelona: UOC-Huygens Editorial, acceso en http://edcp. uoc. edu/symposia/idp2014/proceedings/

existencia de colectivos sin forma jurídica y que sólo existen en internet y las redes sociales, sin que ello en modo alguno implique una menor importancia política, social o administrativa. De igual modo, los registros de participación deben regularse para potenciar su difusión en la red –para facilitar tejer redes ciudadanas- al tiempo de cumplirse con la normativa de protección de datos.

Respecto de la difusión de la información pública a través de las TIC en general sería de interés la categorización jurídica de la actividad misma de divulgar información pública y de hacerlo a través de medios electrónicos; a partir de tal tipología puede aplicarse un régimen jurídico diferente. Otro elemento muy importante a regular es el régimen de responsabilidad jurídica por la mala información pública difundida por medios electrónicos. La Ley 11/2007 incluye requerimientos y derechos de calidad de la información a través de medios electrónicos (arts. 4 y 6), con exigencias más concretas respecto de la información de la sede electrónica (art. 10). Pero este marco jurídico no es suficiente ni para la ciudadanía ni para la Administración.

También, cabe mejorar el régimen jurídico del uso de redes sociales por las Administraciones públicas[92]. La incorporación de las instituciones y los servidores públicos a las redes sociales no se ha hecho de forma planificada, organizada ni con previsión de todas las complejas consecuencias jurídicas que implican. Cabe dotar de cobertura jurídica a esta realidad e introducir algunas pautas[93]. Una regulación adecuada puede: aminorar y mitigar posibles problemas jurídicos relativos al acceso por los empleados a las redes sociales, condiciones y horarios y si es uso personal o profesional; la normativa puede definitir la política de administración de cuentas, la separación entre el uso personal y profesional por los empleados y las normas de identidad corporativa. También hay que hacer referencias a las pautas a seguir respecto del lenguaje, así aclarar los tipos de contenidos a difundir y los que no proceden. Igualmente, pueden hacerse especificaciones de seguridad y sobre la conservación de los contenidos difundidos en las redes. Respecto de la conducta ciudadana se precisa el establecimiento de reglas de políticas de uso y, especialmente, que doten de cobertura a las posibilidades de controlar o moderar los contenidos integrados por terceros en espacios 2. 0[94], como foros, comentarios, redes, etc. [95] Asimismo cabe fijar pautas para no cometer discriminaciones al momento de "seguir" o "ser amigo" de unos u otros

[92] Cabe destacar las mejores prácticas referidas en el Directorio *Web 2. 0 Governance Policies And Best Practices – Reference*, elaborado por la red de empleados públicos Govloop. (http://bit. ly/ZlOtwr). Asimismo, Bonsón, E. y otros: "Local e-government 2. 0: Social media and corporate transparency in municipalities". Government Information Quarterly. Vol. 29 (2), págs. 123-132 y Chun, S. A. y otros: "Government 2. 0. Making Connections between Citizens, Data and Government". *Information Polity: The International Journal of Government & Democracy in the Information Age*. Vol. 15, págs. En España, cabe remitir a los manuales y guías referidos *infra* y en la doctrina, Cerrillo i Martínez, A. : "Web 2. 0 y la participación ciudadana en la transparencia administrativa en la sociedad de la información", en COTINO HUESO, L. : (coord.) *Libertades de expresión e información cit.* págs. 131-148.

[93] Desde las primeras investigaciones se han determinado ocho elementos esenciales de una política de *social media* de las instituciones, así, el estudio comparativo de 26 documentos de agencias gubernamentales sobre el uso de medios sociales por Hrdinová, J. y otros: *Designing Social Media Policy for Government: Eight Essential Elements,* The Research foundation of State University of New York, University at Albany, 2010. (http://bit. ly/cHDb58).

[94] De especial interés, Fundación CTIC: *Políticas de uso de servicios de participación ciudadana en el contexto de las administraciones públicas*, 2010 acortado http://bit. ly/bf5RyH.

[95] Sobre la materia no se dan prácticamente estudios jurídicos, a excepción de Rollnert Liern, G: "La neutralidad ideológica del Estado en las redes sociales", en *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Corredoira Alfonso, L. y Cotino Hueso, L. (dirs.): *Libertad de expresión…ob. cit.*

ciudadanos en unas redes u otras. No en vano está el riesgo de lesión de la libertad de expresión e información de la ciudadanía que interactúa con las Administraciones, al tiempo de la neutralidad y objetividad de la Administración. Además, es preciso determinar la unidad u órganos responsables de la gestión de las redes y las posibilidades de comunicación eficaz con ellos por los ciudadanos, así como determinar algunas garantías de la ciudadanía y sus las posibilidades de quejas y denuncias por contenidos y comentarios, etc. Puede ser de interés aclarar aspectos del uso de datos personales derivados de estas interactuaciones, y la necesidad de incluir avisos legales y políticas de privacidad.

Dada la naturaleza flexible informal de esta relación electrónica de la Administración a través de redes, pero con posibles consecuencias jurídicas, a mi juicio es idónea la técnica de que una norma jurídica especifique los aspectos orgánicos y competenciales y que remita a las recomendaciones y obligaciones que se contengan en las cada vez más habituales guías de usos y estilo o guías de comunicación digital[96]. De este modo, tales guías o manuales cobran existencia jurídica al tiempo de que puedan ser continuamente actualizadas[97].

VI. El nuevo derecho fundamental de transparencia y acceso a la información pública. Nuevas tecnologías y posibilidades de mejora de la Ley 19/2013 por autonomías y entes locales.

1. La fundamentalización del derecho de acceso a la información pública

En el ámbito de la Unión Europea la emergencia de la transparencia es muy clara. Se configura como un elemento de legitimación del sistema político de la Unión y premisa de la participación. Desde 2000, la Carta de los derechos fundamentales de la Unión Europea reconoció en el artículo 42 del "Derecho de acceso a los documentos"[98]. Dicho derecho para las instituciones y órganos de la Unión Europea adquirió valor jurídico con el Tratado de Lisboa de 3 de diciembre de 2007 (en vigor desde 2009), con una obra jurisprudencial amplia del Tribunal de Justicia de la Unión Europea. En 2001 se aprobó el avanzado Reglamento (CE) n° 1049/2001, la norma de acceso a la información ante las instituciones y órganos de la Unión. Este reglamento entre otras cosas ya reguló el ejercicio electrónico de acceso y potenció la transparencia activa electrónica hace doce años. En el marco del Consejo de Europa, constituye un hito el Convenio nº 205 del Consejo de Europa sobre el Acceso a los Documentos Públicos de 2009[99], no ratificado por España, que vincula este derecho con el artículo 10 CEDH y con el artículo 19 DUDH[100] que reconocen la libertad de expresión e información. En

[96] Así, cabe destacar desde 2010 la "Guía de usos y estilo en las redes sociales de la Generalidad de Cataluña" http://bit. ly/mCVjAV, emulada por el País Vasco http://bit. ly/jS58xP. También, entre otras la guía de Castilla y León http://bit. ly/Qb4xba o el manual de la Generalitat Valenciana http://goo. gl/5QHbr. Desde 2013 destaca sin duda la Guía de Comunicación Digital para la AGE http://goo. gl/m1AAj0

[97] Esta técnica respecto de la Administración electrónica se sigue, por ejemplo, en Colombia, donde el Decreto 1151 del 14 de abril de 2008 remite al cumplimiento del "Manual para la implementación de la Estrategia de Gobierno en línea Entidades del Orden Nacional" que a fecha de 2014, va por su versión 3. 1.

[98] Su redacción final es: "Todo ciudadano de la Unión y toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte. "

[99] Existe una muy completa traducción no oficial al español, conjunta al texto oficial en inglés, realizada por M. Sánchez de Diego en http://goo. gl/Kz7EA

[100] A este respecto cabe recordar el Comité de Derechos Humanos: *Observación General núm. 34 (2011). Artículo 19. Libertad de opinión y libertad de expresión*. Especialmente ver párrafos 18 y 19.

esta línea y también en 2009, el TEDH comienza a seguir la estela de la decisión de 2006 de la Corte Interamericana[101], que reconoció el acceso a la información pública sin interés legítimo como integrante del derecho a la libertad de expresión del artículo 10 del Convenio. El TEDH en los asuntos contra Hungría *Társaság a Szabadságjogokért*, (sentencia de 14 de abril de 2009, en especial, aps. 35-39), y *Kenedi,* (sentencia de 26 de agosto de 2009) ha afirmado que el derecho de acceso a los documentos públicos es "un elemento esencial del ejercicio […] del derecho a la libertad de expresión (ap. 43, Sentencia Kenedi)". Y especialmente cabe destacar la sentencia dictada en el caso *Youth Initiative for Human Rights* c. Serbia (de 25 de junio de 2013), en la que se afirma la lesión del artículo 10 CEDH a una ONG interesada en la información pública —esto es, no se trataba de profesionales de la información— y "el Tribunal recuerda que la noción de "libertad para recibir información" abarca un derecho de acceso a la información" (ap. 20)[102].

Así pues, el doble influjo europeo hace incuestionable el carácter de derecho fundamental para el Derecho nacional en razón del artículo 10. 2º CE. Los componentes esenciales de la transparencia y el acceso a la información quedan integrados en contenido constitucional declarado del artículo 20. 1 CE. Asimismo y como consecuencia obligada, hay que interpretar la Ley de transparencia bajo la perspectiva de que el acceso a la información pública es un derecho fundamental. Ello es así sin perjuicio de que la fundamentalidad se refuerce —aún más— en algunos supuestos, como el acceso a la información por parte de cargos públicos, en razón del artículo 23 CE[103]. Como consecuencia general se impone *tomar en serio* toda LA normativa de desarrollo y ejercicio del derecho de acceso, con especial incidencia a la hora de ponderar sus límites (art. 15 Ley 19/2013). Asimismo, en razón de la dimensión objetiva de los derechos fundamentales se impone el mandato constitucional para los normadores, administraciones y jueces de hacer efectivo este derecho fundamental. Ello ha de tener especial incidencia respecto del futuro desarrollo legal y reglamentario así como en implantación y puesta en práctica efectiva de la ley por los poderes públicos. También los tribunales deben tomarse este derecho en serio al aplicar la ley. Por ello, cabe esperar una actualización de la jurisprudencia constitucional, pues en 2013 el TC no parece haber recibido estos estímulos[104]. También hay que aguardar la puesta al día por la jurisprudencia ordinaria[105]. Ello sería de especial utilidad para impulsar y mejorar

[101] Caso, Claude Reyes y otros vs. Chile, la sentencia reconoce en su apartado 77 y al amparo de la libertad de expresión la existencia de un derecho humano fundamental de acceso a la información en manos de los gobiernos en su apartado sin necesidad de acreditar interés directo y a salvo de las restricciones del Convenio.

[102] Y como nos recuerda Rollnert en este libro, además, en una opinión concurrente conjunta, los jueces Sajó y Vučinić recalcaron "la necesidad general de interpretar el artículo 10 de conformidad con el desarrollo de la legislación internacional respecto a la libertad de información, que supone el acceso a la información que disponen los organismos públicos".

[103] Recientemente destaca la STS de 28 de septiembre de 2012 de la Sala Tercera que considera que el acceso a la información de los parlamentarios forma parte del contenido del artículo 23 CE y son los reglamentos parlamentarios los que deben dotarle de la oportuna configuración legal con las necesarias garantías (FJ 3º).

[104] Así, cabe tener en cuenta los dos autos de 9 de septiembre de 2013 en los que las dos Secciones de la Sala Primera del Tribunal Constitucional han inadmitido los recursos de amparo promovidos por Access Info Europe 3254/2012 y 4145/2012 "dada la manifiesta inexistencia de violación de un derecho fundamental tutelable en amparo". Access Info ha afirmado su voluntad de acudir al TEDH.

[105] Al respecto cabe tener en cuenta las sentencias que fueron impugnadas en los recursos de amparo citados *supra*, SAN de 22 de octubre de 2009 y STS de 29 de mayo de 2012. De igual modo, hay que tener en cuenta las SSTS de 30 de marzo de 1999, de 14 de noviembre de 2000 y de 19 de mayo de

la actuación ordinaria de las administraciones, así como del Consejo de la Transparencia y otros órganos afines autonómicos que deban resolver al respecto del derecho de acceso y todos los que deban cumplir con la normativa de información activa.

2. Las posibilidades de mejora de la ley estatal desde el ámbito autonómico o local

Son muchas críticas mayoritariamente acertadas que ha recibido la Ley 19/2013[106], entre las que cabe incluir las formuladas del presente libro. Sin perjuicio de tales críticas, a mi juicio la valoración general de la Ley 19/2013 es necesariamente positiva, cuanto menos, dada la situación precedente. Bien es cierto que puede calificarse como una *ley gatopardesca*[107] bajo la máxima de Lampedusa de "cambiar todo para que nada cambie". Jurídicamente es una ley mucho más sólida y con compromisos jurídicos más serios que las referidas regulaciones locales y regionales. Asimismo, en términos generales, es una ley homologable a las legislaciones de transparencia al uso y, salvo matices, adecuada al ya referido Convenio nº 205 del Consejo de Europa de 2009 del que no somos parte.

Son diversos los aspectos mejorables de la Ley 19/2013 a los que se hace ahora referencia, no sin antes señalar que en muchos casos y precisamente estas debilidades son una oportunidad para las regulaciones autonómicas o en su caso locales[108]. El ámbito de actuación es especialmente intenso en materia de publicidad activa. Así, las actuaciones y regulaciones autonómicas o locales pueden, por ejemplo, ampliar los contenidos obligatorios a los que se ha de dar información activa. De hecho, los artículos 5. 2º y 10. 3º hacen expresa referencia a la actuación autonómica en este sentido. Se puede ser especialmente activo e innovador respecto de los portales de transparencia. Asimismo, se puede mejorar la escasa garantía de cumplimiento de estas obligaciones que se da en el artículo 9. Se puede obligar a "ciudadanizar" la información pública al punto de que la ciudadanía pueda exigir su cumplimiento.

2003. Como señala Rollnert, no se puede concluir que el TS tenga una posición determinante en la materia.

[106] Por todos, Coalición Pro Acceso: *Propuestas de la Coalición Pro Acceso para mejorar la Ley de Transparencia, Acceso a la Información y Buen Gobierno* Madrid, 19 de septiembre de 2012. http://goo. gl/rbUUxp; Fernández Ramos, S. : "El acceso a la información en el Proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno", ponencia en el Seminario de Modernización y Apertura de la Administración Pública, Zaragoza, 27. 09. 2012, págs. 9-10, disponible en http://goo. gl/eegn2k, también "El acceso a la información en el Proyecto de Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno", *Transparencia, participación ciudadana y Administración Pública en el siglo XXI*, Bermejo Latre y otros *ob. cit. ,* págs. 233-298, disponible en http://goo. gl/tR0vo7). Una visión especialmente crítica Sánchez De Diego, M. : "Transparencia y acceso…" *ob. cit.* Más recientemente cabe tener especialmente en cuenta las obras monográficas coordinadas por Guichot Reina, Emilio: *Transparencia, acceso a la información pública y buen gobierno,* Madrid. Civitas. 2014 y Fernández Salmerón, M. y Valero Torrijos, J. (coords.): *Régimen jurídico de la transparencia en el sector público: acceso, uso y reutilización de la información administrativa*, Thomson-Aranzadi, Madrid, 2014. También, Blanes Climent, Miguel Á.: *La transparencia informativa de las Administraciones Públicas. El derecho de las personas a saber y la obligación de difundir información pública de forma activa*, Thomson-Aranzadi, Madrid, 2014.

[107] Así, Nuez Sánchez-Cascado, E. : "El proyecto de Ley de Transparencia, Acceso a la Información Pública y buen Gobierno ¿Una ley gatopardesca?" en *¿Hay Derecho?* 24 septiembre 2012. http://goo. gl/LbA5w

[108] En el ámbito local es muy destacable a mi juicio el texto a partir de Muñoz Soro, Ordenanza sobre transparencia y libre acceso a la información de Zaragoza, (aprobación inicial Pleno el 31. 01. 2014, publicado en BOPZ nº 30 de 07. 02. 2014) ver http://www. zaragoza. es/ciudad/normativa/detalle_Normativa?id=3983

También se puede incluir catalogación y difusión de los listados y tipología de información pública activa.

Respecto del derecho de acceso, de la Ley 19/2013 es reprochable que no se regule el acceso a la información como derecho fundamental, no obstante, ello facilita si cabe el juego a la normativa regional y local. En este sentido, el artículo 12 hace expresa referencia a la regulación autonómica respecto del derecho de acceso. Un especial marco de actuación autonómico y local es regular y hacer efectivo el ejercicio electrónico del acceso a la información. Pese a que es "preferente" para la ley (arts. 17. 2º y 22. 1º), no se concretan los requisitos y medios. En este punto, la flexibilización de la identificación electrónica del solicitante, e incluso la innecesariedad de tal identificación puede ser muy importante. En la Ley 19/2013 son muy mejorables las garantías y los mecanismos de control y revisión frente a las denegaciones de acceso, queda por tanto un buen ámbito de actuación para la regulación de desarrollo. A este respecto, el plazo de un mes del artículo 21 para que las Administraciones den respuesta a las solicitudes de acceso a la información puede recortarse o, por ejemplo, disponerse que a partir de 15 días de la solicitud la Administración habrá de justificarse el retraso. Del mismo modo, se puede regular mejor la reclamación tras la denegación o incluso regular el sentido del silencio negativo de la Administración ante una solicitud de acceso (siendo positivo en art. 30 Ley Foral 11/2012 de Navarra). Puede limitarse dicho silencio negativo sólo a unos supuestos tasados, por ejemplo.

Habrá que ver el papel que adopte el finalmente denominado Consejo de la transparencia. Por su regulación y composición hay motivos para ser escépticos sobre el dudoso activismo que asumirá. Pues bien, en razón del artículo 24. 6º y la Disposición adicional 4ª, hay un amplio espacio de regulación autonómica respecto del órgano de control y garantía del derecho de acceso. En este punto bien es posible contemplar la participación de *ombudsmen* autonómicos (art. 68 Ley Foral 11/2012 de Navarra) o autoridades de protección de datos donde las haya (País Vasco o Cataluña) o crear nuevas, como parece ser el futuro Consejo de Transparencia y Protección de Datos de Andalucía por cuanto a la autoridad independiente autonómica a quien atribuir la resolución de la reclamación tras la denegación o silencio negativo. Asimismo, también cabría reducir el —excesivamente amplio— plazo máximo de tres meses para resolver esta reclamación (art. 24. 4º). Otro espacio de regulación de interés es el relativo a la fijación de infracciones y sanciones del personal de las Administraciones en razón de la transparencia y el acceso a la información. La Ley 19/2013 casi lo desconoce y, en razón del artículo 57 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, este régimen sancionador del personal queda en manos de las Comunidades Autónomas, que hoy día no contemplan infracciones en la materia. Destaca en este sentido, la recién aprobada Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Entre los reproches de la Ley 19/2013 cabe a mi juicio destacar el potencial peligro de que, en razón de la Disposición adicional primera, cualquier regulación especial de acceso a la información, incluso por reglamento, hace que la ley no sea aplicable[109]. Pues bien, de nuevo esta debilidad puede ser positiva. Si hay voluntad, es posible mejorar la regulación en amplios sectores de actuación que son competencia autonómica e incluso se cuenta con atribuciones locales.

[109] En especial Fernández Ramos, S. : "El acceso a la información …", *ob. cit.* Recientemente, Barrero Rodríguez, M. C. : "La disposición adicional 1. 3º del Proyecto de Ley de Transparencia, acceso a la información y buen gobierno y sus negativos efectos en el ámbito de aplicación del derecho de acceso a la información", en *Civitas. Revista española de derecho administrativo*, nº 158, 2013, págs. 221-246.

Estas mejoras de la regulación propuestas a llevar a cabo por Comunidades Autónomas o en su caso por entes locales, fácilmente quedan bajo el amparo de la ley estatal y no afectarían a la dimensión subjetiva del derecho fundamental de acceso a la información, sino que se trataría de regular elementos conexos o relativos al ejercicio del derecho, no al "desarrollo" del mismo. Además, los Estatutos de Autonomía por lo general con sus nuevos derechos y competencias dotan de cobertura a la regulación autonómica, siempre bajo las potestades de auto organización administrativa o los derechos y competencias vinculados a la sociedad de la información[110] y generalizada asunción autonómica de competencias en materia de archivos y registros. El desarrollo puede darse a través de ley autonómica, pero también cabe la vía reglamentaria en la mayoría de supuestos. Aunque tuviera conexidad con derechos fundamentales, en muchos supuestos, la normativa relativa al uso de tecnologías por las Administraciones consistiría en el desarrollo instrumental o tecnológico secundario que no exige de rango legal (STC 77/1985).

VII. Campañas electorales, TIC y voto electrónico

En el ámbito de los derechos de participación, las TIC son ya herramienta indispensable de comunicación y campaña para candidatos y partidos políticos. Jurídicamente, respecto de las limitaciones y prohibiciones en campaña, en España por ejemplo la Instrucción 4/2007, de 12 de abril111, de la Junta Electoral Central ya recordó que "las limitaciones establecidas por la legislación electoral son también aplicables al uso de este tipo de medios electrónicos" (Exposición de Motivos). No obstante, diversas prohibiciones como las de jornada de reflexión electoral o restricciones de difusión de encuestas y sondeos pueden ser fácilmente burladas con medios electrónicos y la eficacia material de las mismas es decadente.

Por cuanto al voto electrónico, en Europa hay general desconfianza, con reacciones políticas en contra en Italia, Holanda y Bélgica. Cabe especialmente hacer referencia a la sentencia del Tribunal Constitucional Federal alemán de 2009[112] donde se analizaron las dificultades de transparencia real del proceso y posibilidades efectivas de control por cualquier ciudadano y se afirman reglan imprescindibles a cumplir. En aquél caso se consideró inconstitucional la ley de un Länder sometida a debate. Por lo que aquí interesa, se concluyó que ventajas del e-voto como la disminución (o incluso supresión) de los errores involuntarios del elector, que generan votos nulos no deliberados, o la rapidez en la publicación de los resultados no constituyen argumentos de peso suficiente como para deshacer la regla común de la publicidad y la comprensión electoral. En España, desde antiguo existe la Ley 15/1998 sobre el voto electrónico para el País Vasco, que se ha reformado en varias ocasiones pese a que nunca se ha aplicado. De igual modo el voto electrónico se regula con cierto detalle en la Ley 4/2010, de 17 de marzo, de consultas populares por vía de referéndum de Cataluña. Al parecer la

[110] Como se señala en la nota a pie nº 78, *supra,* he realizado un análisis desde el punto de vista autonómico en los trabajos ahí citados. Destaca en este sentido el artículo 19 del Estatuto valenciano, en buena medida copiado por el artículo 34 del Estatuto de Andalucía, también copia título competencial en nuevas tecnologías (art. 58. 2º), asimismo, se asume la competencia ejecutiva "*en materia de comunicaciones electrónicas"* (art. 64. 9º). El acceso a las TIC se regula como mandato de promoción en los estatutos catalán (art. 53), balear (art. 29) o aragonés (art. 28. 2º). El Estatuto de Extremadura copia la competencia valenciana en su artículo 9. 1. 23ª. Por cuanto a las competencias, el artículo 29 del Estatuto balear regula el impulso del acceso a las nuevas tecnologías; el artículo 28. 2º del Estatuto de Aragón incluye la promoción del acceso y el "fomento y desarrollo de las tecnologías para la sociedad de la información".

[111] http://goo. gl/jCAIzT

[112] En inglés en http://goo. gl/xnT5mc

cuestión del e-voto no genera especial polémica en un marco de inactividad sobre su implantación en España.

Conclusiones y propuestas

Ni las nuevas tecnologías son tan nuevas ni, por tanto, son rabiosamente actuales todas las dificultades jurídicas que plantean. Lo que sí que es cierto es que constantemente se generan nuevas preguntas jurídicas al mismo ritmo que cambian las tecnologías y los usos que les damos. Se trata, pues de grandes vías de agua abiertas que inundan el barco y, lo que es peor, sin que se hayan cerrado las más antiguas y sin que se achique el agua a un buen ritmo.

El legislador, la jurisprudencia y en muy buena medida la doctrina vienen mirando hacia otro lado mientras esto sucede. Durante mucho tiempo estas disfunciones parecen casi imperceptibles, salvo para quienes directamente les afectan: empresas del ámbito tecnológico que ejercen con inseguridad e incertidumbre en su sector, o el sector de los contenidos que ve como menguan extraordinariamente sus ganancias sin que haya un marco jurídico que les proteja efectivamente, muchísimas empresas que se ven amenazadas por una posible sanción de protección de datos; policías y fiscales, que tienen que practicar investigaciones y manejar comunicaciones electrónicas, datos personales y de tráfico, al filo de la inconstitucionalidad, a riesgo de que todas sus actuaciones devienen ineficaces. O a los millones de empresas y ciudadanos obligados a interactuar con la Administración electrónicamente sin posibilidad de acudir a los canales convencionales. Sin embargo, en la mayoría de los casos, los riesgos de un deficiente marco jurídico y legislativo no se aprecian porque directamente no se aplica la normativa o se torna casi un simbolismo. Por ello, cuarenta millones de españoles no se ven amenazados por una normativa de protección de datos que nos sitúa a todos masivamente en la ilegalidad, a riesgo de unas sanciones administrativas del todo punto desproporcionadas, peores en la práctica que las sanciones penales. Millones de españoles que no saben si para tratar datos necesitan del consentimiento de las personas afectadas o les basta con un "interés legítimo" que les exima de tal consentimiento. Son estos españoles los mismos que tienen un derecho de protección de datos basado en un teórico consentimiento y unas garantías que no ejercen en la práctica. Cientos o miles de webs o millones de usuarios de redes sociales rutinariamente vulneran la legislación de propiedad intelectual, de protección de datos o la Ley 34/2002 de Servicios de la Sociedad de la Información, incumplimientos que por lo general no se persiguen; en consecuencia la ciudadanía se cree exenta de responsabilidad. Millones de trabajadores pueden ser plenamente monitoreados por sus empresarios sin que prácticamente tengan noción de ello. Todas las administraciones que practican cesiones de datos amparadas en leyes que por lo general no vienen a cumplir los estándares constitucionales. Millones de usuarios de webs institucionales o que intercambian correos con los servidores públicos y no saben que no pueden confiar en la información pública a la que acceden y parece que jurídicamente no tiene valor ni certeza alguna. El largo etcétera se hace cada vez más largo y ya se hace casi imposible eludir cuestiones que afectan prácticamente a toda la población en su quehacer diario. Se cuentan por decenas o cientos de miles las personas impunemente amenazadas, injuriadas, acosadas a través de internet. Y quedan desamparados y sin garantía alguna de que *Youtube, Twitter, Facebook, Wordpress* y otros tantos prestadores o intermediarios les contesten en alguna ocasión respecto de tales contenidos que lesionan su cada vez más importante reputación digital. El círculo es ya tan grande que mirar para otro lado ya no sirve. Se necesita acometer los problemas. *Sólo* se trata de la actividad cotidiana de unos

cuatrocientos millones de europeos y unos treinta y cinco millones de personas en España, además de todas las administraciones y todo el entramado empresarial y social que implican los prestadores de servicios e intermediarios europeos o extranjeros.

El Derecho, como la venganza, es un plato que se ha de comer frío. Eso es cierto y, por tanto, las soluciones jurídicas necesitan de unos tiempos para decantar los problemas, percibir los intereses sociales, económicos, políticos inherentes y decidirse por una u otras soluciones. Y ello cuesta especialmente en el cambiante y complejo mundo digital. Sin embargo, la inacción conlleva que las soluciones vengan por la vía de hecho y cristalicen los problemas ya sin marcha atrás. Pese a tratarse de un terreno preciso de ponderación para cada caso concreto y de necesaria adaptación al contexto tecnológico y al uso social de las TIC, el Derecho hoy puede dar alguna fijeza y certidumbre. La provisionalidad es y será una constante en el ámbito de las TICs y siempre será mejor hacer algo y rectificar si no es la vía correcta. De hecho la flexibilidad y adaptación constante al cambio es un elemento definitorio de la web 2.0 y debe proyectarse también al Derecho.

Cualquiera dirá con razón que hoy día no es nada escasa la normativa española o europea vinculada a las nuevas tecnologías, como la relativa a comercio electrónico, telecomunicaciones, prestadores de servicios de la sociedad de la información, protección de datos, propiedad intelectual, delitos informáticos, Administración electrónica, etc. Sin embargo, como se ha expuesto a lo largo de estas páginas, el conjunto normativo hace auténticas aguas en no pocos temas clave. Y aquí sólo se ha centrado la atención en materias vinculadas a los derechos fundamentales.

La jurisprudencia y los altos tribunales español o supranacionales son esenciales para perfilar muchos problemas que genera internet y que aquí se han expuesto. Aunque en general los jueces han sido primero ignorantes y luego reticentes a implicarse en las movedizas tierras de internet, se han visto compelidos a ello especialmente por la inacción legislativa. Es más, en casos como el del derecho al olvido y *Google* parece que han sido los jueces los únicos con valor de enfrentarse a un auténtico poder fáctico que influye sobremanera en la toma de decisiones políticas. O más bien en el retraso en la adopción de tales decisiones. Sin embargo, ya es hora de que el legislador europeo y nacional asuma su responsabilidad democrática, puesto que al fin y al cabo los jueces sólo pueden hacer de legislador negativo y marcar algunas direcciones.

A lo largo de este estudio en numerosas ocasiones se han apuntado temas clave que necesitan de la acción normadora y líneas generales de solución. Lo idóneo en general es una regulación europea que imponga criterios de homogeneización y marcos nítidos de solución de conflictos. No obstante, es en sede nacional donde deben y pueden resolverse y ponderarse los conflictos concretos de los derechos fundamentales con otros derechos, bienes e intereses. Precisamente hay que significar que la pereza y elusión de responsabilidades ha sido muchas veces del legislador nacional escudándose en las más elevadas competencias europeas. Sin embargo, en muchos de los terrenos conflictivos que aquí se han analizado, los tribunales supranacionales siguen concediendo un grado de discrecionalidad muy amplio en sede nacional. Por ello, hay que exigir que el legislador asa las riendas y marque algunas pautas en sede española, especialmente ante el palmario retraso en la toma de decisiones en la Unión Europea. Es más, en algunos casos las soluciones pasan incluso por el ámbito autonómico y local, especialmente en temas de gobierno abierto y Administración electrónica. El tiempo demuestra que tampoco vale echar balones fuera acudiendo a la necesidad de una autorregulación que no llega. Es hora de exigir procedimientos o mecanismos para

establecer con la industria, como la configuración por defecto de los servicios de la sociedad de la información.

No hay que temer la especialización o sectorialización del régimen jurídico. Internet es como la calle y no todo lo que puede haber en la vía pública merece una regulación idéntica, sino una adecuación y contextualización. A la vista de la experiencia y sin perjuicio del dinamismo de la red, es bien posible describir funcionalidades y servicios para aplicarles regímenes jurídicos singulares. Baste apuntar que la normativa hoy día desconoce que existen buscadores, redes sociales, lugares de comercio masivo, grandes centros de consejos y opiniones para los usuarios, lugares que facilitan el acceso a contenidos concretos, servicios de almacenamiento masivo por usuarios, etc.

Son muchas las sugerencias aquí realizadas a los legisladores, así como la enunciación de necesidades a las que intentar dar respuesta. Todo ello, si se me permite, con la casi certeza de que esta *carta a los Reyes* caerá en saco roto. Me atrevo a compartir cierta desesperanza respecto de la adecuación del Derecho a las nuevas, y no tan nuevas, tecnologías que con gran acierto Rodríguez ha verbalizado:

"En la medida en que cada vez mayor número de ciudadanos acudirán a internet para confiarle más y más facetas de su existencia, estos problemas no harán sino incrementarse y resultar más patentes.

Por otra parte, todo parece indicar que en una buena porción de importantes cuestiones el ciberespacio y el Derecho seguirán sus respectivas órbitas tranquilamente, desconocidos el uno para el otro. Puede que de modo eventual esas "órbitas" se alineen en algún punto, pero esto no será lo frecuente. […] La rápida evolución de internet contrasta con la lentísima evolución de la creación del derecho, y nada hace pensar que ambos rasgos vayan a cambiar."[113]

[113] Rodríguez García, Luis Fernando: "Políticas de la Federal Communications Commission en materia de neutralidad de la red", en Cotino Hueso, L. (editor): *Libertades de expresión e información en Internet… cit.* págs. 99-113.