“Democracia electrónica y libertades en la red”, por Lorenzo Cotino Hueso, versión actualizada a marzo de 2016

Contenido:

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.

86. 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, TIC) 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 TIC, valen como un concepto amplio de democracia electrónica.

87. Versión fuerte y versión débil de democracia electrónica

El instrumento que son las TIC 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 TIC 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 era por lo general escaso y poco profundo, y buena parte de los estudios eran bastante visionarios y utópicos y, también por lo

general, partían de una crítica –destructiva o constructiva, según los casos- de la democracia representativa, como algo a superar gracias a las TIC. En este sentido, las TIC venían a ser la *excus*a para cambiar el sistema político. Así las cosas, bajo terminologías diferentes, con la "democracia electrónica" parecía 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". Estas visiones de la democracia electrónica han quedado bastante trasnochadas frente a la emergencia de la web 2.0 que viene de la mano con la democracia deliberativa a la que se hace referencia a continuación.

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 TIC 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 "TIC" 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 y, especialmente en los últimos años a través de las redes sociales. 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 TIC 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

88. Conceptos afines: especial atención al "gobierno electrónico" y la actual tendencia hacia el "Gobierno abierto". La Alianza para el Gobierno Abierto

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

El concepto de "TIC" 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 TIC 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 TIC.

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".

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 movimientos que influyeron en la Declaración Ministerial sobre administración electrónica aprobado por unanimidad en Malmö, Suecia, el 18 de noviembre 2009 que hacía referencia a los elementos básicos de este gobierno 2.0 http://ec.europa.eu/information_society/activities/egovernment/conferences/malmo_2009/press/ministerial-declaration-on-egovernment.pdf

En todo caso, el protagonismo y el impulso vinieron dados con la noción Open Government introducida por Obama en su famoso discurso de 2009 http://goo.gl/aTB8P donde afirmaba:

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

Desde entonces, los elementos básicos del concepto de gobierno abierto son más transparencia, reutilización de la información, participación pública y colaboración. . Lo más original y reciente del concepto a mi juicio es la colaboración. También cabe destacar la usabilidad y el empleo institucional de redes sociales. De igual modo, es innovador el hecho mismo de que todos los componentes de gobierno abierto se den bajo la filosofía de la web 2.0, como pauta que en las organizaciones políticas y administrativas impone la primacía del conocimiento frente a la jerarquía, la flexibilidad y el logro de objetivos colectivos frente a la individualidad y la burocracia, entre otros. Asimismo, el gobierno abierto supone un especial aporte no por la reutilización de la información, sino en el énfasis en que las instituciones faciliten activamente dicha reutilización bajo la noción de datos abiertos u "open data". Debe tenerse en cuenta que los datos abiertos no hacen referencia a la transparencia directamente, sino a que la información pública sea liberada como materia prima para generar riqueza. Bien es cierto que todos los elementos de la noción interactúan

unos con otros, al punto de que la mayor transparencia que se logra lo es de forma colaborativa y participativa, de mayor calidad y usabilidad, centrada en intereses ciudadanos, a través de las TIC y de las redes sociales. Como puede apreciarse el Gobierno Abierto queda mucho más vinculado a las vías de una democracia débil a través de internet que a las del e-voto y la democracia directa.

El lanzamiento de la noción de "Gobierno Abierto" ha sido un gran revulsivo que se ha articulado internacionalmente a través de la Alianza para el Gobierno Abierto (http://www.opengovpartnership.org/). Esta entidad fue lanzada el 20 de septiembre de 2011 cuando los 8 gobiernos fundadores (Brasil, Indonesia, México, Noruega, las Filipinas, Sudáfrica el Reino Unido y los Estados Unidos) suscribieron la Declaración de Gobierno Abierto (http://www.opengovpartnership.org/es/acerca-de/declaraci%C3%B3n-de-gobierno-abierto) y anunciaron sus planes de acción nacionales. Pronto pasaron a ser más de 60 países participantes. El Iberoamérica, Ecuador, Bolivia, Venzuela, Nicaragua no forman parte (por voluntad); tampoco Cuba y Haití por no reunir requisitos.

Para ser miembro es necesario reunir unos indicadores de gobernanza objetivos, asumir públicamente la Declaración de Gobierno Abierto de la OGP y presentar un plan de acción nacional. Dicho plan ha de ser resultado de una consulta pública con la sociedad civil y contar con compromisos concretos que reflejen los cuatro principios básicos de OGP: transparencia, participación ciudadana, rendición de cuentas y tecnología e innovación. A los doce meses y a los dos años el Gobierno remite un informe de auto-evaluación. Los gobiernos deben participar y apoyar el proceso del Mecanismo Independiente de Evaluación, que ofrece informes semestrales sobre cada país participante en OGP.

Se trata, pues, de un mecanismo suave en el que los gobiernos son los que –con la sociedad civil- se marcan sus propios objetivos y luego informan de su cumplimiento. Finalmente se revisan dichos informes. La OGP tiene un Comité Directivo con nueve representantes de gobiernos y nueve de sociedad civil.

La experiencia es positiva como motor y estímulo de políticas de gobierno abierto y de su exhibición ante otros gobiernos.

APREHENSIÓN JURÍDICA GENERAL DEL FENÓMENO

88. Ventajas generales de las TIC 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.).

89. 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 TIC 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 –ya derogada- Ley 11/2007 sobre e-administración que ya reconoció un auténtico derecho "*a relacionarse con las Administraciones Públicas utilizando medios electrónicos."* En la actualidad en la Ley 39/2015. Este derecho a la interactuación electrónica va siendo reconocido en diversas leyes administrativas en Iberoamérica y hay que estar especialmente por su realidad y garantías efectivas.

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.

En todo caso, la transparencia o publicidad activa, en forma de obligaciones jurídicas exigibles de disponer informaciónde relevancia jurídica a través de internet en los portales corporativos o sedes electrónicas institucionales se está generalizando en América Latina y, recientemente, en España.

ACCESO A LAS TIC, BRECHA DIGITAL Y SU TRATAMIENTO JURÍDICO

90. Acceso a internet en Latinoamérica y España

Los datos más recientes (noviembre de 2015, http://www.internetworldstats.com/stats.htm) señalan que en 2016 ya la mitad de población mundial -3.500 millones- accede a internet. América Latina viene a suponer uno de cada diez internautas, siendo que la mitad están en Asia. En Iberoamérica un 56% de la población está ya conectada. Tres de cada cuatro europeos y nueve de cada diez norteamericanos están contectados.

WORLD INTERNET USAGE AND POPULATION STATISTICS
NOVEMBER 30, 2015 - Update

World Regions	Population (2015 Est.)	Population % of World	Internet Users 30 Nov 2015	Penetration (% Population)	Growth 2000-2015	Users % of Table
Africa	1,158,355,663	16.0 %	330,965,359	28.6 %	7,231.3%	9.8 %
Asia	4,032,466,882	55.5 %	1,622,084,293	40.2 %	1,319.1%	48.2 %
Europe	821,555,904	11.3 %	604,147,280	73.5 %	474.9%	18.0 %
Middle East	236,137,235	3.3 %	123,172,132	52.2 %	3,649.8%	3.7 %
North America	357,178,284	4.9 %	313,867,363	87.9 %	190.4%	9.3 %
Latin America / Caribbean	617,049,712	8.5 %	344,824,199	55.9 %	1,808.4%	10.2 %
Oceania / Australia	37,158,563	0.5 %	27,200,530	73.2 %	256.9%	0.8 %
WORLD TOTAL	7,259,902,243	100.0 %	3,366,261,156	46.4 %	832.5%	100.0 %

Por países, en América Latina (http://www.internetworldstats.com/stats10.htm), y con referencia a usuarios más avanzados con interactuación 2.0 (Facebook), los datos se muestran en la siguiente tabla. Costa Rica (88%), Ecuador (con un gran aumento, duplicando el acceso sólo en tres años, un 84%) Argentina (80%), Chile (72 %), Uruguay (65%), Venezuela (61%) y Colombia (59%) destacan entre los países de mayor penetración. Diversos países de Centroamérica destacan por el estaso acceso, además de Cuba (30%), Bolivia (39%), Paraguay (43%).

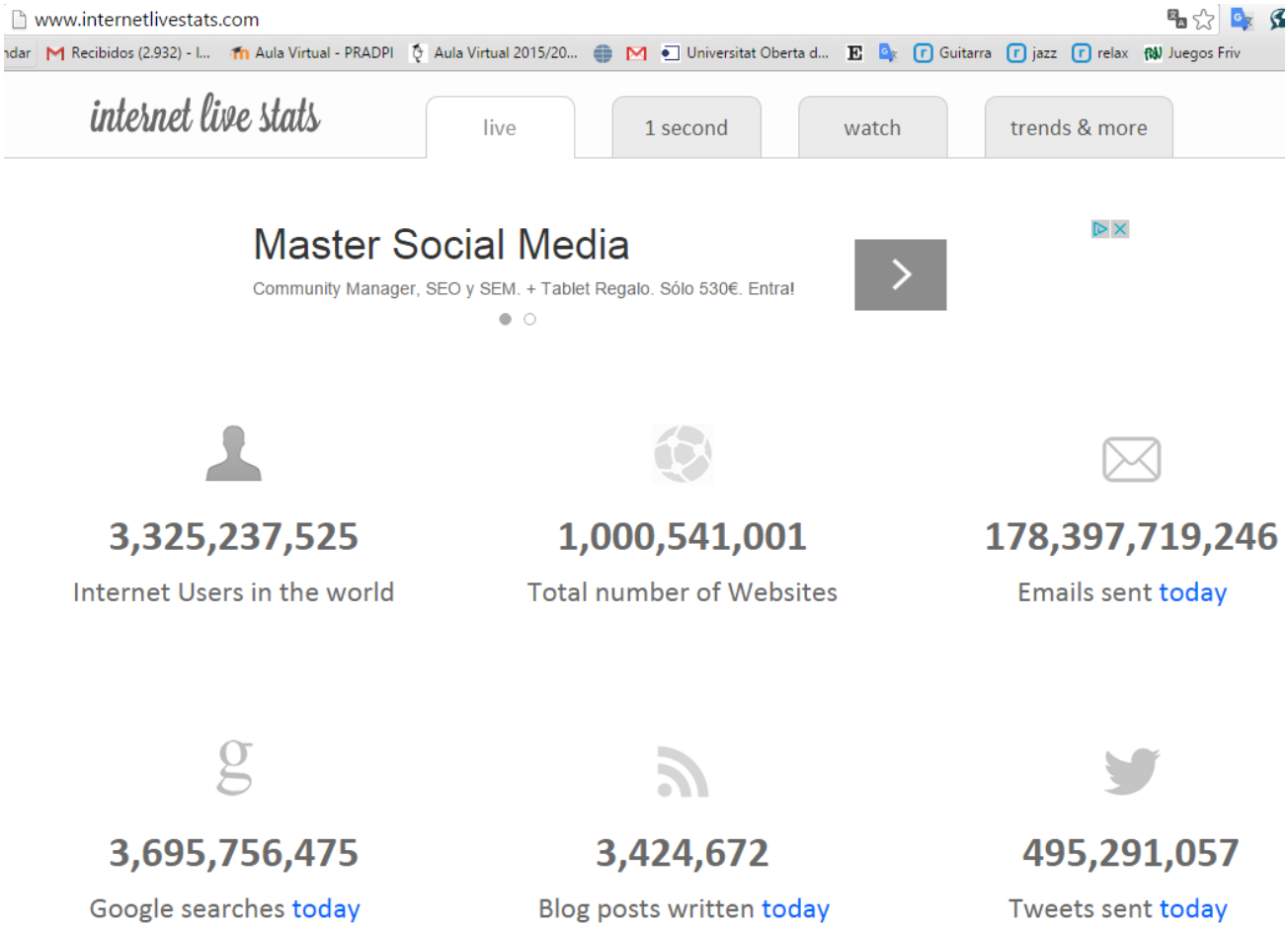
Latin American Internet Users - November 2015					
COUNTRIES / REGIONS	Population (Est. 2015)	Internet Users, 30-Nov-15	% Population (Penetration)	Users % in Region	Facebook 15-Nov-15
Argentina	43,431,886	34,785,206	80.1 %	10.3 %	27,000,000
Bolivia	10,800,882	4,214,504	39.0 %	1.2 %	3,800,000
Brazil	204,259,812	117,653,652	57.6 %	34.7 %	103,000,000
Chile	17,508,260	12,667,226	72.3 %	3.7 %	11,000,000
Colombia	48,203,405	28,475,560	59.1 %	8.4 %	24,000,000
Costa Rica	4,814,144	4,236,443	88.0 %	1.3 %	2,800,000
Cuba	11,031,433	3,309,430	30.0 %	1.0 %	n/a
Dominican Republic	10,478,756	6,054,013	57.8 %	1.8 %	3,800,000
Ecuador	15,868,396	13,471,736	84.9 %	4.0 %	8,700,000
El Salvador	6,141,350	2,900,000	47.2 %	0.9 %	2,900,000
Guatemala	14,918,999	4,700,000	31.5 %	1.4 %	4,700,000
Honduras	8,746,673	2,400,000	27.4 %	0.7 %	2,400,000
Mexico	121,736,809	60,000,000	49.3 %	17.7 %	60,000,000
Nicaragua	5,907,881	1,000,000	27.1 %	0.5 %	1,000,000
Panama	3,657,024	1,899,892	52.0 %	0.6 %	1,500,000
Paraguay	6,783,272	2,916,807	43.0 %	0.9 %	2,600,000
Peru	30,444,999	16,000,000	52.6 %	4.7 %	16,000,000
Puerto Rico	3,598,357	2,834,786	78.8 %	0.8 %	2,100,000
Uruguay	3,341,893	2,200,000	65.8 %	0.6 %	2,200,000
Venezuela	26,457,369	16,276,611	61.5 %	4.8 %	12,000,000
TOTAL	598,131,600	338,595,866	56.6 %	100.0 %	292,100,000

En España en 2015, los conectados a internet son el 77% (38.7% en 2006), con 35,7 millones de usuarios de Facebook, ocupando un lugar medio en la Unión Europea frente a países como Holanda (95%) o Noruega (96 %).

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 y por ello son significativos los datos de uso de la popular red social.

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.

Datos de http://www.internetlivestats.com/ indican que hay mil millones de webs, 15 billones (europeos) de mails diarios, 1600 millones de usuarios activos de Facebook, 45 billones de Tuits al año, 340 millones de tuiteros activos, entre otros datos.



91. 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, esto es, la obligación de usar el gobierno abierto. Esto no es en modo alguno impensable, siendo que desde los años 90 ya hay obligaciones. La ya derogada Ley 11/2007 española en su artículo 27. 6º ya permitió que un reglamento pudiera obligar a *"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."* Al tiempo, se afirmaba la obligación del Estado de garantizar "e*n todo caso"* el acceso a los servicios electrónicos a toda persona. Dando un paso más en este camino de imposición, el artículo 14 la nueva Ley 39/2015 permite ya "por defecto" imponer la e-administración a toda persona jurídica, representantes de individuos o funcionarios públicos sin justificación alguna y a las personas físicas con los anteriores requisitos. Es más, pese a que el artículo 12 impone a la Administración la "asistencia en el uso de medios electrónicos a los interesados", no hay obligación de asistencia alguna precisamente a todo sujeto obligado, quien, probablemente, será quien más la necesite.

Pese a que en ocasiones puedan surgir dudas o problemas, 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.

Un detalle a tener en cuenta en esta cuestión, es que cada vez es más generalizada la obligación para todo ciudadano de usar internet para cumplimentar un formulario o plantilla, para así grabar los datos del procedimiento del que se trate. Sin embargo, este uso obligatorio de formulario o plantilla no se considera como imposición de e-administración porque el documento final se genera en papel para ser firmado por el administrado. No obstante, se trata de una obligación de uso de internet que sí que puede generar una barrera para determinados colectivos y, por lo tanto, deben regir las garantías de una imposición de Administración electrónica.

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".

Más recientemente destacan dos importantes documentos y declaraciones internacionales. Entre los mismos a mu juicio destaca por su calidadd la

Declaración conjunta sobre libertad de expresión e internet de 2011 por altas instituciones internacionales de libertad de expresión, incluyendo la ONU y la OEA.

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

Al respecto del acceso a internet destaca el apartado 6, donde se afirma la "obligación positiva de facilitar el acceso universal a Internet" afirmándose unos mínimos de acción ("establecer mecanismos regulatorios ", creacción de "puntos de acceso público", asegurar "el acceso equitativo a Internet para personas con discapacidad y los sectores menos favorecidos" y para todo ello, "adoptar planes de acción detallados".

También en 2011, destaca el Informe del Relator Especial a la Asamblea de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, uno de los autores del documento anterio, de 16.5.2011, en el que se centra en el "derecho de todas las personas a buscar, recibir y difundir información e ideas de todo tipo por Internet."

http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27&Lang=S

Respecto del acceso a internet se formula la obligación de (nº 85) "elaborar una política eficaz y concreta en consulta con personas de todos los sectores de la sociedad, entre ellos el sector privado, y con los ministerios gubernamentales competentes, a fin de que Internet resulte ampliamente disponible, accesible y asequible para todos los sectores de la población."

Obviamente, un derecho fundamental de acceso a internet no implica la gratuidad del acceso de modo generalizado, sino su asequibilidad y, en su caso, acceso gratuito en determinados supuestos o, especialmente, para colectivos o territorios que tengan singulares barreras económicas de acceso.

En 2001 la Constitución griega introdujo su artículo 5 A que reconocía que "'2. Todas las personas tienen el derecho de participar en la sociedad de la información. Constituye una obligación del Estado la facilitación del acceso a la información transmitida vía electrónica, así como de la producción, el intercambio y la difusión de la misma, siempre en observancia de las garantías de los artículos 9, 9A y 19."

En la Unión Europea el acceso a internet se garantizó especialmente merced al artículo 3. 1º de la Directiva 2002/22/CE. El TS alemán el 24 de enero de 2013 afirmó que internet se ha convertido en algo "esencial para la vida".

Como hito –simbólico- mencionable, el 30 de julio 2010 un fallo de la Corte Suprema de Costa Rica declaró: "Sin temor a equívocos, se puede decir que estas tecnologías han impactado la forma en que los seres humanos se comunican, lo que facilita la conexión entre las personas y las instituciones de todo el mundo y la eliminación de las barreras de espacio y el tiempo. En este momento, el acceso a estas tecnologías se convierte en una herramienta básica para facilitar el ejercicio de los derechos fundamentales y la participación democrática y el control ciudadano, la educación, la libertad de pensamiento y de expresión, el acceso a la información y los servicios públicos en línea, el derecho a comunicarse con gobierno electrónico y transparencia administrativa, entre otros. Esto incluye el derecho fundamental de acceso a estas tecnologías, en particular, el derecho de acceso a la Internet o la World Wide Web".

Por su relevancia mundial es menester hacer referencia a la Declaración del Presidente de los Estados Unidos Barack Obama de 10 de noviembre de 2014 : "Un internet abierto es esencial para la economía estadounidense, y cada vez más en nuestro modo de vida. Reduciendo el costo de lanzar una nueva idea, encendiendo nuevos movimientos políticos, y uniendo cada vez más a las comunidades, internet ha sido uno de las influencias más democratizadoras que el mundo nunca ha conocido." Siguiendo su propuesta, en febrero de 2015 la Comisión Federal de Comunicaciones de

Estados Unidos declaró internet como un "bien público" y no como un servicio de información, lo cual implica, entre otras cosas, una mayor garantía de acceso a la red tal y como hoy se concibe.

En España el *ius comunicationis* ya tuvo 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.

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.

a) 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.

b) 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. En este sentido cabe mencionar la llamada Teoría 90-9-1 formulada en 2006 por Jakob Nielsen https://es.wikipedia.org/wiki/Teor%C3%ADa_90-9-1 . Se denomina también "Desigualdad Participativa" en virtud de la que un 90% de los usuarios observan, pero no participan, un 9% lo hacen esporádicamente y sólo a un 1% de los usuarios se le atribuye más del 90% de las participaciones ("superusuarios" o *Heavy Contributors*)

La atribución de una sobre representación al activista por medio de las TIC vendría a ser como atribuir una mayor significación política a los mensajes políticos que suelen decorar el entorno urbano, por lo general nada moderados.

c) 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.

93. 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. Las normativas de retención de datos de tráfico y geolocalización son cada vez más habituales medios para el control de internet y la obtención de pruebas, y más con los atentados y amenazas islamistas de los últimos años.

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 entonces 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 expresióna

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, criptografía, 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 condenó 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. Esta condena luego fue revocada por un tribunal superior

El Reglamento (UE) nº 211/2011, regula la novedosa iniciativa ciudadana europea. Luego se hará referencia al mismo, si bien cabe llamar ahora la atención sobre que buena parte de esta normativa se centra en la obligada protección de datos personales respecto de los millones de ciudadanos europeos que pueden apoyar iniciativas políticas. La sensibilidad de los datos vinculados a la ideología política exige medidas de seguridad por lo general altas, así como prevenciones como la llamada seguridad por diseño o por defecto que deben realizar profesionales de la seguridad informática. Así lo exige, por ejemplo, el nuevo Reglamento europeo de protección de datos que se aprueba en 2016.

Más allá de las obligaciones concretas de seguridad exigibles por normativa de protección de datos, cabe tener en cuenta un presunto "derecho a la criptografía". Aunque la cuestión excede con mucho al objeto concreto de este escrito, especialmente tras las revelaciones por Snowden en 2013 de espionaje masivo por la NSA y la presunta colaboración de los grandes de internet, no hay que obviar la creciente demanda de productos tecnológicos que confieren seguridad y confidencialidad. Ello se logra en muchas ocasiones a través de sistemas de cifrado y códigos. 2016 es posiblemente el año del –ya viejo- debate sobre la ponderación del derecho a usar y fabricar medios de cifrado y las necesidades de seguridad y defensa por parte de los Estados (a este respecto cabe tener en cuenta los conflictos de Apple para no cambiar su sistema de protección de los smartphones frente a los servicios policiales, o la encarcelación en febrero de 2016 en Brasil de un responsable de Facebook-Whatssap por no facilitar el acceso a los mensajes por estar encriptados y porque además no se conservan por la compañía.

ADMINISTRACIÓN ELECTORAL Y TIC, LAS TIC EN LAS CAMPAÑAS ELECTORALES

94. Administración electoral y la creciente emergencia de las TIC en campaña

El empleo de las TIC 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 TIC. Así, es posible la comprobación electrónica de la corrección del censo por los ciudadanos electrónicamente.

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 TIC 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]. Las redes sociales causaron furor en las elecciones presidenciales colombianas de 2010 y en España en 2011, la resistencia en internet a la legislación de control de contenidos ilícitos está en el germen del nacimiento del llamado movimiento del "15-m", que de la red dio posteriormente el "salto" a la calle.

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. Desde 2006, movimientos sociales en la red han desembocado, por ejemplo, en el "Tea Party" (http://en.wikipedia.org/wiki/Tea_Party_movement), que en ocasiones parece dominar la agenda y la elección misma de cantidatod por el Partido Republicano.

Más allá del voto electrónico, cabe tener en cuenta la implantación de sistemas electrónicos para la administración del escrutinio y comunicación de resultados. Por ejemplo, el "Colegio Administrado Electrónicamente" implantado en España las Elecciones al Parlamento Europeo del 7 de junio de 2009[5], desde 2011 hasta la fecha, denominado "Mesa Administrada Electrónicamente"[6]. Se trata de un sistema de herramientas informáticas de apoyo a la mesa electoral. Su uso no requiere especial formación técnica. El sistema facilita la confección automática del acta de constitución de la mesa, facilita el escrutinio de votos y si se incorpora la firma electrónica y un canal seguro, la transmisión de resultados a las autoridades electorales correspondientes.

95. Las típicas prohibiciones previas a los comicios electorales y su exigencia en internet

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).

https://www.boe.es/buscar/pdf/2007/BOE-A-2007-8181-consolidado.pdf

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

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

[5] http://elecciones.mir.es/europeas2009/cae.html La cobertura jurídica se la concede, en parte, la Orden INT/1025/2009, de 28 de abril. Asimismo, El citado *Elecciones Parlamento Europeo 2009. Manual* ... para el CAE en las Elecciones del 7 de junio de 2009 fue supervisado por la Junta Electoral Central el 2 de abril de 2009.

[6] Puede seguirse una explicación sencilla virtual en:
http://elecciones.mir.es/generales2011/Visitas_virtuales/Mesa_Administrada_Electronicamente_(MAE)/Mesa_Administrada_Electronicamente_(MAE).htm
El manual de MAEs en http://elecciones.mir.es/locales2011/almacen/pdf/MMM%20Huesca%20definitivo.pdf
También en http://goo.gl/up2Tk

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.

La difusión de este sondeo prohibido ya ha pasado a ser una nueva “tradición” electoral, siendo que los medios de comunicación del país donde rige la prohibición no tienen estupor alguno en reenviar a la información del sondeo electoral prohibido.

VOTO ELECTRÓNICO: TIPOS Y GARANTÍAS

96. 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)

PE2D09-DD1

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

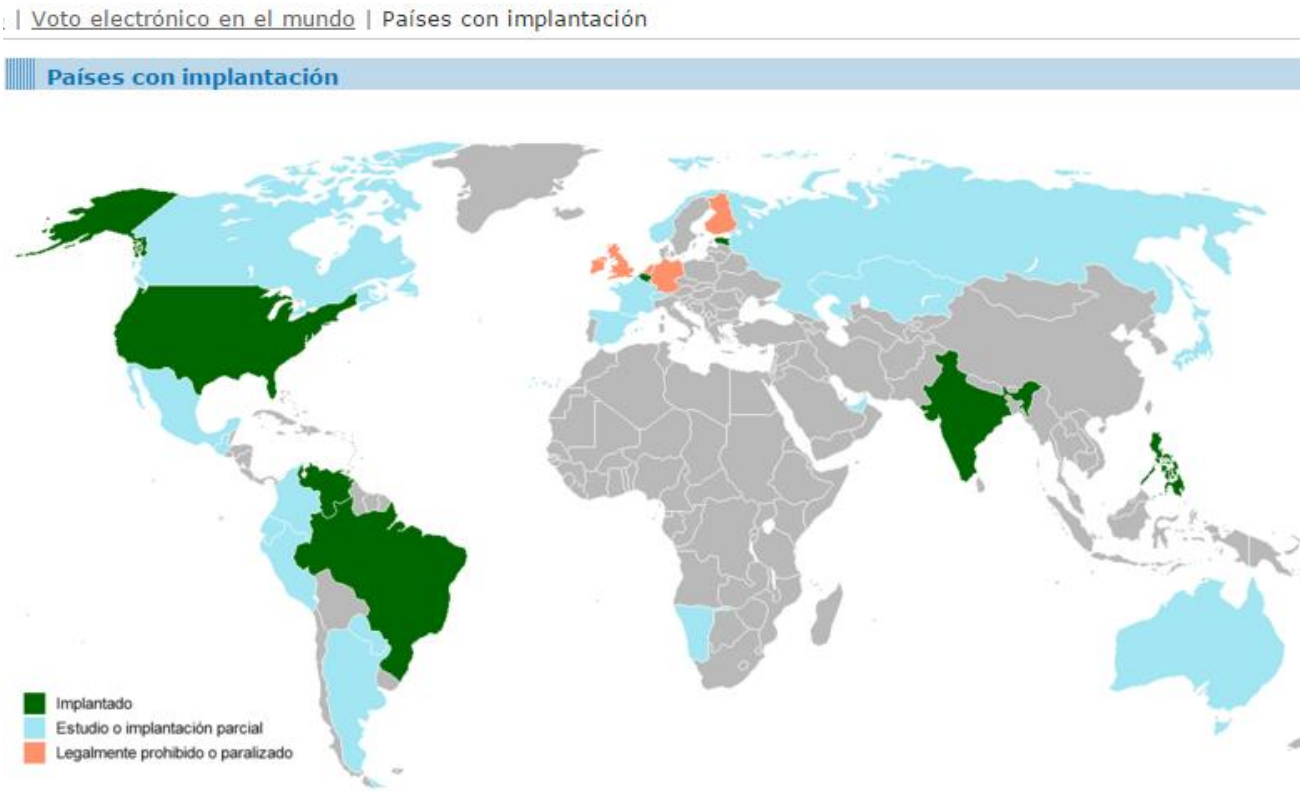
directamente en la memoria de la urna electrónica (esta modalidad se prevé en Perú, República Dominicana, Panamá y Colombia).

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.

En el siguiente mapa puede verse la evolución de este tipo de voto en el mundo: http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_impl_c.htm



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 TIC 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 o *Whatssap* 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, en 2015 ya un 30% de los votantes lo hacen a distancia a través de internet. Requieren su documento de identidad, la firma electrónica y un contraseña en un ordenador dotado de un lector electrónico de tales elementos (ver http://estonia.eu/about-estonia/economy-a-it/e-voting.html) . 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. En este punto, existen informes independientes sobre la seguridad de estos procesos de votación en Estonia que afirman estar "alarmados" por la falta de seguridad. https://estoniaevoting.org/

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.

97. 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 resolución se revisa cada dos años y se espera actualizar en 2016. En 2010 se elaboró un manual sobre voto electrónico.[7]

[7] http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/CoEvotingHandbook_en.pdf

sta 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.

98. 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.

99. 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).

100. 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"[8]. Si el escrutinio manual puede hacerlo incluso un analfabeto, el escrutinio electrónico requiere de conocimientos. Señala Jones[9] 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)[10] 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 Ley Fundamental) ponderadas respecto de los intereses en juego a favor del e-voto.

En dirección contraria, cabe mencionar la muy fundamentada y amplia sentencia de 150 folios pronunciada por el Tribunal Electoral del Poder Judicial de la Federación mexicana el 12 de enero de 2012. (http://goo.gl/zvuBo) Esta sentencia da el visto bueno al uso del voto electrónico para los electores del Distrito Federal en el extranjero para las elecciones locales de 2012 para la Jefatura de Gobierno del Distrito federal. Entre otros aspectos, esta sentencia destaca porque reafirma el necesario papel de control del e-voto por los partidos políticos:

"a pesar de que expresamente no se prevea la participación de los partidos políticos en todas y cada una de las etapas del procedimiento de votación por internet, en la medida que resulte razonable y no se atente contra los principios rectores de la función electoral y las características del sufragio, se debe permitir su calidad de observadores o verificadores"

Ya son diversas las sentencias sobre e-voto en el mundo[11]. 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.

---

[8] 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

[9] 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

[10] 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

[11] Al respecto destaca la obra de DRIZA MAURER, Ardita y BARRAT, Jordi, *E-voting Case Law: a Comparative Analysis*, Publishing House, 2015.

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"[12]. 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, que sigue activo hasta 2016: 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

Videos –parodia contra el e-voto

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

Homer Simpson tries to vote for Obama
https://www.youtube.com/watch?v=EV_c1-YTk8M

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

EJERCICIO ELECTRÓNICO FORMAL E INFORMAL DE INICIATIVA LEGISLATIVA POPULAR Y DEL DERECHO DE PETICIÓN

101. 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 2016 son más de 40 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.

A partir de ello se han desarrollado en España plataformas puestas a disposición del público usables con el DNI electrónico:

http://www.openilp.org/

https://www.mifirma.com/

No obstante, hasta 2016, la experiencia es discreta, por no decir que un rotundo fracaso.

En América Latina no cabe descartar mecanismos de apoyos electrónicos con validez oficial como pudiera ser recoger apoyos electrónicamente en plantillas en una aplicación que exigiera, por ejemplo, subir la fotografía de la cédula o identificación del firmante. Pese a las probabilidades de falseamiento que pueden darse, creo que estos riesgos son mayores en la recogida tradicional de firmas únicamente señalando el número de cédula o identificación de la persona.

Cabe destacar el Reglamento (UE) nº 211/2011, sobre la iniciativa ciudadana europea proyecta la iniciativa legislativa popular al ámbito supranacional y, por lo que aquí interesa también es revolucionaria por estar pensada esencialmente para internet. Se regula el sistema de recogida de apoyos ciudadanos a través de páginas web, es más, además de una extensa regulación se obligó a que la propia Comisión Europea dispusiera al público un software de código abierto para hacer efectiva la recogida de apoyos.

La novedosa norma regula los mecanismos de identificación necesarios, la protección de datos y la seguridad en el almacenamiento y posterior destrucción de los apoyos electrónicos, la verificación electrónica de los apoyos recibidos por las autoridades.

Cabe seguir la información oficial de la Comisión
http://ec.europa.eu/citizens-initiative/public/welcome
Y desde abril de 2012 se han lanzado las primeras Iniciativas Ciudadanas Europeas, siendo tres las que han prosperado.

Sobre la esta novedosa institución puede seguirse el texto de una ponencia, así como el breve audio de 10 minutos en

http://www.cotino.net/2011/07/295/

102. 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, el más famoso en español: www.change.org). Que se trate de un ejercicio informal de derechos no resta el valor político que puedan tener estas iniciativas o movimientos.

TIC, TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA POR EL PÚBLICO

103. El derecho acceso a la información pública, un nuevo derecho fundamental

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

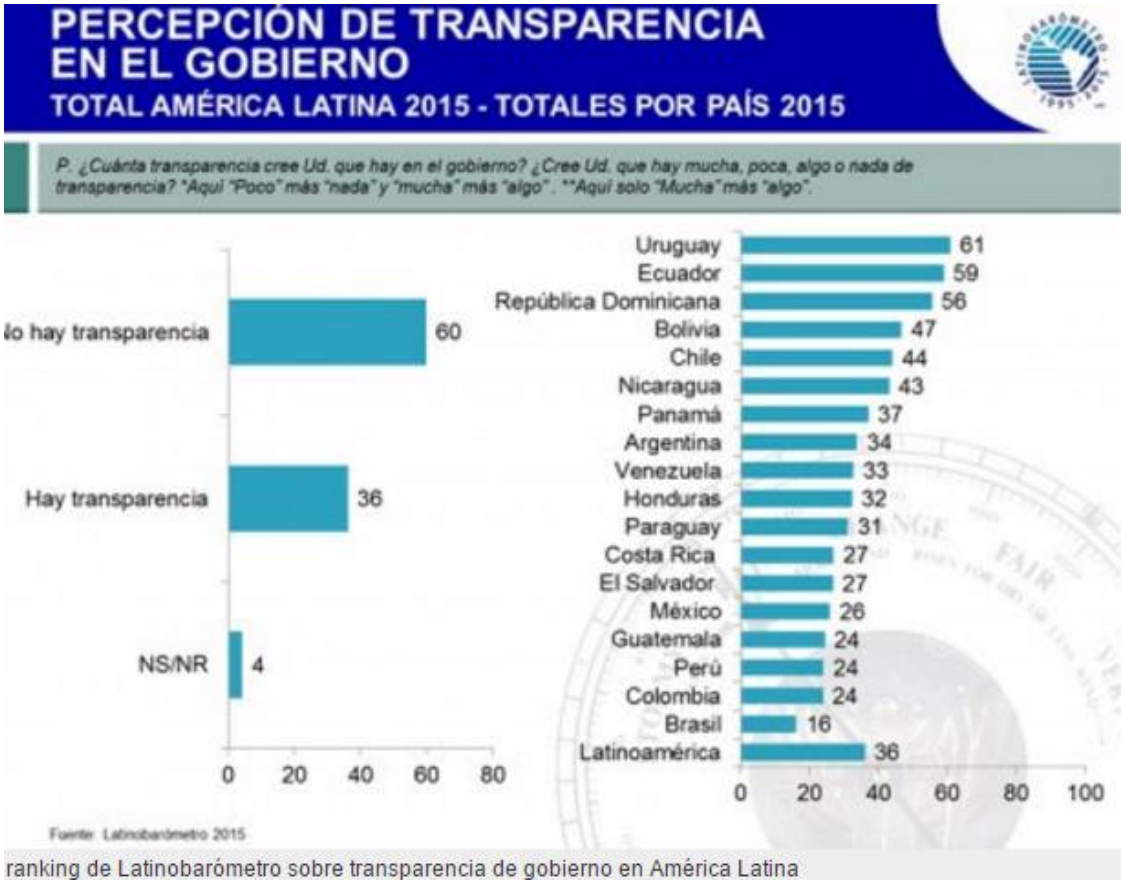
La Directriz 15 de la Recomendación de e-democracia de 2009 es clara:

"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 TIC 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 TIC. 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 habituales en América Latina desde 2002, aunque la percepción de la transparencia no se corresponde con los países pioneros en su regulación (como México o Perú, por ejemplo).



ranking de Latinobarómetro sobre transparencia de gobierno en América Latina

España ha sido el último país de la Unión Europea en regular de forma global la transparencia, a salvo de Chipre. Ha habido que esperar a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887) a la que han seguido numerosas leyes autonómicas de desarrollo.

La sentencia de la Corte Interamericana del caso Claude Reyes y Otros v. Chile, de 19 septiembre 2006 afirmó que el acceso a la información pública es un derecho fundamental en el marco de la libertad de expresión. Luego ha sido ratificada en el caso Gomes Lund y otros vs. Brasil de 24 de noviembre de 2010. Ese mismo año se adoptó la Ley Modelo Interamericana sobre Acceso a la Información en la OEA, aprobada en junio de 2010. El TEDH en Europa ha sido algo más tímido en el reconocimiento de este derecho fundamental, si bien la Carta de derechos fundamentales de la Unión Europea reconoce el de acceso a la información pública como derecho autónomo en su artículo 42 (en vigor desde 2009). 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.

104. Obligaciones de transparencia activa y obligación de información pública en la red

La legislación norteamericana y las legislaciones de transparencia que ya se han generalizado en los últimos años en el mundo, como la mexicana no sólo reconocen la transparencia pasiva, esto es, la posibilidad de que el ciudadano solicite el acceso a la información pública. Asimismo la transparencia exige que la información no espere a ser solicitada por el ciudadano y se la publicación de unos items de información mínima que debe brindarse por las Administraciones en sus portales de transparencia. Así, se imponen importantes obligaciones jurídicas de "publicidad activa", es decir, de mínimos de información obligatorios de relevancia jurídica, política, social o económica que deben ser satisfechos en portales de transparencia. Todo ello se fundamenta en el mito de Bentham de que cambiamos nuestro comportamiento cuando sabemos que somos observados, lo cual es teóricamente predicable también de la Administración.

Además, no sólo se trata de poner a diposición la información, sino que determinar los formatos y soportes electrónicos de esta información, para que la sociedad civil pueda reutilizarla es también decisivo (Open Data, datos abiertos). El legislador debe regular también estos aspectos técnicos. De hecho, la nueva versión de la Directiva 2003/98/CE, de 17 de noviembre de 2003 de reutilización de la información pública modificada por la Directiva 2013/37/UE, de 26 de junio de 2013 impone que los datos se publiquen en formatos estándares, abiertos y procesables legibles por las máquinas de modo automatizado, con la mayor granularidad posible para que la reutilización pueda ser eficaz (art. 5 de la Directiva de 2013). Puede decirse que el acceso a la información pública en formatos abiertos se está conformando como un derecho que sigue la estela de la información pública, puesto que se va generando el derecho a solicitar la información en formatos abiertos y, al igual que la transparencia activa, se va generalizando la difusión activa de datos abiertos en portales especializados, si bien, hoy por hoy no es una obligación, a diferencia de la transparencia activa.

105. 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 y hay que tener en cuenta la confianza legítima del ciudadano. 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 que pasó a ser también luego autoridad de protección de datos (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (www.ifai.org.mx/). Pasó así a seguir 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 cambio, países como España han preferido tener dos autoridades independientes, una para la

protección de datos (www.agpd.es) y un Consejo de la Transparencia (www.consejodetransparencia.es) .

TIC 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 TIC 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, fueron clásicos los informes mundiales de Steven Clift http://www.publicus.net/e-government/ en los años 2000 y hoy día cabe seguir las mejores prácticas de participación, por ejemplo, en la Alianza para el Gobierno Abierto.

En todo caso, las posibilidades de la TIC 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.

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": entre los que son clásicos Arabia Saudí, Birmania, China, Corea del Norte, Cuba, Egipto, Irán, Siria, Túnez, Turkmenistán, Uzbekistán y Vietnam. Se 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. Es ya un clásico el informe de "Enemigos de internet" de Reporteros Sin Fronteras:

http://www.rsf-es.org/grandes-citas/dia-contra-censura-en-internet/

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.

108. 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.

Destaca la ya mencionada Declaración conjunta sobre libertad de expresión e internet de 2011 por altas instituciones internacionales de libertad de expresión, incluyendo la ONU y la OEA.

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

En la misma se afirman unos "principios generales" (I) que son plenamente suscribibles:

a La libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación. Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba "tripartita").

b. Al evaluar la proporcionalidad de una restricción a la libertad de expresión en Internet, se debe ponderar el impacto que dicha restricción podría tener en la capacidad de Internet para garantizar y promover la libertad de expresión respecto de los beneficios que la restricción reportaría para la protección de otros intereses.

c. Los enfoques de reglamentación desarrollados para otros medios de comunicación —como telefonía o radio y televisión— no pueden transferirse sin más a Internet, sino que deben ser diseñados específicamente para este medio, atendiendo a sus particularidades.

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).

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. En esta línea, las conclusiones del caso Google vs AGPD) son rotundas al afirmar que

"Poner contenidos a disposición del público en internet equivale, como tal, a la libertad de expresión […] La publicación en la web es un medio para que los particulares participen en debates o difundan sus propios contenidos, o contenidos cargados por otros, en internet" (nº 122)

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

En su momento se abordó el "ius comunicationis" como derecho fundamental. Hoy día no pasa de las declaraciones internacionales la obligación de que el Estado que facilite el acceso a la red. Ello no obsta para que una medida de restricción del acceso a las TIC 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.

Asimismo, no puede ordenarse a los prestadores que bloqueen contenidos sin discriminar entre los que son lícitos y los ilícitos y para que se adopten medidas de bloqueo es necesaria una regulación legal que dé previsibilidad, certeza y garantías suficientes en la materia. La STEDH de 18 de diciembre de 2012 en el asunto Ahmet Yıldırım c. Turquía ha sido la primera de este alto tribunal que aborda la libertad de expresión en internet . Se entiende que viola la libertad de expresión la imposición –judicial- de medidas de bloqueo de acceso a contenidos en internet que no discriminaron contenidos del sitio de internet implicado en un proceso penal y los de otros sitios del servicio Google sites con contenidos al margen de dicho proceso. El TEDH aprovecha la ocasión para fijar algunos parámetros de la regulación del bloqueo de contenidos en internet (aps. 64 y ss.). Más allá de que sea necesaria una resolución judicial, un elemento esencial es que la ley ha de dejar bien claros los presupuestos, condiciones y requisitos que se han de dar para una restricción grave de la libertad de expresión e información como lo es cerrar, bloquear o impedir acceso a páginas web. Y por lo general las leyes no regulan con precisión estas cuestiones.

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

Además de lo indicado, no puede imponerse a los prestadores o intermediarios que establezcan controles o filtrados técnicos de contenidos en internet sin distinguir entre contenidos lícitos o ilícitos. Las sentencias del TJUE de 24 de noviembre de 2011, Asunto C-70/2010, Scarlet Extended vs SABAM y Asunto C-360/10 SABAM vs Netlog de 16 de febrero de 2012 no permiten que judicialmente se impongan controles y filtrados técnicos y preventivos a prestadores de servicios y redes sociales para evitar la comisión de ilícitos de propiedad intelectual y protección de datos. El TJUE considera que deben prevalecer la libertad de expresión y la protección de los usuarios que serían controlados y rastreados, así como la libertad de empresa frente a la imposición de estos controles. Se afirma la vulneración de la libertad de información, "dado que se corre el riesgo de que el citado sistema no distinga suficientemente entre contenidos lícitos e ilícitos, por lo que su establecimiento podría dar lugar al bloqueo de comunicaciones de contenido lícito". Ahora bien, en 2014 se ha afirmado que sí que es posible que un juez obligue a bloquear contenidos concretos lesivos de la propiedad intelectual.

La citada Declaración conjunta sobre libertad de expresión e internet de 2011, aun sin valor jurídico en su apartado 6 dispone:

"b. La interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún

caso, ni siquiera por razones de orden público o seguridad nacional. Lo mismo se aplica a las medidas de reducción de la velocidad de navegación de Internet o de partes de este.
c. La negación del derecho de acceso a Internet, a modo de sanción, constituye una medida extrema que solo podría estar justificada cuando no existan otras medidas menos restrictivas y siempre que haya sido ordenada por la justicia, teniendo en cuenta su impacto para el ejercicio de los derechos humanos."

Sin embargo, en las leyes no es claro 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). La ley española de propiedad intelectual actualizada en 2014 ya regula de modo concreto el cierre de webs de enlaces bajo fuertes sanciones, así como mandamientos a colaboradores como servicios de pago para no prestar servicios a webs que la Administración declara prohibidas. 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[13], 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 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. Cabe adelantar que este criterio es el determinante para considerar si hay vulneración o no de los derechos de la privacidad y protección de datos del afectado. Así por ejemplo, no se pueden utilizar datos personales que están disponibles en una página web si no hay interés público en la información que se deriva de este tratamiento.

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

[13] 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).

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.

Cabe también tener en cuenta la doctrina de la posición preferente (Estados Unidos) o el reforzamiento de las libertades informativas a través de la llamada garantía institucional (España u otros países de Europa) de la "opinión pública libre", dado que ésta es esencial para el sistema democrático. Clásicamente se atribuye esta posición preferente o la garantía institucional cuando la libertad de expresión o información se ejerce a través de medios de comunicación social. Pues bien, considero que debe reconocerse también esta especial intensidad de protección a los grandes prestadores de servicios de internet (Google, Youtube, Twitter, Facebook, etc.), que hoy día son totalmente esenciales para el sistema democrático.

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 Mathis 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? . De Wikileaks a Mexicoleaks. Una cuestión importante que va a dejar de serlo

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, así como el uso de redes sociales, donde hay perfiles de absoluta relevancia. La cuestión básica es que cualquiera de los tres mil trescientos millones de usuarios de internet a inicios de 2016 puede revelar información de interés público de procedencia o contenido ilegal. Entonces la cuestión es si se puede obligar al internauta que revela la información que señale quién es su fuente. Si no está obligado a revelar la fuente, como los periodistas, la difusión de información ilícita o de origen ilícito queda pues protegido por la libertad de expresión e información.

Los blogueros 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 van protegiendo el derecho a no revelar las fuentes de información o de proteger el anonimato (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).

La cuestión puede generalizarse a partir de la experiencia de *Wikileaks* que indica que internet puede ser un medio de filtración de información y de denuncia idóneo, especialmente si no es obligatorio indentificar la fuente de información que ha filtrado el secreto al periodista o al divulgador de información en internet. Y no hay que pensar en filtraciones masivas, sino en la generalización de medios de filtración locales para alcanzar relevancia e importancia también local. Así, por ejemplo, cabe tener en cuenta www.mexicoleaks.mx

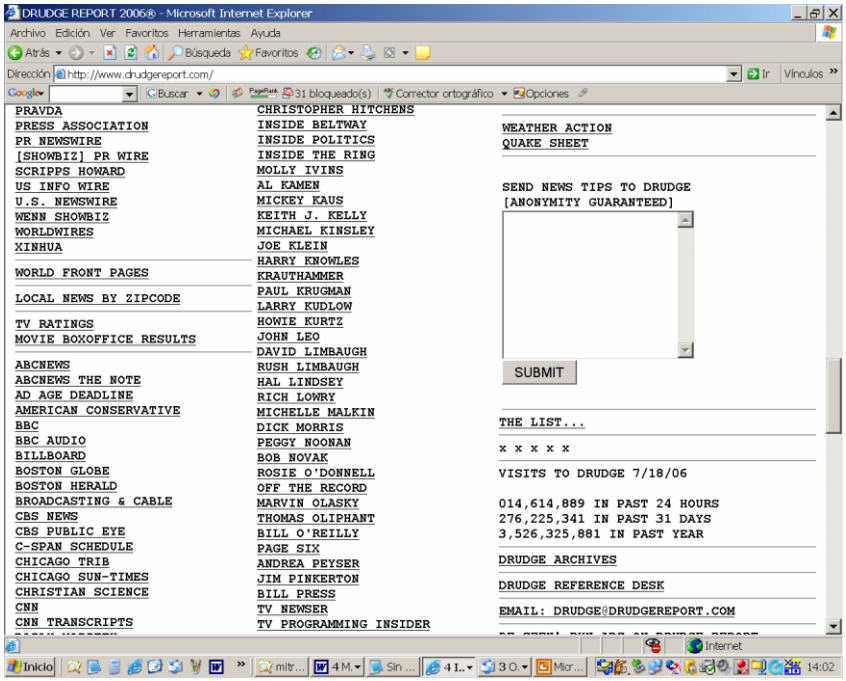
En el caso Obsidian Finance Group, LLC v. Cox en sentencia 2011 de la Corte federal del Distrito de Oregón condenó a una bloguera porque no tenía este privilegio por no reunir las características de periodista. La sentencia ha sido parcialmente ratificada y revocada por la Corte del Noveno Circuito el 17 de enero de 2014, que sigue la línea de tratar de forma igual a los medios y a los ciudadanos que ejercen la libertad de expresión.

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

Pues bien, esta cuestión de importancia ni siquiera había sido resuelta, parece que va a quedar obsoleta. Y es que parece que se van a generalizar medios y plataformas de denuncia y filtración que hacen que técnicamente sea imposible conocer el origen de la fuente de la información, por quedar tecnológicamente anónima para todo el mundo. Así las cosas, quienes reciben la información, constatan su veracidad y su interés público y la divulgarán al público. Y cuando en su caso les pregunten la procedencia de la revelación del secreto, simplemente tendrán que probar que la plataforma hace imposible conocer tal extremo, por lo que no podrán, literalmente, revelar la fuente.

Si se quiere evitar este flujo de información de interés público al público, sólo quedará prohibir la disposición de estas tecnologías y plataformas para impedir el filtrado. Considero que dicha prohibición general no puede darse en un Estado que proteja la libertad de expresión.

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



www.filtrala.org (como www.mexicoleaks.mx) es una "Plataforma independiente de denuncia ciudadana a través de la cual cualquier persona puede revelar información de interés público a medios de comunicación y organizaciones de la sociedad civil de manera segura y anónima". Pertenece a una red mundial de Whistleblowing para la denuncia de corrupción y otras ilegalidades.

110. 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. El TEDH en el caso Delfi vs Estonia de 10 de octubre de 2013 condenó a un medio digital por no vigilar y filtrar los contenidos de los usuarios lectores del mismo, siendo que además tenía un sistema de detección automática de insultos y difamaciones además de un mecanismo de denuncia de contenidos improcedentes por cualquier usuario que llevaba a la revisión humana de los contenidos ilegales. La sentencia de Gran Sala del TEDH el 16 de junio de 2015 ha ratificado el criterio, si bien, ha ceñido la responsabilidad del intermediario a los "medios de comunicación en línea", pero no en general para todo intermediario o red social. Se trata de una línea bien preocupante para la libertad de expresión. Y esta línea es diametralmente opuesta al modelo en EEUU. Ahí es relativamente claro que no se puede hacer responsable a los intermediarios por los contenidos que alojan ni tienen obligación de revisión de tales contenidos hasta que no sean denunciados.

La tantas veces citada Declaración de libertad de expresión en internet de 2011 al respecto señala que:

2. a. Ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo ("principio de mera transmisión").

b. Debe considerarse la posibilidad de proteger completamente a otros intermediarios, incluidos los mencionados en el preámbulo, respecto de cualquier responsabilidad por los contenidos generados por terceros en las mismas condiciones establecidas en el párrafo 2(a). Como mínimo, no se debería exigir a los intermediarios que controlen el contenido generado por usuarios y no deberían estar sujetos a normas extrajudiciales sobre cancelación de contenidos que no ofrezcan suficiente protección para la libertad de expresión (como sucede con muchas de las normas sobre "notificación y retirada" que se aplican actualmente).

112. Pluralismo en internet y posible "censura" por poderes públicos y, en especial, por sujetos privados

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 mil millones 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 es líder indiscutible Google. 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 recordar que la categoría de "censura" sólo se reserva para los poderes públicos, y en este caso se trata de autocensura. En el caso de poderes públicos, las garantías frente a la censura dificultan la capacidad de poner restricciones a los mensajes de ciudadanos en foros y redes sociales que establezcan los poderes públicos. Es más, hay que ser especialmente cuidadoso con la expulsión, rechazo, selección de "amigos" o "seguidores" por los poderes públicos puesto que ello puede afectar a la objetividad y neutralidad de la Administración, al tiempo que incluso expulsar de un ámbito colaborativo o participativo puede ser una censura previa prohibida por las Constituciones.

A diferencia de los sujetos públicos, las posibilidades de restricción son mucho mayores en foros y redes sociales establecidas por sujetos privados. El principio general de libertad y autonomía de la voluntad, la libertad de empresa, o de asociación en el caso de partidos, movimientos, sindicatos, etc. e incluso la libertad de expresión pueden amparar que un sujeto privado imponga condiciones y requisitos para que los usuarios puedan participar en los debates, redes, foros, etc.

Lo mejor en cualquier caso es que existan condiciones de uso de los foros de debate o o comentarios. Y específicamente que se indiquen las circunstancias, requisitos o condiciones para poder restringir comentarios por los usuarios. De este modo se limita algo la discrecionalidad y arbitrariedad por los moderadores, especialmente si son de naturaleza jurídica pública.

En cualquier caso, la libertad de los sujetos privados para restringir contenidos no es total. 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.

El tribunal de apelación de París en febrero de 2016 ha confirmado que la justicia puede controlar si es contrario a la libertad de expresión que una red social (Facebook) decidiera unilaterialmente restringir contenidos de un usuario por entenderlos contrarios a las condiciones de uso. El tribunal frances señala que las condiciones de uso deben considerarse como condiciones generales de consumo, respecto de las que ha de haber una especial protección al usuario –consumidor- de la red social. Bien el texto de una condición de uso, como especialmente la aplicación concreta y unilateral por la red social, puede suponer una restricción desproporcionada de la libertad de expresión.

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.

113. Y para concluir, el derecho al olvido o a la supresión de información que hay en la red que no tiene interés público. En especial, el derecho a pedir a Google que desindexe información de su buscador

Entre los más de mil millones de webs se encuentra mucha información sobre las personas que se ha difundido sin su consentimiento. Y mucha de esa información es frente a los intereses y voluntad de los afectados. Así, como punto de partida, esas páginas web son contrarias a la protección de datos y otros derechos (como la intimidad, honra, imagen, etc.). Hay que señalar que, en muy buena medida, dicha información no sería molesta y sería inaccesible para nadie si no fuera porque buscadores como Google indexan dichas webs y con ello las hacen visibles cuando se busca información a partir de los nombres y apellidos de las personas. Así pues, se trata de información en webs de origen y de la indexación por Google.

La STJUE (Gran Sala) de 13 de mayo de 2014 en el asunto C-131/12, en el procedimiento entre Google Spain, S.L., Google Inc. vs. la Agencia Española de Protección de Datos (AEPD) y Mario Costeja González vino a dar una respuesta a esta situación. Por lo que aquí interesa, se afirma:

-A Google le es de aplicación la normativa de la Unión Europea de protección de datos.

- Ni el interés económico de Google ni el general interés de los usuarios a acceder información de otros justifica suficientemente la grave afección a la privacidad y protección de datos que implica el buscador de Google.

- El interés público de la información concreta y en "supuestos específicos" puede justificar que la información molesta pueda mantenerse indexada por el buscador. Sólo "en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública" (ap. 81). Será Google primero y las autoridades de protección de datos o los tribunales después quienes deberán llevar a cabo la ponderación concreta de si procede la desindexación solicitada.

- Los afectados en la Unión Europea por los resultados de búsquedas en Google pueden dirigirse a esta compañía, allí donde ésta compañía tenga establecimiento –aunque sólo sea para contratar publicidad- para solicitar la retirada de determinados resultados. Se puede solicitar –y ordenar- la desindexación sin que sea necesario haber acudido previamente a solicitar la retirada de contenidos en la web de origen. Es más, la información puede ser legítima en la web de origen pero no en Google, puesto que la difusión por Google "puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de esta página web." (ap. 87).

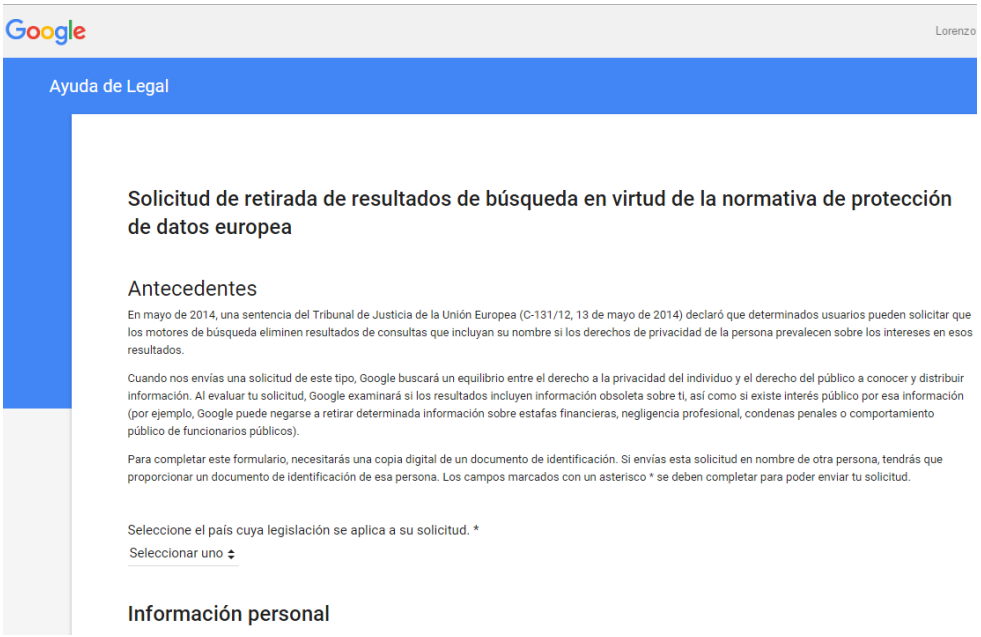
- El tiempo puede hacer que deban desindexarse informaciones que inicialmente sí que estaban protegidas por la libertad de expresión e información : "incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron" (ap. 93). En este sentido el TJUE recuerda que "cada tratamiento de datos personales debe ser legítimo, en virtud del artículo 7, durante todo el período en el que se efectúa." (ap. 95).

Desde mayo de 2014 hasta marzo de 2016 se ha solicitado a Google que no aparezcan en sus resultados de búsqueda 1.4 millones de direcciones de internet, un 40% han sido retiradas mientras que un 60% se ha considerado que debían mantenerse.

El Reglamento de protección de datos de la Unión Europea de 2016 de eficacia directa para los 28 Estados miembros regula expresa y extensamente el derecho a la supresión o al olvido. Tras la sentencia de 2014, diversos países de Iberoamérica han ido reconociendo jurisprudencialmente o por sus autoridades independientes de protección de datos el derecho al olvido, así ha sucedido en México, Argentina, Costa Rica, Nicaragua y Uruguay. En Colombia, por el contrario, se entiende que Google no es responsable de desindexar la información, sino que la web de origen es la que ha de impedir la indexación por Google (sentencias de la Corte T040-2013 o T277-2015).

Formulario de Google para la Unión Europea donde solicitar la desindexación de páginas web para que no sean resultados del buscador

https://support.google.com/legal/contact/lr_eudpa?product=websearch



Resultados desde mayo de 2014 del ejercicio del derecho al olvido en Google en la Unión Europea
https://www.google.com/transparencyreport/removals/europeprivacy/