-Capítulo “Democracia electrónica y libertades en la red”, 51 páginas, materiales del Módulo “Democracia electrónica”, Cuso “Democracia Y Derechos Humanos” (14 créditos), Master en derechos humanos, Estado de derecho y democracia en Iberoamérica, de la Universidad de Alcalá de Henares, Programa Regional de Apoyo a las Defensorías del Pueblo en Iberoamérica (PRADPI), abril de 2010.

Investigador principal del Proyecto I+D+I “Las libertades informativas en el contexto de la web 2.0 y las redes sociales: redefinición, garantías y límites”, del Ministerio de Ciencia e Innovación” (DER2009-14519-C05-01/JURI)

Contenido

I. Terminología, conceptos y concepciones de democracia electrónica

En el primer módulo del curso se hizo clara referencia a la dificultad que implica el tratamiento de democracia como concepto y como concepción. Este mismo problema se reproduce e incluso se acentúa cuando se trata de la llamada "democracia electrónica". De hecho, la variedad y discrepancia parte de la terminología misma.

1. Variada terminología

La terminología en la literatura sobre la materia es muy variada: e-democracia, i-democracia, democracia electrónica, e-participación, participación electrónica, ciberdemocracia, teledemocracia, democratización electrónica, ciberpoder, ciberciudadanía, ciudadanía.com, y un largo etc. A estas formas no dejan de añadirse recientemente otras como e-cognocracia o democracia electrónicamente influida, por ejemplo.

Pese a los intentos por diversos autores de atribuir una connotación particular a estas diferentes terminologías (plasmando diferentes "concepciones" de democracia, en el sentido que se expuso en el módulo 1) lo cierto es que se utilizan unas y otras expresiones casi indistintamente sin consolidarse doctrinalmente.

Por mi parte, prefiero denominar democracia o participación electrónicas, o e-democracia, casi indistintamente, a la concesión de un papel importante a las tecnologías de la información y comunicación (en adelante, TICs) en los procesos democráticos y participativos de los sistemas democráticos liberales. La Recomendación CM / Rec (2009) 1 del Comité de Ministros a los Estados miembros sobre la democracia electrónica (e-democracia), en adelante (Recomendación e-democracia 2009) ha venido a seguir esta noción, al afirmar "como el apoyo y fortalecimiento de la democracia, las instituciones democráticas y los procesos democráticos por medio de las TIC, es sobre todo acerca de la democracia. Su objetivo principal es el soporte electrónico de la democracia." (Recomendación e-democracia 2009, nº 3).

De hecho, se trata de un concepto que afecta a muy variados ámbitos:

"Abarca la E-democracia, en particular, e-Parlamento, e-legislación, e-justicia, e-mediación, e-medio ambiente, e-electorales, e-referéndum, e iniciativa, el voto electrónico, e-consulta, e- peticiones, e-campaña, e-

encuestas, la e-democracia hace uso de la e-participación, e-deliberación y foros electrónicos" (Principio nº 35 Anexo).

En cierto modo, todo el nexo de las materias seguidas en los módulos anteriores de este curso al vincularse con las TICs, valen como un concepto amplio de democracia electrónica.

2. Versión fuerte y versión débil de democracia electrónica

El instrumento que son las TICs bien puede proyectarse en las diversas concepciones de la democracia: tanto en la democracia representativa, la democracia participativa, como en la democracia directa, o más allá de esta terna conceptual, en ámbitos como la llamada democracia social o incluso la empresarial y corporativa. Las TICs son herramientas de comunicación y como tales son medios eficaces para todo proceso participativo de difusión de información y conocimiento, consultas, deliberación, posicionamiento y en su caso, voto.

a) Versión fuerte: e-democracia como democracia directa

Debe advertirse que los estudios sobre democracia electrónica se dan desde mediados del siglo XX. En el tratamiento de la cuestión, hay tanta variedad como autores, en todo caso, puede valorarse de forma genérica el estado de la cuesión. El tratamiento jurídico suele ser escaso y poco profundo, y buena parte de los estudios eran bastante visionarios y utópicos y, por lo general, partían de una crítica –destructiva o constructiva, según los casos- de la democracia representativa, como algo a superar gracias a las TICs. En este sentido, las TICs vienen a ser la *excus*a para cambiar el sistema político. Así las cosas, bajo terminologías diferentes, con la "democracia electrónica" parece latir una apuesta –muy variada- por una democracia directa, en la que cada ciudadano puede expresar instantáneamente, desde su pantalla de ordenador, su punto de vista sobre cuestiones que se sometan a su elección o sobre las que se recabe su opinión, optando a favor o en contra de ellas: una votación continua desde cualquier lugar sobre todos los temas en discusión política. Podríamos decir con Pérez Luño que ésta es una "versión fuerte" de la e-democracia. A mi juicio, vincular las nuevas tecnologías a la democracia directa con votación continua de los asuntos públicos, puede tildarse de "teledemagogia".

Esta visión bastante habitual sobre e-democracia llevaba hasta hace pocos años a que la literatura sobre la materia centre la atención casi monográficamente en el voto telemático o electrónico, descuidando, por

el contrario, otros ámbitos esenciales. Ahora bien, estos "expertos" mayormente desconocían la marcha real y usos de la red por los internautas y la ciudadanía, que les ha sobrepasado por completo por encima. El ciudadano ha pasado a ser el centro de la sociedad de la información en la web 2.0.

b) Versión débil: las TICs como herramienta de mejora de la democracia, no centrada en el voto electrónico.

Como se dijo en el primer módulo, en este curso se apuesta en general por una concepción de la democracia que tienda a ser más deliberativa y más participativa, siempre en el marco de un sistema de democracia representativa e indirecta, que es la que permite el mejor ejercicio y garantía de los derechos fundamentales, vía que ha seguidor la citada Recomendación e-democracia 2009 del Consejo de Europa:

"La democracia electrónica es 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 más legítima decisiones políticas." (Principio nº 9 del Anexo).

No se trata, pues de acabar con la concepción predominante de democracia y suplantarla por otras. De hecho, las democracias representativas deben readaptar su papel, *"Los políticos y los partidos políticos deben aprovechar la e-democracia con el fin de mantener y, si es posible, mejorar su papel esencial como la democracia "intermediarios"... "deben aprovechar las oportunidades que ofrece la e-democracia con el fin de conectar con los ciudadanos y la sociedad que representan, y con compañeros de partido y los órganos del partido." (Criterios 22 y 23 Recomendación e-democracia 2009)*

Las "TICs" no han de ser las protagonistas, sino el *instrumento* de evolución del modelo político. La democracia será lo que las personas queramos, y como afirma Castells, la red será lo que la gente quiera que sea, pues son los usuarios quienes definen su uso. Esta idea también la acoge la Recomendación e-democracia 2009:

"la tecnología más y mejor en sí mismo no conduce a la democracia más y mejor" (Principio nº 49), "La tecnología es de importancia secundaria a las consideraciones democráticas. No debe ser la razón para la introducción de la e-democracia" (Principio 51). Es por ello que "G.1. Al presentar, revisar y mejorar la e-democracia, la atención debería centrarse en la democracia y sus grupos de interés - no en la tecnología." (Criterio nº 1 Anexo).

De igual modo, creo que hay que insistir que la democracia electrónica ni empieza ni acaba, afortunadamente, en el voto

electrónico, pese a que hasta la eclosión de la web 2.0 o web social participativa se suelan identificar.

La web 2.0 o web social o participativa, el ciudadano como protagonista activo

La evolución y el uso real y actual de la red obliga a que cualquier referencia a la participación y democracia electrónicas no eluda la realidad del uso ciudadano y participativo de la red en la llamada web 2.0 o web social . Se trata de la superación de la estática web html –que sería el web 1.0-, información dispuesta de forma jerárquica (del creador del contenido hacia el lector pasivo) y no actualizada frecuentemente. Por el contrario, ahora el uso de la web está orientado a la interacción y redes sociales. Los sitios web 2.0 actúan más como puntos de encuentro , bajo una cultura particular, la cultura blog . Me estoy refiriendo a diversos fenómenos comunicativos a través de la red y alternativos a los medios de comunicación tradicionales , como el periodismo alternativo o ciudadano, los blogs , wikis, foros, etc.- o la expresión de movimientos sociales a través de la web 2.0. Frente a la web 1.0, ahora se permite la integración, interacción y selección de contenidos por el usuario (*youtube*, por ejemplo), que deja de ser un receptor, un consumidor de información, sino un "prosumidor" (prosumer) de información, esto es, un híbrido de consumidor y productor de contenidos , en deliberación continua. También, redes sociales como *Facebook* o *Tuenti* son ejemplos de la web 2.0 en su fenómeno de crecimiento geométrico de las redes sociales. El éxito de la web social estriba, en buena parte, en la gran facilidad de las nuevas herramientas. En todo caso, no hay que olvidar que a diferencia de la web 1.0 el usuario no es pasivo sino activo y requiere de unas destrezas importantes, lo cual agrava la importancia de la alfabetización digital y la posible discriminación de los desconectados.

Como hito de este proceso, la declaración de personaje del año de Time en 2006

Las TICs facilitan el empoderamiento del ciudadano, la construcción desde abajo arriba, el control de la información así como "la e-democracia debe permitir más participación del ciudadano en establecer la agenda, el análisis y la formulación, ejecución y seguimiento de la política." (Directriz nº 7 Recomendación e-democracia 2009).

""la e-democracia puede ser introducida por cualquier interesado. Puede ser iniciada de arriba hacia abajo, es decir, por las autoridades públicas, en todos los niveles de gobierno, o de abajo hacia arriba, es decir, por los ciudadanos. También puede ser de diseño horizontal. Cada enfoque tiene sus méritos." (Principio nº 59).

La noción de web 2.0 es ciertamente interesante para la comprensión de la e-democracia.

Cabe seguir algunos recursos visuales:

(subtitulado) http://www.youtube.com/watch?v=PL-ywltLjzk

En español http://www.youtube.com/watch?v=OwWbvdllHVE&feature=related

3. Conceptos afines: especial atención al "gobierno electrónico" y la actual tendencia hacia la "administración 2.0

Hay diversos conceptos de especial interés y afinidad para la materia abordada.

El concepto de "TICs" desde los años 70 se utiliza para indicar la convergencia que culmina en los años 90 de la electrónica, la informática, las telecomunicaciones. Se hace referencia a aquellas tecnologías que permiten la adquisición, almacenamiento, procesamiento y comunicación de datos en informaciones -textos, voz, imágenes,...etc.- contenidos en señales de naturaleza acústica, electromagnética u ópticas. Aunque no exclusivamente, hoy día internet es emblema de las TICs y concentra toda la atención.

"Sociedad de la Información" "es una fase de desarrollo social caracterizada por la capacidad de sus miembros (ciudadanos, empresas y administración pública) para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera". (Fundación Telefónica, accesible en http://www.telefonica.es/sociedaddelainformacion/espana2000/pdfs/parte1.pdf).

"Sociedad del conocimiento": se alcanza cuando los datos y la información se integren en un marco que permite hacer un uso eficiente y eficaz del gran caudal de los mismos y generar conocimiento "ex novo", lo cual requiere el proceso, análisis, clasificación, reflexión y asimilación de la información, convirtiéndola en acción mediante la toma de decisiones.

Asimismo, procede hacer referencia a algunas definiciones de gobierno o administración electrónica (*egovernment*, indistintamente en inglés). Y es que el mismo concepto viene vinculado a la participación y democracia a través de las TICs.

De entre las diversas definiciones, cabe destacar la que sigue "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. Ministerio Secretaría General de la Presidencia pp 2.

http://hasp.axesnet.com/contenido/documentos/Libro%20Estado%20del%20Arte%20del%20E-Gob%20en%20Chile.pdf

La conexión clara se produce al considerarse el e-gobierno como una evolución, que resumidamente cabe exponer:

1- Acceso y accesibilidad a la información sobre y de la administración.

2- Interacción básica, caracterizada en muy buena medida por la posibilidad de comunicación del administrado con la administración.

3- Interacción avanzada en ambos sentidos administrado-administración, hasta la prestación total de servicios y plena tramitación.

4- Formas de participación y democracia digital.

Según lo dicho, incluso se podría afirmar el continuo lógico de estas nociones:

e-administración → e-gobierno → e-participación → e-democracia

A partir de las nociones web 2.0 y e-gobierno, en la actualidad esta muy en boga la idea de "administración 2.0" o "e-gov 2.0", lanzada por expertos como David Osimo (http://egov20.wordpress.com/). Desde estos movimientos se ha influido en la Declaración Ministerial sobre administración electrónica aprobado por unanimidad en Malmö, Suecia, el 18 de noviembre 2009.
http://ec.europa.eu/information_society/activities/egovernment/conferences/malmo_2009/press/ministerial-declaration-on-egovernment.pdf

Entre otras ideas se insiste en la necesidad de centrar la e-administración en el ciudadano mediante servicios flexibles y personalizados, productos de información basados en la demanda (user-centry); la usabilidad de las aplicaciones de e-administracion, 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. También es esencial a la idea de adminstración 2.0 la transparencia, "Vamos a explorar cómo podemos hacer que nuestros procesos administrativos sean más transparentes" (nº 12) y la apertura y participación "pública a través de métodos más eficaces en todos los niveles del gobierno" (nº 13).

II. Aprehensión jurídica general del fenómeno

1. Ventajas generales de las TICs para la democracia y gobierno

Se pueden alegar una infinidad de ventajas para la implantación de la democracia, la participación y el gobierno electrónicos:

Eficacia: más eficacia en la prestación de servicios públicos, vinculados también a la democracia y participación. Mejor funcionamiento de sistemas electorales, facilidades para mejor ejercicio y funcionamiento de la administración electoral. Facilitación de implantación de mecanismos de acceso a la información y participación en diversos niveles, etc.

Eficiencia: lograr la eficacia a menor coste. Así sucede por ejemplo en procedimientos electorales y administración electoral y, sobre todo, en la facilitación de acceso a la información pública a través de la red, también como canal de participación variada pública o privada.

Transparencia: en principio por una información pública al público más accesible, con diversos niveles de profundidad.

Comodidad, para el ciudadano al que se le añade un canal de información y participación fácilmente disponible desde un punto de acceso informático, generalmente doméstico.

Pluralismo: la pluralidad inherente a la red facilita en principio el mayor pluralismo y que los medios de comunicación clásicos (públicos o privados) , en ocasiones oligárquicos, dejen de constituir un filtro material al libre flujo de información y opinión.

Participación y cultura participativa: las anteriores ventajas, en principio facilitan un aumento de participación por la comodidad de hacerlo para el ciudadano y por la ampliación de posibilidades de llevarlo a cabo.

Inclusión: permite añadir participantes en sectores específicos con tradicionales dificultades (enfermos, discapacitados, emigrantes, desplazados, etc.). Facilita el interés, la información y las posibilidades en algunos sectores sociales así como en territorios con dificultades de acceso y movilidad.

Permite la estructuración de la participación política de los ciudadanos y los grupos en los que se integra: la red permite que colectivos, grupos e individuos se articulen de manera antes desconocida a través de la red, compartan información, deliberen, actúen y participen (asociaciones formales o no, redes ciudadanas, nuevos movimientos sociales temporales o permanentes, etc.).

Facilita la memoria política: la ingente información de la red, su estructuración y permanencia (por ejemplo a través de Google, permite recuperar la memoria política de acontecimientos pasados de trascendencia (afirmaciones de responsables políticos, etc.).

2. La obligación de implantar formas de e-democracia y e-gobierno como principio jurídico-constitucional, concretable por un legislador con voluntad política

Tanto desde la perspectiva de la administración electrónica, como desde una perspectiva más cercana a la democracia y participación electrónicas, ventajas como las anteriormente enunciadas llevan a afirmar que hay un principio jurídico-constitucional objetivo que impulsa a los poderes públicos a adoptar políticas en la dirección de la implantación del gobierno, democracia y participación electrónicas. Así, por ejemplo, todos los documentos resultantes de la Cumbre Mundial sobre la Sociedad de la Información (CMSI, Ginebra, 2003, y Túnez, 2005). En español: http://www.itu.int/wsis/index-es.html

Según las constituciones de cada país, este principio objetivo puede encontrarse, por ejemplo, en los mandatos de eficacia y democracia del gobierno y la administración, de buena administración, de servicio a los ciudadanos, de acceso a la información pública y de transparencia, etc. Asimismo, según lo que concretamente quiera sostenerse este principio objetivo puede considerarse en el marco de la dimensión objetiva de algunos derechos fundamentales, como el derecho al sufragio activo y pasivo, el derecho de participación general, el derecho de petición, el libre acceso a la información (en su caso pública), la libertad de expresión, el derecho de educación, el derecho a la buena administración, derecho de acceso a los registros o archivos, el derecho de audiencia previa a las decisiones y cualquier otra forma jurídica que adquieren derechos subjetivos vinculados al ámbito de la democracia y participación.

En ocasiones, no es descartable que las constituciones y otras normas jurídicas incluyan referencias expresas a las nuevas tecnologías y el deseo de implantación en la administración, poderes públicos y mecanismos participativos. Muchas veces las normas afirman las ventajas de las TICs o formulan derechos que no tienen la estructura de tales, por lo que se hacen difícilmente exigibles o generan sólo obligaciones genéricas para los poderes públicos. No es impensable, sin embargo, que la jurisprudencia futura reconozca exigencias concretas de implantación de democracia y gobierno electrónicos como parte del contenido subjetivo sí directamente exigible de algunos derechos fundamentales.

Ahora bien, el legislador en ocasiones adopta compromisos concretos y exigibles. Como ejemplo en España, el artículo 6 de la Ley 11/2007 sobre e-administración que reconoce un auténtico derecho:

"Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992,

de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos."

Al fin y al cabo, todo depende de la voluntad política, *"la e-democracia prospera mejor donde hay la voluntad política y liderazgo para hacer que funcione con eficacia mediante la introducción de los cambios estructurales necesarios para tener en cuenta las opiniones expresadas. La incorporación de las TIC en los procesos democráticos por lo general requiere cambios estructurales y la reforma procesal." (Recomendación e-democracia 2009, Principio nº 63).*

Por múltiples motivos, es cierto que el Derecho recibe mal y tarde la incuestionable implantación y evolución de las nuevas tecnologías: dinamismo, variabilidad técnica, desconocimiento, costes, necesidad de reposo que exige el Derecho, etc.

No obstante, es posible imponer compromisos y obligaciones concretas a través del Derecho. El ejemplo más llamativo y relevante para la materia de transparencia y democracia electrónicas es el que se produjo tras la quiebra de la empresa norteamericana Enron (http://es.wikipedia.org/wiki/Enron) a principios de la década. Y es que desde entonces se ha producido una ola legislativa por la que se exige una muy elevada transparencia –también a través de internet- y la implantación de mecanismos de participación telemática, a grandes empresas cotizadas en bolsa en favor de la transparencia económica. La crisis financiera de 2008 y el escándalo del caso Madoff (http://es.wikipedia.org/wiki/Bernard_Madoff), a buen seguro supondrá un nuevo impulso a la transparencia financiera. Estas son buen ejemplo de que sí posible exigir jurídicamente obligaciones concretas de transparencia e información pública, que "sólo" habría que trasladar a los distintos poderes públicos. Y es que lo irónico es que por lo general los poderes públicos no se obligan jurídicamente a ellos mismos a facilitar información pública por medios electrónicos ni facilitar la participación y apertura.

III. Acceso a las TICs, brecha digital y su tratamiento jurídico

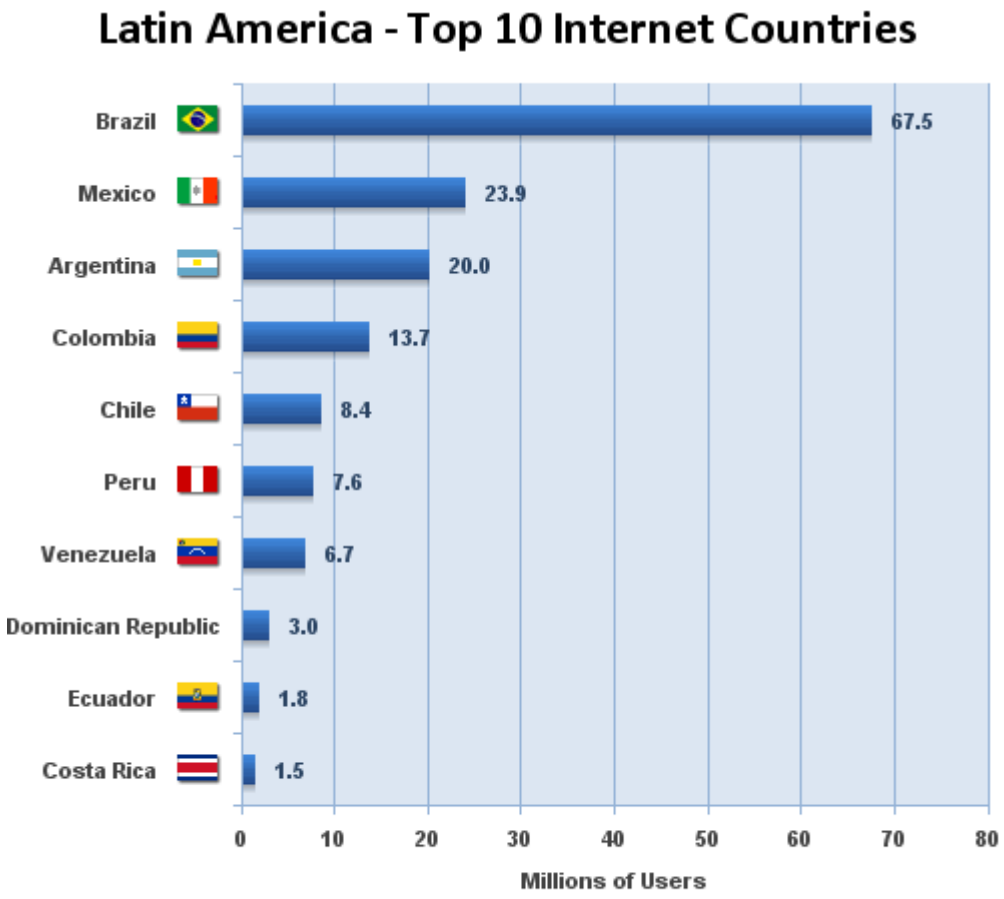
1. Acceso a internet en Latinoamérica y España

Los datos más recientes (diciembre de 2009, http://www.internetworldstats.com/stats.htm) señalan que un 32,1 %

(14,4% en marzo de 2006) de la población de América Latina (sin Caribe) están ya conectados a internet. El total de los internautas mundiales es aproximadamente de mil ochocientos millones. La media de acceso en Europa, según esos datos es de 53 %, la Unión Europea de 27 el 59% y de Norte América 76, 2% (68.6% en 2006).

WORLD INTERNET USAGE AND POPULATION STATISTICS				
World Regions	Population (2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetrat (% Populati
Africa	991,002,342	4,514,400	**86,217,900**	8.7 %
Asia	3,808,070,503	114,304,000	**764,435,900**	20.1 %
Europe	803,850,858	105,096,093	**425,773,571**	53.0 %
Middle East	202,687,005	3,284,800	**58,309,546**	28.8 %
North America	340,831,831	108,096,800	**259,561,000**	76.2 %
Latin America/Caribbean	586,662,468	18,068,919	**186,922,050**	31.9 %

Por países, en América Latina (http://www.internetworldstats.com/stats10.htm#spanish), en febrero 2009 destaca la penetración de internet en Chile 44,9 % (35.7% en 2006) o Argentina 39,3% (26.4% en 2006). Por orden de penetración de internet: Chile 44.9 %; Argentina 39.3 %; Costa Rica 35.7 % (22.7% en 2006); Uruguay 31.6 %(20.8% en 2006); Colombia 30.5 %(9.7% en 2006); Peru 26.2 % (16% en 2006); Brazil 26.1 %(14.1% en 2006); Puerto Rico 25.3 %; Venezuela 22.5 %(12% en 2006); Dominican Republic 22.1 %; Mexico 21.6 % (16.2% en 2006); Guatemala 10.2 %; El Salvador 9.9 %; Ecuador 8.0 %(5.2% en 2006); Panama 8.0 %; Bolivia 6.3 %(3.8% en 2006); Honduras 4.5 % (3.3% en 2006); Paraguay 3.8 % (2.7% en 2006; Nicaragua 2.7 %(Nicaragua 2.2% en 2006) y finalmente en la cola, Cuba con un 2.1 %.



Source: Internet World Stats - www.internetworldstats.com
162,466,535 estimated Internet Users in Latin America for Dec. 2008
Copyright © 2009, Miniwatts Marketing Group

En España, los conectados a internet son el 63,3% (38.7% en 2006), ocupando un lugar medio en la Unión Europea ampliada a 27 (59 %) frente a países como Holanda (90%) o Noruega (87,7%). Ahora bien, España se sitúa bastante por encima de la media latinoamericana. En diciembre de 2009 el grado de penetracion es del 71, 8 % en España.

Sin perjuicio de que los datos de Latinoamérica puedan llevar a relativizar la cuestión que aquí se afronta, debe tenerse en cuenta un significativo crecimiento. Así, para Latinoamérica es especialmente llamativo el índice de crecimiento de 2000-2005, el segundo en el mundo al multiplicarse el uso de la red en 3.42 veces. En el periodo 2000-2008, el crecimiento de la zona ha sido de 8,2 veces.

Ahora bien, debe tenerse en cuenta que se trata de datos de acceso a internet, sin que pueda considerarse que los usuarios conectados sean capaces de hacer un uso funcional y eficaz de la red, como el que requieren en los más de los casos las diversas formas de participación y democracia electrónica.

También, a falta de datos concretos para Latinoamérica, debe tenerse en cuenta que los estudios generales muestran cómo los

accesos –y más los usos eficaces de internet- se dan entre los sectores medios y altos de la población, más entre hombres que entre mujeres, más entre jóvenes que mayores, más en zonas urbanas que en zonas rurales. Como se ha adelantado, el uso algo avanzado es capital para la web social participativa o web 2. 0.

Hoy por hoy la red reproduce, incluso intensifica las pautas de marginalidad social no virtuales. Y no cabe duda de que se trata de un factor nada despreciable cuando se trata de la democracia y participación electrónicas.

2. Brecha digital y elitocracia electrónica

Por lo expuesto, un peligro de obligatoria advertencia y atención jurídica es el de una dualización (conectados/desconectados), la llamada "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 y necesitados de representación de intereses y de conformación de interés general sobre la base de sus necesidades 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. Ello conduciría, como diversos autores han alertado a una democracia de elites.

Desde el punto de vista jurídico, el tratamiento puede venir dado desde el principio de igualdad y los derechos fundamentales (y su dimensión institucional y prestacional).

a) No discriminación en la implantación del gobierno y democracia electrónicas

Desde la igualdad, debe garantizarse que la implantación de servicios electrónicos 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 esto discriminatorio por sí 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.

En este punto, las acciones presuntamente discriminatorias se dan cuando no se duplican las ventajas de la red en el mundo no virtual y,

sobre todo, la discriminaciones pueden provenir de la imposición de interactuar sólo electrónicamente. Como ejemplo, el artículo 27. 6º de la ya referida Ley 11/2007 española sobre 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."

Estas medidas deben ir acompañadas de garantías de acceso a todos a las TICs (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 los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada."

Según lo visto, basta un reglamento para imponer la obligación de relacionarse electrónicamente con la Administración. Por ejemplo, millones de pequeñas empresas o empresarios autónomos, o comunidades de propietarios quedan obligados a ser notificados electrónicamente de, por ejemplo, las multas de tráfico o comunicaciones con Hacienda, respectivamente.

No obstante, no puede ser automático considerar discriminatoria esta imposición de relacionarse electrónicamente. Esta evaluación jurídica debe hacerse sobre todo desde los parámetros del derecho a la igualdad, reforzada jurídicamente su garantía en conexión con el derecho o libertad de que se trate (derecho de sufragio, general de participación, derecho de acceso a la información pública, derecho de petición, etc.). Pueden tenerse en cuenta especialmente dos elementos, uno formal y otro material:

-garantías formales: facilita la admisibilidad de la imposición de la interactuación electrónica que ésta venga fijada en ley formal, sin perjuicio de que luego remita al desarrollo reglamentario. Mayor legitimidad contará en cuanto la regulación legal concrete en mayor medida las condiciones para que sea obligatoria la interactuación electrónica y fije los espacios que debe concretar una norma inferior. Así, la norma legal puede fijar pautas a la norma inferior de quién, cuándo, cómo y porqué puede exigirse la interactuación electrónica.

-garantías materiales: las normas que fijen la interactuación obligatoria, deberían determinar con una certeza mínima el colectivo de personas u organizaciones a los que se obliga a la interactuación electrónica. El acierto y certeza en su fijación pueden ser un criterio determinante para la admisión de la medida desde las pautas de

razonabilidad. Asimismo, deben contener previsiones para evitar posibles situaciones y dificultades concretas, como la garantía de acceso a puntos de internet, garantías técnicas frente a caídas del servicio, asistencia técnica, etc.

b) Las políticas de acceso a internet y alfabetización digital. ¿Un derecho fundamental al acceso a la sociedad del la información?

En todos los sistemas constitucionales no faltan anclajes jurídico-constitucionales para apoyar jurídicamente todas las políticas conducentes a facilitar la sociedad de la información y del conocimiento, la alfabetización digital y el acceso a internet por la ciudadanía: afirmación de la igualdad material, derecho a la educación y dimensión objetiva y prestacional de los derechos fundamentales, en especial, derechos de información y comunicación, etc.

Cada vez tiene más acogida la afirmación de un derecho a la comunicación (*ius comunicationis, los"Communication Rights*) de naturaleza constitucional o casi-constitucional. El artículo 19 de la Declaración Universal de Derechos Humanos que en su artículo 19 se afirma que: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión." Este artículo, con sus sesenta años a la espalda puede –y debe- interpretarse en clave de la sociedad de la información. Así lo hace Naciones Unidas en la *Declaración de Ginebra*, 2003 y la *Declaración de Principios* Túnez en Noviembre de 2005 (http://www.itu.int/wsis/index-es.html). Sin valor jurídico son referentes donde se afirma el "derecho de acceso como acceso universal".

En España el *ius comunicationis* ha tenido clara acogida en algunos Estatutos de autonomía (máxima norma institucional de las regiones). Así, destaca 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."* Se trata de muestras o expresiones del alcance de este nuevo derecho, pero más como principios que como derechos subjetivos exigibles. De hecho, éstas y otras proclamaciones tienen singular valor jurídico en sentido negativo, pues valen especialmente como apoyo jurídico para la adopción de medidas de implantación de políticas de universalización del acceso a internet, de extensión territorial o social de servicios, etc.

Sin embargo, es bastante discutible que se generen derechos subjetivos para los particulares de que el Estado les garantice acceder a la red, recibir formación digital, etc. Cuestión diferente, como se verá, es la del derecho fundamental en juego ante medidas que suponen la restricción del acceso a la red, en las que sin duda está en juego la libertad de expresión e información como derecho subjetivo.

IV. Cautelas respecto de la democracia y participación electrónicas

92. Ya se ha insistido en los peligros de una elitocracia en internet y de la discriminación política. También, brevemente, cabe tener en cuenta algunas cautelas que pueden tener su traslación jurídica.

1. Necesidad de control político y fiscal de políticas de la sociedad de la información

Es general el desconocimiento y falta de práctica en estas materias, especialmente entre los tradicionales responsables del control político, parlamentario, administrativo y contable de los poderes públicos. En la implantación del gobierno, democracia y participación electrónicas se amplían diversas posibilidades de corrupción en los diversos niveles de los poderes públicos y el conglomerado de empresas e intereses privados que son los que habitualmente *tejen* la red e implantan los servicios públicos de gobierno y democracia electrónicas. Aun sin malicia, la combinación de ignorancia y fascinación por lo moderno llevan a un muy ineficiente gasto en la implantación de medidas de e-democracia.

2. Peligro de sobre representación al ciudadano que participa a través de internet

En todo proceso participativo, el perfil más activo de los participantes suele corresponder con las posiciones más polarizadas. Dotar a su participación de especial significación puede suponer infravalorar las posiciones mayoritarias y más moderadas. A la vista de diversas experiencias en la red, esta cautela adquiere especial importancia. En conexión con lo anterior, no debe descuidarse el particular perfil que pueden tener los usuarios de las nuevas tecnologías más participativos, puesto que es más que posible que en modo alguno reproduzca transversalmente el perfil del cuerpo social.

La atribución de una sobre representación al activista por medio de las TICs vendría a ser como atribuir una mayor significación política a los mensajes políticos que suelen decorar el entorno urbano, por lo general nada moderados. En este punto, no está demás recordar el

fenómeno de los *frikis* de internet o *geeks*, usuales participantes de la web 2.0 http://es.wikipedia.org/wiki/Geek. Eso sí, con la penetración incesante de internet, los usuarios avanzados en España, participantes de la web social son no menos de un tercio, unos ocho o diez millones de personas que ya no responden a perfiles muy caracterizados.

3. Fraccionamiento social

Autores importantes como Sunstein alertan del fraccionamiento social que puede provocar internet, donde los individuos y los colectivos en los que se integra se retroalimentan continuamente, desconectándose de otros fenómenos y preocupaciones sociales y radicalizando sus posiciones endogámicas. Por esta vía, desaparece no sólo la idea del foro público, sino que acaba prevaleciendo una idea de democracia como mera agregación de intereses. Aunque no tanto en el momento de formulación de esta teoria, esta tesis puede ir confirmándose en el futuro.

4. La seguridad y el peligro del "gran hermano". La especial protección jurídica de los ciudadanos que participan a través de la red y la garantía de su anonimato y protección de datos

Los primeros años de éxito de la red se generó un espíritu libertario en internet que ha marcado su historia, como tiene reflejo en la conocida Declaración de Independencia del Ciberspacio (http://www.internautas.org/documentos/decla_inde.htm). Bajo este espíritu libertario, anárquico, se transmitió –incluso por los Tribunales de los EEUU- que internet, esta conversación mundial sin fin, no era controlable ni regulable y que esta falta de regulación había sido uno de los secretos de su éxito. Lejos de todo idealismo propio de los inicios de internet, la red es un espacio mucho más controlable que el mundo real, como especialmente Lessig demostró

http://www.uned.es/ntedu/espanol/master/segundo/modulos/audiencias-y-nuevos-medios/ciberesp.htm

Se puede afirmar que pasamos de un internet más liberal y autoregulado a un internet más regulado. Un buen ejemplo de esta última tendencia puede ser la Directiva 2006/24/CE, de 15 de marzo de 2006 de retención de los datos de tráfico o la creciente proyección de la legislación de protección de datos en internet en toda su extensión.

Los peligros potenciales son infinitos. A las infinitas fórmulas de tratamiento de datos personales, debe añadirse que las herramientas de

minería de datos (*data mining)*[1] e inteligencia artificial permiten esta gestión del conocimiento de ingentes cantidades de información de forma automatizada. Son muchos los interesados en botín (gobierno, partidos políticos, grupos de poder, etc.). Se trata de una excelente *materia prima* ideológica para la elaboración de perfiles, para la selección de objetivos de ataques[2] y coacciones –informáticos o no- o, en sentido positivo, para fijar el objetivo de campañas, etc. Cabe pensar en el peligro de acceder al listado de miles de personas que suscriban electrónicamente una iniciativa popular sobre un tema político significado. Se han afirmado supuestos de este tipo, por ejemplo, en Venezuela o España[3].

La identidad del participante es una garantía de responsabilidad jurídica y política exigible -voto secreto- y en otros muchos casos y posibles diseños de mecanismos participativos, el anonimato puede ser una precondición de un debate y deliberación libres a través de la red. No hay una respuesta unívoca.

---

[1] Siguiendo la voz en *wikipedia*: " se engloban un conjunto de técnicas encaminadas a la extracción de "conocimiento" procesable implícito en las bases de datos de las empresas. Las bases de la minería de datos se encuentran en la inteligencia artificial y en el análisis estadístico. Mediante los modelos extraídos utilizando técnicas de minería de datos se aborda la solución a problemas de predicción, clasificación y segmentación".

[2] Baste mencionar una noticia cercana, "ETA cruza los datos del censo, el registro mercantil y el padrón para intimidar más a los empresarios", en *Heraldo.es*, 24 de junio de 2007.

[3] Así, siguiendo diversos artículos de prensa (entre otros, El Mundo, 20 de octubre de 2006), cabe relatar dos casos:

1. Los datos de los ciudadanos venezolanos que solicitaron activar el referéndum revocatorio de agosto de 2004 contra el Presidente Hugo Chávez, rellenando unas plantillas del Consejo Nacional Electoral han sido objeto de tratamiento por un programa informático *Maisanta* que genera una ficha individual de cada ciudadano en la que constan datos como "abstencionista" o "si firmó contra el Presidente". Ante la Comisión Interamericana de Derechos Humanos se han denunciado prácticas de persecución política a los ciudadanos incluidos en "listas negras" –denominadas *listas Tascón*- elaboradas, al parecer, sobre la base de los datos de quienes solicitaron la activación del referéndum revocatorio.

2. Un ciudadano votó afirmativamente en un referéndum electrónico sobre los matrimonios homosexuales organizado por la Universidad Complutense de Madrid (España) en el marco de un proyecto de investigación. Desde entonces recibe continuamente mensajes de spam en los que se le insta a someterse a tratamiento, a cambiar de actitud y a apoyar la defensa del matrimonio tradicional. Los mensajes provienen de la asociación norteamericana que proporcionó gratis a los investigadores el software necesario para realizar el e-referéndum. El asunto está siendo investigado por la Universidad y por la Agencia Española de Protección de Datos.

a) Anonimato en la participación política en la red como garantía de la libertad de expresión

Se habla de un derecho al anonimato en internet, pero éste tiene una difícil construcción jurídica a partir de la concurrencia de varios derechos fundamentales: la libertad de expresión e información, del derecho y garantías al secreto de las comunicaciones y el derecho fundamental de protección de datos (expresamente reconocido en algunos casos, en otros casos considerado integrado en el derecho a la intimidad, la vida privada o el libre desarrollo de la personalidad).

Antes de internet, en Estados Unidos sí que se ha llegado a considerar en alguna sentencia que el anonimato está incluido en la libertad de expresión (por ejemplo, Tribunal Supremo federal norteamericano en 1960, *Talley* v. California). Más recientemente, en *McIntyre* v. *Ohio Elections Comm'n* (1995), el Tribunal Supremo Federal afirmó la necesidad de aplicar el escrutinio más restrictivo para la limitación de la libertad de expresión, y la necesidad de argumentar un general interés público para levantar el anonimato en las opiniones políticas manifestadas durante los procesos electorales o referéndums.

Al igual que se ha dicho que el anonimato es derecho al voto secreto en el caso de voto electrónico, en algunos casos, el anonimato puede considerarse que forma parte del secreto del periodista y su derecho a no revelar las fuentes. Se trata de una cuestión muy discutible en la medida en la que ser "periodista" en internet lo puede ser cualquiera y se duda si este derecho debe ser reservado a los profesionales. En EEUU ya se ha considerado que este clásico "privilegio" de los periodistas puede disfrutarlo cualquier periodista no profesional en la red, prácticamente cualquier persona. Así en sentencia de marzo de 2005 en Santa Clara –*caso Dan Gillmore*- (afirmado aún más claramente por la Corte Estatal de Apelaciones de San José en mayo de 2006) y en caso John Doe nº1 v. Cahill, de octubre de 2005, en Delaware.

Obvio es decir que en unos y otros casos, este anonimato y confidencialidad, pese a considerarse parte de un derecho fundamental, puede estar sometido a límites y justificaciones objetivas, razonables y proporcionales a las finalidades como persecución de delitos, ofensas al honor, intimidad y propia imagen, protección de menores, jóvenes, etc. Sin perjuicio de ello, cuando se vincula a la democracia y la participación electrónicas, debe considerarse más intensa su protección jurídica.

En el marco del Consejo de Europa, algún documento sin valor jurídico ha conectado expresamente el anonimato con la libertad de comunicación en internet. Así la Recomendación nº R(99)5 del Comité de Ministros de los Estados miembros del Consejo de Europa sobre la

protección de la intimidad en Internet se afirma "la necesidad de desarrollar técnicas que garanticen el anonimato de las personas afectadas y de la confidencialidad de la información intercambiada a través de las "autopistas de la información", en el respeto de los derechos y libertades de los demás y de los valores de una sociedad democrática". Más recientemente, la Declaración del Comité de Ministros del Consejo de Europa, de 28 de mayo de 2003, sobre la libertad de comunicación en Internet, Principio 7: Anonimato.

La tendencia en Europa parece ser la de la restricción del anonimato bajo la excusa del control del acceso de los menores a las redes sociales. Sin perjuicio del interés del menor, debe tenerse en cuenta el efecto amenazante e inhibitorio para cualquier usuario que libremente se expresa y se informa hoy día en la red al saber que de un modo u otro va a poder monitorizarse lo que hace.

b) Anonimato, privacidad y sus garantías

A pesar de las citadas resoluciones, la protección en Europa del anonimato en la red se canaliza por medio de los derechos fundamentales a la vida privada, secreto de comunicaciones y protección de datos. No es lugar éste de llevar un mayor análisis sobre estos conocidos derechos fundamentales, baste decir que jurídicamente su protección debe intensificarse cuando queden conectados al ejercicio de derechos de participación política. En especial, deben guardarse especiales cautelas con los datos personales unidos a expresiones políticas, por el peligro para los participantes que pueda comportar su tratamiento por autoridades, por partidos o por sujetos privados. A este respecto, las penas y sanciones pueden ser terribles, y de ellas no escapan ni los periodistas. Así, la polémica sentencia 531/2009, de 18 de diciembre de 2009, Juzgado de lo Penal Nº 16 de Madrid, que condena a un año y nueve meses de prisión, seis meses de multa e inhabilitación para la dirección de medios de comunicación y el periodismo al director y subdirector de la Cadena Ser (la de más audiencia en España) por revelación ilegítima de datos personales de ideología política. Como prueba de irregularidades en la afiliación en un municipio, se divulgaron en una web del grupo datos de setenta y ocho (78) afiliados sin consentimiento.

V. Administración electoral y TICs, las TICs en las campañas electorales

1. Administración electoral y la creciente emergencia de las TICs en campaña

El empleo de las TICs es una realidad en cualquier sector, y también en la organización y procedimiento electorales. En el ámbito de las actuaciones de administraciones electorales son diversas los reflejos de las TICs. Así, es posible la comprobación electrónica de la corrección del censo por los ciudadanos electrónicamente.

https://censoelectoral.ine.es/censo/ce_internet1_noelectoral.menu

En diversos países de América Latina el uso de censos electorales electrónicos añade algunas funcionalidades. Resultan a mi juicio peligrosas las funcionalidades que añaden automáticamente en el censo electoral los registros de si el ciudadano ha votado a cada comicio, incluso en tiempo real el día de las elecciones. Ello tiene ventajas en la depuracion y actualización del censo o padrón. Sin embargo, el conocimiento automatizado del comportamiento electoral del electorado permite un peligroso y abusivo control por gobiernos, partidos y cantidatos. Ello facilita, por ejemplo, tratamientos específicos por candidatos o partidos de los votantes según su carácter mas o menos abstencionista.

De otro lado, se ha señalado con acierto que las administraciones electorales van a tener que añadir en su composición a técnicos en TICs que garanticen, vigilen, resuelvan -y expliquen a los miembros no técnicos- las nuevas cuestiones relativas al voto electrónico, *software* empleado, etc.

No procede ahora recordar todas las posibilidades que la red permite para la difusión de información, la deliberación, la movilización de recursos económicos, personales y emocionales entre la población, en especial, la población internauta. Se dice, con diversa fundamentación sociológica y politológica, que los *blogs* (a modo de páginas web personales) en EEUU marcaron la agenda política durante el último semestre de las elecciones Bush vs. Kerry en 2004 y, finalmente, decidieron la victoria, gracias al predominio republicano en la red, superando la incidencia de los medios de comunicación clásicos. En las elecciones presidenciales EEUU de 2008, la fuerte presencia de Obama en las reces sociales, con centenares de miles de “amigos” en *Facebook* por ejemplo, fue un elemento más para su victoria[4].

Al respecto, http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

[4] A texto completo, puede seguirse http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

Aunque pueda sorprender, los elementos básicos del uso de la red en campaña electoral ya los empleó un personaje como Jesse Ventura (ex lucha libre y sustentador de numerosas teorías de la conspiración) para lograr el puesto de Gobernador de Minessota en 1998 sin ser de partido mayoritario alguno. Recientemente, movimientos sociales en la red han desembocado, por ejemplo, en el "Tea Party" (http://en.wikipedia.org/wiki/Tea_Party_movement), con logros como arrebatar para el Partido Republicano un senador en Boston, lo que no se lograba en 50 años.

2. Novedades en internet por cuanto a típicas prohibiciones previas a los comicios electorales

Como es de sentido común, "las limitaciones establecidas por la legislación electoral son también aplicables al uso de este tipo de medios electrónicos" (Exposición de Motivos Instrucción 4/2007, de 12 de abril, de la Junta Electoral Central).

http://www.juntaelectoralcentral.es/portal/page/portal/JuntaElectoralCentral/JuntaElectoralCentral/DocJEC/Instrucciones/12042007

a) Internet y jornada de reflexión electoral:

Es típico en muchos países la existencia de un periodo de prohibición de la solicitud del voto. Esta prohibición en general debe trasladarse a internet, así como las posibles sanciones por su incumplimiento.

Ahora bien, debería en todo caso tenerse en cuenta la necesidad de adecuar y flexibilizar criterios para juzgar su posible incumplimiento en internet. Por lo general, debe seguir prohibiéndose cualquier fórmula activa de promoción del voto en internet, no requerida por el usuario (por ejemplo mensajes emergentes, correos electrónicos). También, debe considerarse prohibida la publicidad en medios clásicos de comunicación en internet que se actualizan frecuentemente (por ejemplo, un periódico en internet). Por el contrario, la prohibición debe relativizarse y flexibilizarse para modos de comunicación en internet que siguen accesibles el día de la prohibición, en los que retirar los contenidos prohibidos exigiría importantes esfuerzos para su eliminación (foros, webs de partidos pequeños sin medios, páginas personales de partidarios de un sentido del voto, etc.).

En este punto, debe tenerse en cuenta la actividad positiva del internauta que voluntariamente accede a estos sitios.

b) Prohibición de encuestas y sondeos

Se suscitan problemas fácticos también por cuanto a la prohibición de realización y publicación de encuestas y sondeos electorales durante un periodo previo a la elección, algo común en diversos países. Dicha obligación es fácilmente eludida cuando la información prohibida se ubica en medios de comunicación no sometidos a la legislación –o a la acción- del país de que se trate. El ciudadano internauta del territorio donde rige la prohibición puede fácilmente acceder a tales contenidos prohibidos, lo cual es difícilmente evitable, e incluso resultaría desproporcionada la mera amenaza al usuario de que su acción es ilícita. Por ejemplo, en las elecciones generales de 2008 en España, la semana de prohibición de difusión de sondeos, algunos periodicos online incluyeron un enlace en su portada en la red hacia sondeos publicados por medios situados en Andorra (muy pequeño país fronterizo con España), por ejemplo. La prohibición española, obviamente, no alcanzaba a aquel país.

VI. Voto electrónico: tipos y garantías

1. Voto electrónico y su tipología: una importante distinción

La informatización del proceso electoral no es en modo alguno nueva. No en vano la concentración de resultados se realiza normalmente de forma electrónica, si bien, el rastro en papel se conserva para verificar datos y efectuar los oportunos recuentos. Aquí se analiza especialmente la introducción de dispositivos electrónicos en el momento en el que ciudadano emite su voto. Y hay que añadir que el uso de máquinas para la votación tampoco es nuevo, se remonta a fines del siglo XIX en EEUU. Máquinas de votación por palanca o con perforadores no son nuevas. Lo nuevo, y en ello se centra el análisis del e-voto estriba en la desmaterialización física del voto que hace difícil o imposible comprobar los resultados sobre la base del voto emitido puesto que los votos quedan guardados en soporte electrónico y el elector no puede comprobar por sí mismo la corrección de la votación.

En este punto, por ejemplo, cabe señalar las papeletas electrónicas recientemente introducidas en España, las mismas facilitan el escrutinio, pero el soporte sobre el que se basa el escrutinio sigue siendo el papel, no la información electrónica. Se trata del escrutinio electrónico *e-counting*, pero no del voto electrónico. A diferencia de este supuesto son los casos en los que aun siguiendo un posible rastro en papel (a efectos de detectar discrepancias o dejar resguardos para el votante, el resultado de la votación proviene de la información electrónica.


ANEXO

Especificaciones:

Tamaño aproximado 105 x 310 mm. En todo caso adecuado al número de candidatos y suplentes.

Gramaje aproximado 70 g/m².

Papel blanco en cualquier tonalidad, impreso en tinta negra.

Los tipos de letra deberán ser idénticos para cada candidato.

Impresión por una sola cara.

El tipo de fuente a utilizar para la confección del código de barras será "C39HrP24DhTt", con un paso de 28 pt. e incrementando el cuerpo un 20% verticalmente para facilitar la lectura.

El código de barras constará de dos cuerpos, el primero referenciará al proceso electoral correspondiente y el segundo identificará a la candidatura. Ambos irán separados por un guión, no admitiéndose espacios. Tanto el carácter de inicio como el de fin del código será, obligatoriamente, un asterisco.

EP5A.1

ELECCIONES AL PARLAMENTO EUROPEO 2009
DIPUTADOS

Doy mi voto a la candidatura presentada por:
CANDIDATURA Nº 1
(SIGLA-CAND Nº 1)
(Símbolo)
PE2009-001

Suplentes

Imagen: ejemplo de modelo de papeleta, con código electrónico

Una vez centrada la noción de voto electrónico, es especialmente necesaria una precisión conceptual sobre el voto electrónico y su tipología. Tales distinciones tienen una también muy diversa en el sistema político y en su tratamiento jurídico-constitucional.

a) Voto electrónico local en entornos sí controlados

Se trata del uso de medios electrónicos de votación en entornos controlados oficialmente, como los colegios tradicionales de votación o, en general, en cualquier otro lugar que cuente con suficiente

supervisión a cargo de la administración organizadora. Así, se hace referencia al voto a través de papeletas ópticas (sus datos son grabados por un lector óptico, por ejemplo, códigos de barras). De igual modo, el voto en urnas que son ordenadores: se vota con botones, lápiz óptico o la misma mano. El voto queda registrado en el ordenador, implica la supresión de las papeletas tradicionales como medio de votación, aunque es posible que estas máquinas emitan un comprobante en papel.

Así las cosas, vemos que es muy posible hacer referencia al "voto electrónico" a supuestos en los que poco o nada cambia el sistema electoral al exigirse unas fuertes medidas de control sobre el proceso y, sobre todo, no se trata de voto telemático que permita al votante no acudir al lugar controlado.

Estas modalidades están muy generalizadas precisamente en diversos países de Latinoamérica, como Brasil. En dicho país se ha ido extendiendo en los últimos veinte años, al punto de alcanzar el 100% de las votaciones y regularse como excepcional y subsidiario el voto no electrónico (art. 59 Ley nº 9504, de 30 de septiembre de 1997). En Venezuela comenzó a emplearse en 1998 (a partir del impulso de la Ley Orgánica del sufragio y participación política, de 13 de diciembre de 1997) y se generalizó su uso en el refrendo revocatorio de 2004. Por lo general se extiende la modalidad llamada "RED" (Registro Electrónico Directo, *Direct Recording Electronic*): el voto se registra directamente en la memoria de la urna electrónica (esta modalidad se prevé en Perú, República Dominicana, Panamá y Colombia).

Entre las modalidades, cabe señalar el voto por computadora, con al menos un dispositivo para elegir la candidatura y otro para emitir el voto. Se necesita la conexión entre la mesa electoral y el votante tanto para asistirle como para evitar fraudes de este último. Como recuerda Barrat:

"las máquinas holandesas *Nedap* incorporan, por ejemplo, dispositivos sonoros y, en México, el *Instituto Electoral del Distrito Federal* (IEDF) ha desarrollado un máquina de votación que solo puede activarse apretando un botón que se encuentra a disposición de la Mesa electoral y está conectado con un cable con la propia máquina. *Indra*, por último, utiliza tarjetas anónimas que se proporcionann al elector una vez que se ha identificado, en Coahuila (México) se proporcionan con objetivos similares recibos con código de barras y *Scytl* facilita a los electores código alfanuméricos que deben introducir en la pantalla de votación."

Por cuanto al método de elección de candidaturas, hay sistemas como Venezuela en el que el lector ve una papeleta –en papel- como la tradicional, sobre un un dispositivo electrónico sensible al tacto y capaz

de transmitir estos impulsos a la urna propiamente dicha. La máquina recibe la opción y el elector confirma que ésa era la opción deseada.

b) Voto electrónico telemático, "pyjama voting" a distancia en entornos no controlados

El voto electrónico en entornos controlados, no a distancia guarda escasas diferencias con el voto no electrónico y poco o nada altera sistema político, sólo facilita el proceso electoral. Está claro que la potencialidad de las TICs respecto del e-voto lo es por cuanto el voto a distancia, telemático, desde cualquier lugar.

El voto telemático electrónico es habitual en ámbitos no reglados, como votaciones a concursos de televisión a través de mensajes por teléfono móvil. Incluso algunas actuaciones administrativas pueden realizarse también expresando el consentimiento por vía de mensajes SMS desde celulares. Se trata de actuaciones de mayor o menor relevancia social o administrativa, pero que en modo alguno exigen las garantías políticas y jurídicas de un sufragio electoral.

De igual modo, el voto telemático electrónico en entornos no reglados ya es una realidad en el mundo empresarial, donde las garantías no se requieren con la intensidad que en el ámbito electoral general de la política pública. Incluso en algunos casos, normativas de transparencia para el mundo empresarial y societario exigen su implantación. Por el contrario, esto no sucede cuando se trata del derecho de voto político.

El voto telemático electrónico es habitual en ámbitos no reglados, como votaciones a concursos de televisión a través de mensajes por teléfono móvil. Incluso algunas actuaciones administrativas pueden realizarse también expresando el consentimiento por vía de mensajes SMS desde celulares. Se trata de actuaciones de mayor o menor relevancia social o administrativa, pero que en modo alguno exigen las garantías políticas y jurídicas de un sufragio electoral. De igual modo, el voto telemático electrónico en entornos no reglados ya es una realidad en el mundo de las sociedades anónimas , donde las garantías no se requieren con la intensidad que en el ámbito electoral general de la política pública. Algunos países ya lo regulan como algo a implantar en el futuro (como Colombia, Ley 892 de 2004, para ciudadanos en el extranjero) o se detectan proposiciones de ley, como recientemente Francia para ciudadanos en el extranjero (Ley modifica la Ley orgánica nº 76-97 de 1976, 31 de enero sobre el voto de los franceses residentes en el extranjero para las elecciones del Presidente de la República). Lo más llamativo en todo caso es la puesta en práctica real de este sistema en Ginebra en 2004 , un lugar donde un 90% de los ciudadanos ya ejercía el voto por correo –sin garantías de certificado- y que se habilita

el voto telemático con iguales garantías que el voto por correo. Asimismo, y de mayor relevancia, resulta el caso de Estonia, después de las elecciones locales de 2005, en marzo de 2007 y para elecciones parlamentarias un 3% de los ciudadanos votaron a través de un portal habilitado al efecto. Requerían su documento de identidad, la firma electrónica y un contraseña en un ordenador dotado de un lector electrónico de tales elementos . La clave: el avanzado estado letón en la implantación de la administración electrónica y la plena confianza en el sistema, pese a que las garantías reales hoy por hoy son muy discutibles.

Ahora bien, hoy por hoy, todo parece indicar que las tecnologías no permiten el mismo aunando las garantías exigibles en un proceso electoral democrático. Así, el proceso más ambicioso de voto a distancia, telemático –no sólo electrónico- fue un rotundo fiasco (*Secure Electronic Registration and Voting Experiment* (SERVE), promovido por el Gobierno de Estados Unidos para quienes estuvieran fuera del país, como militares. Por ello, hoy día se sigue prefiriendo el voto postal por las garantías que presenta. En todo caso, las experiencias son continuas en diversos países y no se sabe lo que el futuro ha de deparar.

2. Las garantías constitucionales del voto electrónico: los "principios" del Consejo de Europa

Son diversas las normas que regulan las posibilidades y garantías del voto electrónico, casi siempre, con exclusiva referencia al voto local en entornos controlados, no a distancia o telemático. Sobre la proyección de las garantías constitucionales tradicionales, ínsitas en el mismo contenido del derecho al sufragio activo o pasivo, parece conveniente remitirse a la Recomendación del (2004)11 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre los estándares jurídicos, operativos y técnicos del voto electrónico. Adoptada por el Comité de Ministros del 30 de septiembre de 2004 en su 898ª reunión (original, https://wcd.coe.int/ViewDoc.jsp?id=778189, en castellano en los materiales del curso)

Esta Recomendación, sin exigibilidad jurídica, expresa las normas mínimas que debe contener la regulación de los estados miembros sobre voto electrónico. Se considera que siguiendo sus llamados "principios" y sus "normas de procedimiento" se garantizan los requerimientos democráticos y de los derechos fundamentales. La Recomendación aunque está pensada para el voto electrónico local –el actual-, no excluye su aplicabilidad para el voto a distancia, que reúna las garantías que exige.

La citada resolución recoge como “principios” diversas garantías de estas exigencias ineludibles consagradas en los estados democráticos.

Garantía de voto universal

Se afirman cuatro exigencias:

1º Que el sistema utilizado sea comprensible y fácilmente utilizable por el mayor número de personas posible.

2º Sencillez en el procedimiento para inscribirse y utilizar el sistema de voto electrónico, que no sea una barrera.

3º Que el sistema maximice las posibilidades para los discapacitados.

4º Que mientras no sea universalmente accesible, el e-voto sólo sea un sistema añadido y complementario.

Garantía de voto igual

Se afirman cuatro directrices:

-que se garantice que sólo sea posible un sólo voto electrónico por el elector

- Seguridad de no duplicidad de voto virtual y no virtual.

-Garantía de que el voto se contabilice sólo una vez.

- Que los mecanismos de recuento permitan fácilmente compatibilizar votos electrónico y no electrónico.

Garantía de sufragio libre

- Garantía de identidad (persona real y viva, datos biométricos).

- Garantía de no coacción (en particular para voto a distancia).

- Que la votación electrónica no induzca a un voto concreto, irreflexivo, precipitado o desviado.

- Que sea posible modificación del sentido del voto durante el proceso, sin necesidad de asistencia de un tercero, hasta conclusión del procedimiento de e-voto.

- Posibilidad de no mostrar preferencias, voto en blanco exista también electrónica

- Que el sistema indique con claridad la culminación del proceso con éxito. Mensaje de confirmación y terminación del procedimiento.

- El sistema debe imposibilitar cualquier modificación del sufragio.

Garantía de voto secreto

La garantía del secreto es relativamente sencilla de garantizar en el voto tradicional y en el electrónico local, dada la separación física entre la identificación del votante y la papeleta o el voto electrónico en la urna local (aunque sea electrónica). Por el contrario el secreto es más difícil en el voto a distancia, puesto que debe saberse quién vota (en especial cuando el sufragio es obligatorio), pero no debe saberse su voto. Obviamente es necesario adoptar medidas para que las informaciones requeridas en el tratamiento electrónico no puedan ser utilizadas para violar el secreto del voto.

3. Las "Reglas de procedimiento" del Consejo de Europa

En la Recomendación europea se contienen también un segundo grupo de reglas, relativas a garantías del procedimiento, sobre transparencia (primero), verificación y responsabilidad (segundo) y fiabilidad y seguridad (tercero).

Transparencia

Respecto de la transparencia se exige adoptar siempre medidas para la confianza y comprensión del sistema. Se recomienda que sea posible practicar previamente al voto definitivo. También se exigen medidas que permitan al ciudadano observar el procedimiento electoral electrónico. En este punto se fijan garantías como el conocimiento del programa utilizado –*software*-, medidas físicas y electrónicas de seguridad. En todo caso, la posibilidad de observación debe evitar la posibilidad de manipulación.

Verificación y responsabilidad

Se trata de las cuestiones más discutidas. Se recomienda la divulgación de los componentes del sistema técnico de voto electrónico, al menos a las autoridades electorales competentes, incluyendo información sobre el sistema, código fuente, intentos de intrusión, etc. Asimismo, la Recomendación señala que un organismo independiente debe verificar el sistema de voto regularmente. También, se indica la posibilidad de un segundo recuento de verificación, lo cual tiene muchas variantes (por el mismo sistema, de forma paralela, impresión de papeletas y recuento manual).

Fiabilidad y seguridad

La Recomendación recoge numerosas previsiones, entre las que cabe destacar: verificaciones de seguridad previas al comicio, selección de personal autorizado con accesos al sistema, con sistemas de

actuación por parejas –mínimo- y rotación de personal, la incorporación de mecanismos de seguridad a lo largo del procedimiento electoral frente averías y ataques. Mecanismos de encriptación para el caso de salida de la urna electrónica de los datos de los votos, etc.

Para parte de la doctrina, el rastro en papel es "exigencia ineludible", que el resguardo de voto sea depositado en un recipiente: "Cualquier tipo de auditoría posterior de las elecciones realizadas a través de voto electrónico requiere de la constancia impresa." (Martínez Dalmau). Se trata del conocido en términos ingleses como *Voter Verified Papel Audit Trail* (VVPAT)

http://dialnet.unirioja.es/servlet/articulo?codigo=3172502

A mi juicio, esta imposición del rastro de papel puede conllevar la ineficacia del e-voto y la inhibición de todas sus ventajas. Si se da la desconfianza social en el sistema electrónico que lleve a esta exigencia, no debería implantarse un sistema de voto electrónico. Cuestión diferente es el comprobante en papel del voto efectuado o del sentido del voto emitido para la confianza del elector.

4. La duda del voto electrónico nulo

Una de las ventajas del voto electrónico es que excluye la posibilidad de votos nulos, evitando la existencia de un porcentaje pequeño pero indeseable de errores de los electores.

Sobre la base de los principios, si bien debe garantizarse el voto en blanco, parece que no tiene lugar el mantenimiento electrónico del voto nulo. No obstante, la realidad política lleva a que no sea en modo alguno extraño que algunos electores voten voluntariamente de forma nula. Tales mensajes suelen expresar repulsa a la votación, al sistema electoral, al régimen de partidos políticos, desmarcación de posiciones políticas elegidas por otras facciones, etc.

La doctrina no muestra acuerdo sobre el particular, habiendo posiciones en un sentido u otro. Por mi parte, pudiéndose afirmar la existencia en algunos países de una cuarta vía ya casi tradicional de expresión (votar, no votar, votar en blanco y votar nulo), considero que debe mantenerse –por artificial e irracional que resulte- esta posibilidad en el mundo electrónico. Ésta parece ser la opción, por ejemplo, de la Ley 5/1990, de 15 de junio, ley de elecciones vascas reformada por la Ley 15/1998, de 19 de junio de de Elecciones al Parlamento Vasco (art. 132 bis).

5. Las dificultades de control del voto electrónico y la necesaria de confianza social para su implantación

El voto electrónico "plantea, pues, un problema medular, puesto que parece que el voto electrónico impugna la esencia misma de la observación"[5]. Si el escrutinio manual puede hacerlo incluso un analfabeto, el escrutinio electrónico requiere de conocimientos. Señala Jones[6] que con el e-voto se degradan los derechos de los observadores pues "todo lo que el observador puede ver es una caja con algunos ventiladores y luces parpadeantes, y tal vez la espalda del técnico o un programador sentado al teclado que escribe comandos desconocidos en el sistema". Así, con suerte cabe visualizar el proceso, pero no controlarlo. Y esto no es suficiente.

En esta dirección cabe subrayar la reciente sentencia del Tribunal Constitucional Federal alemán de 3 de marzo de 2009 (BVerfG, 2 BvC 3/07)[7] sobre voto electrónico. En la misma se subraya que la transparencia es condición esencial del proceso electoral (§ 106) y que "Cada ciudadano ha de poder seguir y entender de forma fiable las etapas centrales de la elección sin conocimientos técnicos especiales" (§ 109; en el mismo sentido, § 119, 148 y 149). Dicho control real se considera exigible, no bastando que la ingeniería y software hayan sido certificados y auditados previamente (§ 123). El Tribunal exige, entre otras, la publicación de los informes técnicos o el acceso al código fuente (§ 125), lo cual está muy reñido con elementos de seguridad misma y sobre todo, de propiedad industrial. El Alto tribunal estima que ventajas del e-voto como la disminución (o incluso supresión) de los errores involuntarios del elector, que generan votos nulos no deliberados (§ 127), o la rapidez en la publicación de los resultados (§ 130) no constituyen argumentos de peso suficiente como para deshacer la regla común de la publicidad y la comprensión electoral. En el caso enjuiciado se consideran insuficientes las garantías del carácter público de las elecciones (art. 38 en relación con el artículo 20.1 y 20.2 de la

---

[5] BARRAT I ESTEVE, Jordi, "Observación electoral y voto electrónico", en *Revista catalana de dret públic*, nº. 39, 2009 (Ejemplar dedicado a: Els "guardians" de l'autonomia), pags. 277-296, pág. 2 versión electrónica. Texto completo en Dialnet:
http://dialnet.unirioja.es/servlet/articulo?codigo=3100573&orden=242119&info=link

[6] JONES, Douglas W., *The European 2004 Draft E-Voting Standard: Some critical comments*, Iowa City: University of Iowa, 2004, § 56. Disponible en:
http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml

[7] El texto en alemán en
http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html
en inglés, en
http://www.bundesverfassungsgericht.de/en/decisions/rs20090303_2bvc000307en.html

Ley Fundamental) ponderadas respecto de los intereses en juego a favor del e-voto.

Una de las posibles ventajas del e-voto es la celeridad del recuento, que no es manual. No obstante, esta ventaja se hace muy relativa en sistemas con listas cerradas y bloqueadas, como suele ser el caso español, en donde el recuento es bastante sencillo y rápido. En el caso español que el sistema electrónico no puede dar la transparencia que aquí se da, pues como se ha visto se cuenta con una potencial y real capacidad de auditar el proceso de escrutinio y recuento por cualquier ciudadano y, sobre todo, por los representantes, partidos y candidatos.

Ahora bien, tampoco hay que cerrar la puerta al e-voto y las ventajas que trae consigo siempre que se consiga la suficiente confianza social. Y es que, todo se hace depender de la confianza ciudadana pues como afirma Barrat "el voto electrónico sería compatible con los principios electorales de cualquier democracia, siempre y cuando las medidas garantistas generaran la suficiente confianza ciudadana"[8]. La confianza es cuestión de adaptación no sólo tecnológica sino, especialmente, social.

En este sentido no parecen muchas las muestras de desconfianza en el voto en países que lo tienen generalizado, como Brasil o India. En Europa, destacan movimientos claramente contrarios al e-voto en Países Bajos

ONG "No confiamos en las máquinas de votación" (We don´t trust voting computers)

http://www.wijvertrouwenstemcomputersniet.nl

o el Movimiento belga contra el e-voto: http://www.poureva.be/

En Italia se ha llegado a paralizar cualquier avance en la materia bajo la afirmación pública de "Basta con il voto elettronico"

http://www.corriere.it/Primo_Piano/Politica/2006/11_Novembre/29/amato.shtml

Por muy seguro que sea objetivamente un sistema de e-voto, si la desconfianza en la población es también un dato objetivo, el voto electrónico es perverso en sus efectos y condicionar el comportamiento del electorado. Incluso el gobierno puede tener la diabólica conducta de inducir temores sobre el secreto del voto electrónico inhibiendo la votación a favor de la oposición.

Video de Argentina contra el voto electrónico en 10 argumentos por un famoso hacker

http://www.youtube.com/watch?v=7iAgXT8lh10

http://www.youtube.com/watch?v=kizqOsUEATQ&feature=related

[8] Ob cit. pág. 10 versión electrónica.

Videos –parodia contra el e-voto

Movimiento antibelga:
http://www.youtube.com/watch?v=4g0zbaIQL90

Homer Simpson tries to vote for Obama
http://www.youtube.com/watch?v=1aBaX9GPSaQ&feature=related

VII. Ejercicio electrónico formal e informal de iniciativa legislativa popular y del derecho de petición

1. Iniciativa legislativa popular y ejercicio del derecho de petición por vía electrónica

Entre las fórmulas de democracia semi-directa o de democracia participativa (según se conciba), se encuentra la incitación o excitación de los órganos políticos, legislativos y administrativos para que adopten decisiones políticas o normativas. Ello se realiza a través de iniciativas populares u otros mecanismos de participación de la sociedad civil. Las variedades constitucionales y legislativas son muchas tanto por países como en razón de ámbitos de decisión política. Al igual que el derecho de petición, el ejercicio de estas fórmulas según los requisitos, sólo garantiza su tramitación, pero obviamente no el logro del objetivo político o normativo deseado.

El ejercicio electrónico de estas vías democráticas requiere de la conjunción de premisas fácticas, jurídicas y técnicas.

-Por cuanto a las bases materiales, una de las claves para el ejercicio vía electrónica de estas posibilidades se hace depender de la generalización en la población de medios de firma electrónica. Esto en modo alguno está generalizado en América Latina, si bien en España, en marzo de 2010 son más de 14 millones los DNI electrónicos expedidos. Cuestión diferente es que no muchos sepan o quieran usar estos medios que acreditan la identidad.

-Jurídicamente es necesaria cierta cobertura legal en la regulación de firma electrónica y la específica de iniciativa legislativa o petición. Ha de haber transparencia y seguridad en la comprobación del cumplimiento de requisitos del ejercicio de estos derechos. No obstante, las exigencias no deben ser desproporcionadas para estas finalidades. Del mismo modo, considero que han de adoptarse medidas normativas y de garantía de los ficheros de datos personales de los suscriptores de tales iniciativas, un *botín* político de gran sensibilidad que debe ser jurídica y técnicamente custodiado. En España, la regulación del derecho de petición (Ley orgánica 4/2001, art. 4) menciona su ejercicio electrónico y el antes referido artículo 6 de la Ley 11/2007 garantiza que se puedan formular peticiones de forma electrónica. De otra parte, Ley Orgánica 3/1984 que regula la Iniciativa Legislativa Popular, gracias a su reforma por 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: "Las firmas se podrán recoger también como firma electrónica conforme a lo que establezca la legislación correspondiente.").

- Técnicamente, son necesarios sistemas que permitan la recogida de firmas de forma fiable, que sean auditados por las entidades de control. Pues bien, en 28 de enero de 2010 la Junta electoral Central en España ha homologado por primera vez una plataforma de recogida de firmas para presentación de Iniciativa Legislativa desarrollada por una Universidad.

2. Ejercicio informal de iniciativas y peticiones vía electrónica

Hay fenómenos electrónicos de apoyos políticos hasta ahora impensables por cuanto a su magnitud. Quizá el precedente lo encontremos en las campañas de Amnistía Internacional de 2002 para salvar de la lapidación en Nigeria por adulterio a Amina Lawal (luego para Safiya Hussaini), que alcanzaron apoyos millonarios. Desde entonces, han sido muchos los movimientos de "recogida de firmas" o "apoyos" electrónicos informales. Informales por cuanto no se garantiza la verdadera identidad de quien realiza el apoyo o la firma o el número de veces que lo realiza, lo cual, como se ha visto no es muy sencillo. Existen plataformas para el ejercicio informal del derecho de petición o el apoyo a iniciativas (por ejemplo: www.petitiononline.com). Además de sitios donde inscribirse como suscriptor de una iniciativa, una fórmula reciente, por ejemplo, es la del manifiesto electrónico, que supone recoger el texto de un manifiesto en las webs personales o de organizaciones que lo apoyan. Así, por ejemplo, el texto del Manifiesto "En defensa de los derechos fundamentales en internet" de diciembre de 2009 se encuentra en más de 90.000 sitios en la red (http://www.cotino.net/2009/12/manifiesto-en-defensa-de-los-derechos-fundamentales-en-internet/). Que se trate de un ejercicio informal de derechos no resta el valor político que puedan tener estas iniciativas o movimientos, pero tampoco hay que magnificarlos puesto que la manipulación de los mismos es bien sencilla.

VIII. TICs, transparencia y acceso a la información pública por el público

1. Principios y derechos de transparencia y acceso a la información pública

La transparencia y el acceso a la información pública han sido objeto de estudio en un módulo anterior.

La Directriz 15 de la Recomendación de e-democracia de 2009 es clara:

"La transparencia en la e-democracia debe incluir la transparencia en el proceso de participación en todos los niveles políticos y en todas las fases de deliberación y en el proceso de toma de decisiones, y durante la ejecución, seguimiento y evaluación."

Las TICs permiten, facilitan y abaratan enormemente esta transparencia. Basta una suscripción a una mera lista de correo para estar informado de cada momento del proceso de toma de decisiones y de las decisiones adoptadas. Sin embargo, como se dijo, hoy por hoy la legislación es bastante renuente y refractaria de imponer obligaciones a los poderes públicos –y derechos a los ciudadanos- en el ámbito de su transparencia e información, obligaciones de empleo de las TICs. Hay mucho desconocimiento y sobre todo, una total falta de compromiso político y jurídico, como es prueba que sí que se exija jurídicamente la "transparencia electrónica" a empresas y sociedades mercantiles.

Las leyes de transparencia son bastante más habituales en América Latina que en España (http://www.bibliojuridica.org/libros/libro.htm?l=1156). En todo caso, en España se ha dado cierto impulso al acceso a la información pública por medios electrónicos con la ya citada Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos. Dicha norma impone la la existencia de "sedes electrónicas" de los poderes públicos con unos contenidos mínimos, impulsa los boletines oficiales electrónicos –cuya versión en papel jurídicamente está desapareciendo; promueve la información institucional de calidad y asegura que el derecho de acceso se pueda ejercer electrónicamente o conocer el estado de procedimiento. No obstante, queda mucho por hacer.

Cabe señalar que la Unión Europea, donde su Carta de derechos fundamentales reconoce el de acceso a la información pública. Y la normativa incluye el pleno acceso de forma electrónica, lo cual viene además exigido por la normativa de desarrollo de este derecho, el Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

2. Propuesta de obligaciones jurídicas y derechos de los ciudadanos de acceso a la información pública en la red

En las diferentes legislaciones abundan falsos compromisos y obligaciones no exigibles jurídicamente de implantación de las TICs en favor de la transparencia e información. A continuación, me permito incluir una propuesta de obligaciones y derechos que deben incorporarse bien en las normativas de desarrollo de los mencionados

principios y derechos o que, incluso, pueden en casos considerarse obligaciones derivadas del carácter fundamental de algunos derechos en juego, a saber:

-que una institución pública disponga de un sitio web. Esta obligación puede articularse y regularse a partir de parámetros como presupuesto de la institución, número de ciudadanos que componen la población, etc.

-que dicho sitio web cumpla con unas obligaciones de estructura, diseño y servicios.

-que la información de dicho sitio sea accesible (para sectores con dificultades) siguiendo unos estándares reconocidos internacionalmente.

-que la información de dicho sitio sea usable y manejable. Ello se puede obligar jurídicamente estableciendo, por ejemplo, número de "clicks" máximo para alcanzar algunas informaciones temáticas clave u obligando al reenvío a portales temáticos directamente vinculados con la participación y democracia. Con la obligación de disponer de forma sencilla de un mapa del contenido de ese sitio web.

-obligando a la existencia de contenidos mínimos de interés para la participación e información. Por ejemplo:

- la obligación de incluir una serie de contenidos estructurados por temas,
- imposición de temas mínimos para instituciones municipales, provinciales, ministeriales, etc. Según sus competencias jurídicamente reconocidas.
- la normativa básica reguladora de la institución.
- La normativa básica que genera la institución.
- Información sobre las decisiones políticas y normativas en trámite, el procedimiento y posibilidades de participación en las mismas, grupos interesados y posiciones de los actores políticos.
- Información sobre los responsables políticos de la institución, con contenidos mínimos (responsabilidades públicas anteriores, declaración de haberes, resultados electorales, etc.

Steven Clift, por ejemplo, señala para el futuro la necesidad de reconocimiento de unos derechos mínimos como:

-que no pueda darse cualquier reunión pública sin agendas y documentos publicados previamente en la red. "Sin aviso electrónico, no reuniones";

- que toda propuesta legislativa y sus enmiendas fueran accesibles, así como no posible entrar en vigor una norma aprobada no publicada en la red. "Sin transparencia... no autoridad ni dinero".

- derecho ciudadano a ser notificado por correo electrónico sobre

información pública basada en el perfil de sus intereses y territorial.

-derecho de acceso sencillo a directorios siempre actualizados y locales de "mi democracia", con datos de contactos de todo cargo público elegido. "Ningún dato de contacto, ningún poder".

Como puede observarse, la propuesta hacer referencia a entes y órganos públicos, entre los cuales, obviamente puede considerarse los parlamentos o órganos representativos de que se trate, al igual que si se trata de entes de naturaleza gubernamental o administrativa.

3. Calidad de la información pública y mecanismos de control de la transparencia

Estas obligaciones para los poderes públicos hoy día extrañamente son reconocidas –sólo en algunas leyes de administración electrónica de países avanzados-, pese a la paradoja de que se están imponiendo a particulares Es factible que en unos años, estas pretensiones se consideren jurídicamente integrantes de derechos de los ciudadanos.

El proceso de reconocimiento será, posiblemente, sectorial (procedimientos administrativos en masa: medio ambiente, urbanismo, planificación, etc.) y gradual.

Hay que advertir que una mayor información no implica un público más y mejor informado. La saturación de información, la manipulación o el control sobre la misma, la falta de posibilidades, la falta de calidad de la información o de estímulos para que la información se torne conocimiento llevan correr el peligro de peor información y ciudadanos peor informados. Además, es el emisor quien selecciona la información y la hace más o menos accesible en parámetros materiales (difícil de controlar jurídicamente) con todas las consecuencias que ello entraña.

Es por ello que se consolidan conceptos no difíciles de trasladar al ámbito jurídico, como acceso y accesibilidad a la información, como los propuestos por el G-8:

"Acceso significa la posibilidad real de consultar o acceder electrónicamente a la información.

Accesibilidad significa la facilidad con la que uno puede hacer uso real de la posibilidad de acceder a la información electrónica."

Y son diversos los parámetros que sirven para fijar el grado de accesibilidad a la información pública electrónica, a saber: Recognoscibilidad y localizabilidad; disponibilidad; manejabilidad; Precio razonable (*affordability*); responsabilidad y confianza; claridad; accesibilidad para los limitados.

Jurídicamente debe subrayarse la responsabilidad patrimonial de los

poderes públicos por la información propia que difundan en sus sitios. Aunque incluyan cláusulas de exención de responsabilidad por la calidad de sus contenidos, el alcance de éstas ha de ser muy relativo. En todo caso, habrá que estar a la regulación concreta de la responsabilidad patriminonial en cada país.

Los principios expuestos deben aceptarse como criterios inspiradores de toda actuación de información pública por la red. Y el control de la regulación y el cumplimiento estos principios puede ser responsabilidad de distintas instituciones. En ocasiones hay instituciones específicas para velar por el acceso a la información pública, como el Instituto Federal de Acceso a la Información Pública (IFAI) en México (www.ifai.org.mx/) en razón de su avanzada ley de transparencia de 2003. En algunos países se sigue el modelo anglosajón por el que la autoridad independiente que controla la protección de datos personales, controla también el acceso a la información pública. En países donde desde hace lustros existen agencias de protección de datos con una fuerte inercia hacia su protección frente a la transparencia, este modelo puede ser negativo para el acceso a la información público. También, diversas instituciones pueden pasar a responsabilizarse del cumplimiento de normativa de transparencia, como las mismas defensorías del pueblo o comisionados ya existentes en diversos países del mundo anglosajón (*Information Commissioner* o *Information Tribune*).

IX. TICs y democracia participativa

106. La experiencia y la literatura constata la existencia de fases y subfases en todo procedimiento participativo, a saber:

Previas

- Decisión de si procede abrir un proceso concreto de participación
- Selección y reconocimiento de participantes.
- Selección de ámbitos sobre los que participar.

Difusión: Difusión de información y del conocimiento. Transparencia electrónica inteligente, con garantías democráticas y seguimiento de los criterios de “accesibilidad”.

Consulta: Mecanismos de consultas e interacción, deliberación.

Participación activa: Mecanismos de decisión (desde el voto, hasta la adopción de decisiones).

Ver, Manual de información, consultas y participación en la toma de decisiones de la OCDE http://www.oecd.org/dataoecd/20/37/37873406.pdf

También resulta oportuno recordar algo que creo que es obvio: no hay que emplear necesariamente las TICs en todas y cada una de las fases del proceso participativo, sino que pueden ser empleadas específicamente en algunas de ellas, en las que resulten más idóneas.

Pues bien, hoy por hoy las mejores prácticas mundiales de democracia electrónica se centran en las primeras fases del proceso (mejor y mayor información), nunca en la fase de toma de decisiones, en concreto, nunca en las experiencias de voto electrónico. (Así, los informes mundiales de Steven Clift http://www.publicus.net/e-government/)

En todo caso, las posibilidades de la TICs no se limitan a la mayor y mejor información, sino también son elementos esenciales para conformar y estructurar la sociedad civil, facilitar su generación, emergencia y consolidación así como su participación concreta en los procesos participativos.

Hay que recordar, de nuevo, que estas posibilidades se dan respecto de todos los poderes públicos, incluidos, obviamente, los parlamentos, en tanto en cuanto los procesos participativos de información y consultas (democracia participativa) no se limitan a la participación administrativa.

Por desgracia, las mejores oportunidades que brinda la red no suelen ser bien aprovechadas por las autoridades. En muchos casos se gasta dinero en proyectos bastante inútiles y, sobre todo, escasamente utilizados por la población. Asimismo, no se adquieren compromisos jurídicos.

X. Libertades informativas y su difícil adaptación a internet

107. Hoy día no cabe duda de que no son democráticos los doce países denominados “enemigos de internet”: Arabia Saudí, Birmania, China, Corea del Norte, Cuba, Egipto, Irán, Siria, Túnez, Turkmenistán, Uzbekistán y Vietnam) utilizan distintos métodos: desde los que impiden el desarrollo tecnológico y de infraestructuras para tratar de impedir el acceso a Internet, como Corea del Norte, Birmania o Turkmenistán, a los que desarrollan sofisticados sistemas y emplean a miles de personas para vigilar la Red, como China. En el último año, Vietnam e Irán han aumentado extraordinariamente el control y las detenciones de internautas.

http://www.elpais.com/articulo/sociedad/Control/guerra/libertad/Internet/elpepusoc/20100311elpepusoc_13/Tes

Son ya muy diversos fenómenos comunicativos a través de la red y alternativos a los medios de comunicación tradicionales –como los *blogs*- o la expresión de movimientos sociales a través de la red. Curiosamente, la mayoría de las aproximaciones a la democracia

electrónica, desatendían hasta la eclosión de la web 2.0 o web participativas estos fenómenos de nuevas formas de ejercicio de las libertades de expresión de información, siendo que superan y con mucho en importancia a las acciones públicas de democracia y participación electrónicas.

1. La libertad de expresión e información protege en general internet y a todos los internautas sin mayores límites que en otros medios

Internet está protegido por la libertad de expresión. En consecuencia, en tanto en cuanto Internet es un canal de comunicación, queda protegido por la libertad de expresión e información, como desde 1997 afirmase con claridad el Tribunal Supremo de los EEUU (*ACLU vs Reno* de 1997). Como punto de partida, tanto los modos de comunicación interpersonal en internet (correo, chat, foros, etc.), cuanto los medios de comunicación en internet (blogs, páginas web, periódicos digitales, etc.) sí están protegidos por estas libertades. A este respecto puede citarse el principio nº 1 de la "Declaración sobre la libertad de comunicación en internet", del Consejo de Europa de 28 de mayo de 2003 (sin valor jurídico normativo). Ahí se dispone que:

"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."

Es más, en Estados Unidos se ha dicho que el estándar de limitación ha de ser el mínimo en internet, como el de la prensa escrita.

Además, al no contar con las limitaciones del espacio radioeléctrico, sería contrario a la libertad de expresión exigir una autorización previa para la presencia en la red o someterlo a los requisitos del servicio público.

Las libertades de expresión e información se reconocen "a cualquier otra persona que facilite la noticia veraz de un hecho y a la colectividad en cuanto receptora de aquélla (por todas, SSTC 6/1981, 105/1983, 168/1986, 165/1987, 6/1988, 176/1995, 4/1996)". Sin embargo, se detecta una inercia sociológica y jurídica en los tribunales de reservar las libertades informativas para los medios de comunicación. Asi por ejemplo la sentencia del TS de 26 de junio de 2008 de ha ratificado la sanción de la Agencia de protección de datos 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. Afirma el Tribunal Supremo que "la libertad de información "alcanza su máximo nivel 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).

La Agencia de protección de datos suele considerar de interés público y legítima constitucionalmente la difusión de datos personales por periodistas clásicos, pero no por asociaciones, sindicatos, empresas o particulares, llegando a afirmar en 2010 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." (*Resolución 211/2010, PS 439/2009).

Argumentos como este no pueden abolir la protección de datos, sino la misma libertad de expresión en la red.

Frente a esta inercia, la sentencia del Tribunal de Justicia de las Comunidades Europeas (Gran Sala) de 16 de diciembre de 2008, cuestión prejudicial asunto C 73/07 afirma que las exenciones de protección de datos no quedan reservadas a "a las empresas de medios de comunicación, sino también a toda persona que ejerza una actividad periodística" (nº 58) por medios clásicos o electrónicos.

Y frente a esta inercia, en sentido bien contrario destaca la ya citada sentencia 531/2009, de 18 de diciembre de 2009, Juzgado de lo Penal Nº 16 de Madrid, que a directivos de la Cadena Ser (la de más audiencia en España) por revelación de datos de afiliados a un partido: se entiende que por ser profesionales debían haber tenido mayor diligencia con la gestión de datos personales sensibles y haber percibido mejor que cualquier particular la innecesariedad de su publicación. Esta sentencia ha suscitado ataques muy duros desde los medios clásicos.

2. Garantías frente al cierre de webs o al corte de acceso a internet

En su momento se abordó el "ius comunicationis" como derecho fundamental. Se señaló que hoy día no se puede exigir como derecho al Estado que facilite el acceso a la red. Ello no obsta para que una medida de restricción del acceso a las TICs con el que ya se cuente por el particular o abonado sí que deba ser considerada como limitación a la libertad de expresión y de emitir y recibir información y que requiera de autorización judicial. En este sentido, cabe destacar la Decisión nº 2009-580 de 10 de junio de 2009 del Consejo Constitucional francés. El

máximo intérprete de la Constitución gala afirma 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.

Desde otra perspectiva es polémica la cuestión de si es necesaria la autoridad judicial para el 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:

"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."

Lo cierto es que hasta 2010 ninguna ley señala que sólo un juez pudiera cerrar una web. En 2010, la Ley de economía sostenible como medida contra la piratería informática establece un sistema para decretar por una entidad no judicial el cierre de webs que enlacen a contenidos ilícitos. Ahora bien y "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). De otra parte, la Agencia de protección de datos no tiene problema en decretar sanciones (sanción grave por no consentimiento del afectado: 60 mil euros, con "rebaja" de 600 a 6.000 euros) por difusión ilícita de datos personales en webs. El Tribunal Constitucional español en modo alguno ha dejado claros los términos en que un control administrativo de contenidos es posible[9], pese a que parece que se está generalizando en la red.

Internet es como la calle, donde podemos hacer uso de nuestras libertades, pero no todo es libertad de expresión e información en internet. Siempre se ha dicho que la libertad de expresión no incluye gritar "fuego" en un teatro. Como tampoco supone un ejercicio de la libertad de expresión una página web de *phising*, simulando ser un banco o administración para llevarse nuestros datos. Tampoco ejerce la

[9] 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).

libertad de expresión quien vende medicamentos por internet o productos peligrosos para menores o señala cómo fabricar bombas. En estos casos, una autoridad administrativa (policial, de consumo, etc.) puede adoptar medidas sin esperar a un juez, sin duda. No obstante, cuando existan dudas razonables sobre si se trata del ejericio de la libertad de expresión, será necesaria la participación de una autoridad judicial.

La cuestión subsiguiente es ¿cuándo se ejerce la libertad de expresión? Y 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). Cuestión que se examina más adelante.

3. Proyección de algunas categorías y garantías de las libertades informativa a internet

a) Una clave: la relevancia o interés público de la noticia

Considerar el "interés público" y la "necesidad para la formación de la opinión pública" de una información es clara: hace más intensa la protección de la información al rebajar la protección de otros derechos y bienes constitucionales con los que colisiona. Cualquier información u opinión en internet por cualquier persona puede tener esta protección.

Para considerar la existencia de este interés, relevancia y necesidad, son muchos los parámetros jurídicos elaborados (importancia objetiva de la noticia –naturaleza del hecho u acontecimiento del que se informa, actualidad-, importancia y naturaleza subjetiva de los afectados –cargos históricos, cargos públicos, "famosos", etc. la actividad desarrollada por éstos-, el contexto, etc.). Cabe también recordar que jurídicamente el interés público de la información es un concepto diferente del interés *del* público o curiosidad por dicha información. Asimismo y hasta ahora, el interés público de una información es un concepto objetivo que no viene determinado porque la información haya sido objeto de publicación por un medio de comunicación.

En general, los tribunales no han querido ser severos y restrictivos en la consideración de si una información no era objetivamente de interés público. Es muy posible que hasta ahora los tribunales implícitamente considerasen que la información tenía interés público

sólo por el hecho de que la noticia se recogiera en los medios tradicionales. Los medios de comunicación clásicos eran un filtro *material* –no jurídico- para determinar qué información gozaba de interés público

Sin embargo, con la sociedad de la información, los nuevos modos de comunicación de internet multiplican exponencialmente la información que se genera, ya no existe ese filtro material de los medios de comunicación clásicos que daba "pistas" a los jueces de a qué informaciones había que dotarles de una mayor protección por ser de interés público y contribuir a formar la opinión pública.

b) La veracidad y la diligencia del informador y el derecho de réplica o rectificación

Como sabemos, hay libertad de información y de prensa sobre hechos verdaderos, en el sentido de que el periodista haya sido más o menos diligente en su labor. Es muy posible que poco a poco esta exigencia de veracidad y diligencia de la información tenga que adecuarse a un entorno muy distinto del de la profesión periodística clásica.

No es necesario ser profesional para producir información y opinión en internet, pero la diligencia debe de mantenerse. Para ello puede resultar útil el ejercicio del derecho de rectificación o de réplica ante cualquier información incorrecta en un modo o medio de comunicación en internet.

La aplicación de este derecho se ha reconocido en Estados Unidos en 2003 (Georgia Supreme Court: Georgia rMathis v. Cannon.) o recientemente en España (Audiencia Provincial de Asturias, de Asturias (Sección 6ª) de 3 de junio de 2002, para un foro) exigiendo un juez la rectificación en lo afirmado en un foro de internet.

Lo cierto, en todo caso, es que hoy día es casi imposible controlar la diligencia de la información en internet. En la red los contenidos se multiplican y reproducen de un sitio a otro a veces de forma automática, muchos contenidos –y por supuesto los más polémicos-, se aportan anónimamente en la mayoría de los sitios web. Asimismo, no hay que olvidar que los servidores no tienen ni posibilidad ni obligación legal de controlar la licitud de los contenidos que introducen en las páginas web de las que son responsables técnicos, pero no editores.

Pese al mantenimiento jurídico de las exigencias de diligencia, y la misma protección de la intimidad o el honor, las posibilidades de acción real se reducen. Es muy posible que haya que reconsiderar jurídicamente estas actuales exigencias.

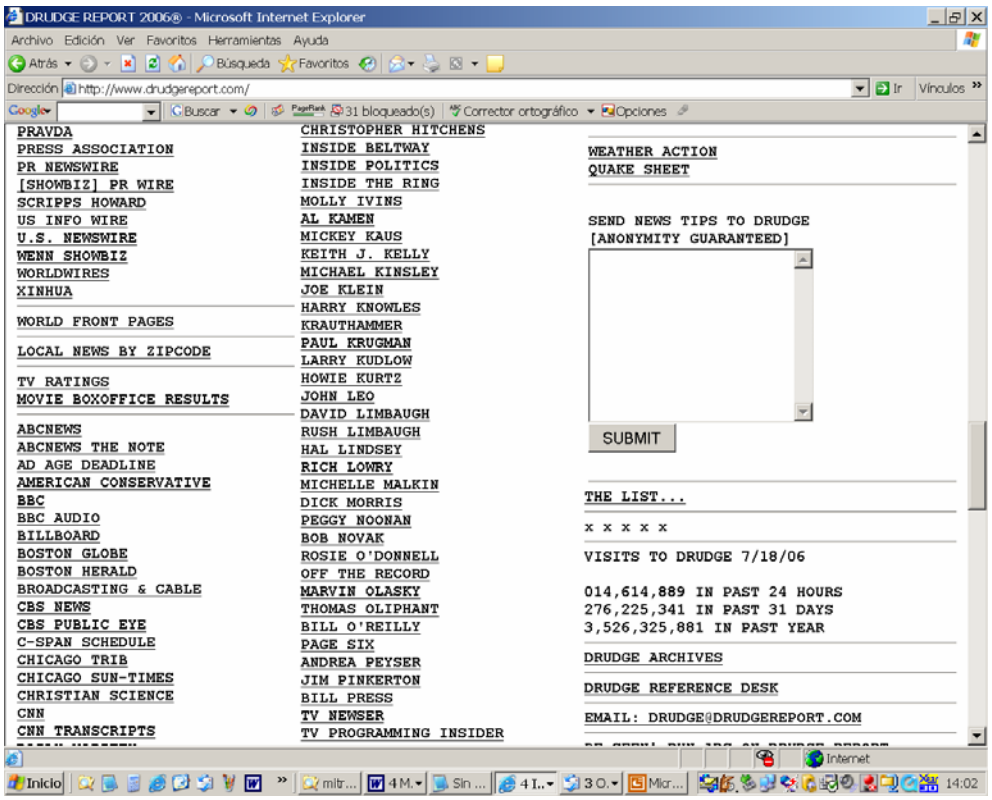
c) El secreto profesional del periodista en internet ¿para todos?

Como se ha dicho, todos somos "periodistas" en internet cuando generamos contenidos, pero está claro que no todos son profesionales. En muchas constituciones el privilegio del derecho a no revelar las fuentes de información se reserva a los profesionales, en otras ocasiones, a los "periodistas".

Lo cierto es que la trascendencia de internet en países como Estados Unidos ha llevado a que muchos particulares tengan a través de sus páginas personales o *blogs*, una trascendencia mucho mayor que los periodistas profesionales.

Por ello, ya en 2004 comenzaron a conseguir acreditaciones como periodistas profesionales, como en las elecciones Bush vs. Kerry. Asimismo, desde 2005 los tribunales de Estados Unidos (juez de Santa Clara, marzo 2005, Caso Apple y Dan Gillmore - de forma más clara en la Corte Estatal de Apelaciones de San José en mayo de 2006-, y en caso John Doe nº1 v. Cahill, de octubre de 2005, en Delaware). Los efectos de este tipo de resoluciones pueden ser decisivos para el futuro de internet, vista la experiencia de los *blogs* en Estados Unidos.

El blog www.drudgereport.com uno de los más visitados del mundo, garantiza el anonimato para quienes le remitan infomación privilegiada "tip"



4. Dificultades de atribución de responsabilidad jurídica en la red

En internet se generan problemas casi insuperables de atribución y persecución de la responsabilidad civil, administrativa o penal, según se trate. Las dificultades materiales son muchas:

- los problemas para para perseguir contenidos ilícitos para el Derecho nacional, por estar ubicados fuera del ámbito territorial.
- Normalmente, quien integra el contenido ilícito lo hace de forma anónima . Conocer su número IP que identifica el ordenador desde el que se conecta –si es que se puede- puede no ser suficiente para conocer la identidad de la persona que ha cometido el ilícito.
- La autoría y difusión colaborativa de los contenidos de la web 2.0 conlleva que sea casi imposible de determinar el responsible del contenido y de su difusión.

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, pero sí tiene el deber de retirar o bloquear los contenidos cuando las autoridades le comunican la ilicitud. Del miso modo, como principio, no hay responsabilidad por el contenido de los enlaces o de los resultados que ofrece un servicio de búsquedas (como Google). Sin embargo, la regulación no da respuesta a los problemas que hoy son los más habituales. El problema principal reside en determinar si cualquier sitio en la red que permite integrar contenidos de terceros usuarios (desde un foro clásico a *Youtube*) puede beneficiarse de las excenciones legales de resonsabilidad. Y lo cierto es que hay respuestas judiciales para todos los gustos, que van desde la exención de responsabilidad del responsable de un foro por los comentarios ilícitos ahí vertidos, a la atribución de responsabilidad penal al responsable de un blog por los comentarios que le insertaron. Asimismo, el TS español en diciembre de 2009 hizo responsable a la Asociación de internautas por los contenidos ilícitos que insertó en su sitio una plataforma contraria a los derechos de autor. Habrá que esperar alguna decisión a nivel europeo.

5. Pluralismo en internet y posible "censura" por empresas privadas

En principio, la facilidad de estar presente en la red es muy grande, sin muchos medios o recursos. Ello facilita la pluralidad en la red. Cuestión muy diferente es ser "visible" en la red. Encontrar contenidos

en más de 10 billones de páginas web puede ser peor que encontrar una aguja en un pajar. Para ello hay medios privados que facilitan el acceso a la información, como Google o Yahoo. Estar presente entre los primeros resultados de estos medios es garantía de visibilidad en la red.

Afortunadamente los criterios de visibilidad en estos buscadores son 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.

Hay que decir que la categoría de "censura" sólo se reserva para los poderes públicos, y en este caso se trata de autocensura.

Considero que las empresas privadas también pueden cometer una lesión de un derecho fundamental, como el caso de que instrumentos tan importantes censurasen políticamente contenidos. El Derecho hasta ahora no da una respuesta, pero considero que el interés público podría justificar una actuación legislativa que impusiese a tales buscadores no utilizar criterios políticos para omitir resultados de búsqueda y, en todo caso, hacer públicos todos los criterios que pueden servir para restringir políticamente resultados.

Al respecto, pueden ser recomendables algunos de los videos en Youtube sobre "google censura" o "google censorship". Más allá de teorías de la conspiración que hay en ocasiones, lo cierto es que la propiedad industrial y libertd de empresa no permiten conocer el alcance de la restricción de contenidos en buscadores como Google, sistemas de vídeo, como Youtube, o los sistemas de filtro y seguridad informática que se instalan en las organizaciones.