

**“Democracia electrónica y libertades en la red, especial referencia a Colombia”, por Lorenzo Cotino Hueso, versión actualizada a diciembre de 2016**

Contenido:

<b>TERMINOLOGÍA, CONCEPTOS Y CONCEPCIONES DE DEMOCRACIA ELECTRÓNICA.....</b>	<b>3</b>
86. VARIADA TERMINOLOGÍA.....	3
87. VERSIÓN FUERTE Y VERSIÓN DÉBIL DE DEMOCRACIA ELECTRÓNICA .....	4
<i>a) Versión fuerte: e-democracia como democracia directa .....</i>	<i>4</i>
<i>b) Versión débil: las TIC como herramienta de mejora de la democracia, no centrada en el voto electrónico. ....</i>	<i>5</i>
<i>La web 2.0 o web social o participativa, el ciudadano como protagonista activo.....</i>	<i>6</i>
88. CONCEPTOS AFINES: ESPECIAL ATENCIÓN AL “GOBIERNO ELECTRÓNICO” Y LA ACTUAL TENDENCIA HACIA EL “GOBIERNO ABIERTO”. LA ALIANZA PARA EL GOBIERNO ABIERTO Y EL “ESTADO ABIERTO” EN COLOMBIA.....	8
<b>APREHENSIÓN JURÍDICA GENERAL DEL FENÓMENO .....</b>	<b>12</b>
88. VENTAJAS GENERALES DE LAS TIC PARA LA DEMOCRACIA Y GOBIERNO.....	12
89. LA OBLIGACIÓN DE IMPLANTAR FORMAS DE E-DEMOCRACIA Y E-GOBIERNO COMO PRINCIPIO JURÍDICO-CONSTITUCIONAL, CONCRETABLE POR UN LEGISLADOR CON VOLUNTAD POLÍTICA .....	12
<b>ACCESO A LAS TIC, BRECHA DIGITAL Y SU TRATAMIENTO JURÍDICO.....</b>	<b>13</b>
90. ACCESO A INTERNET EN LATINOAMÉRICA Y ESPAÑA. EL RELEVANTE ACCESO Y CONECTIVIDAD DE COLOMBIA .....	14
91. BRECHA DIGITAL Y ELITOCRACIA ELECTRÓNICA .....	17
<i>a) No discriminación en la implantación del gobierno y democracia electrónicas .....</i>	<i>17</i>
<i>b) Las políticas de acceso a internet y alfabetización digital. ¿Un derecho fundamental al acceso a la sociedad de la información?.....</i>	<i>18</i>
<b>CAUTELAS RESPECTO DE LA DEMOCRACIA Y PARTICIPACIÓN ELECTRÓNICAS.....</b>	<b>20</b>
A) NECESIDAD DE CONTROL POLÍTICO Y FISCAL DE POLÍTICAS DE LA SOCIEDAD DE LA INFORMACIÓN.....	20
B) PELIGRO DE SOBRE REPRESENTACIÓN AL CIUDADANO QUE PARTICIPA A TRAVÉS DE INTERNET .....	20
C) FRACCIONAMIENTO SOCIAL.....	20
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 .....	21
<i>a) Anonimato en la transparencia y la participación política en la red como garantía de la libertad de expresión, reconocido en Colombia.....</i>	<i>22</i>
<i>b) Anonimato, criptografía, privacidad y sus garantías .....</i>	<i>23</i>
<b>ADMINISTRACIÓN ELECTORAL Y TIC, LAS TIC EN LAS CAMPAÑAS ELECTORALES .....</b>	<b>23</b>
94. ADMINISTRACIÓN ELECTORAL Y LA CRECIENTE EMERGENCIA DE LAS TIC EN CAMPAÑA .....	23
95. LAS TÍPICAS PROHIBICIONES PREVIAS A LOS COMICIOS ELECTORALES Y SU EXIGENCIA EN INTERNET.....	25
<i>a) Internet y jornada de reflexión electoral:.....</i>	<i>25</i>
<i>b) Prohibición de encuestas y sondeos .....</i>	<i>25</i>
<b>VOTO ELECTRÓNICO: TIPOS Y GARANTÍAS .....</b>	<b>27</b>
96. VOTO ELECTRÓNICO Y SU TIPOLOGÍA: UNA IMPORTANTE DISTINCIÓN. LA REGULACIÓN COLOMBIANA DE 2011 .....	27
<i>a) Voto electrónico local en entornos sí controlados.....</i>	<i>28</i>
<i>b) Voto electrónico telemático, “pyjama voting” a distancia en entornos no controlados .....</i>	<i>29</i>
<i>c) La regulación del e-voto de 2011 en Colombia... a la espera de su tardía implantación .....</i>	<i>30</i>
97. LAS GARANTÍAS CONSTITUCIONALES DEL VOTO ELECTRÓNICO: LOS “PRINCIPIOS” DEL CONSEJO DE EUROPA.....	31
<i>Garantía de voto universal .....</i>	<i>31</i>
<i>Garantía de voto igual .....</i>	<i>31</i>
<i>Garantía de sufragio libre.....</i>	<i>32</i>
<i>Garantía de voto secreto .....</i>	<i>32</i>
98. LAS “REGLAS DE PROCEDIMIENTO” DEL CONSEJO DE EUROPA.....	32
<i>Transparencia .....</i>	<i>32</i>
<i>Verificación y responsabilidad .....</i>	<i>32</i>
<i>Fiabilidad y seguridad.....</i>	<i>32</i>

99. LA DUDA DEL VOTO ELECTRÓNICO NULO.....	33
100. LAS DIFICULTADES DE CONTROL DEL VOTO ELECTRÓNICO Y LA NECESARIA DE CONFIANZA SOCIAL PARA SU IMPLANTACIÓN .....	33
<b>EJERCICIO ELECTRÓNICO FORMAL E INFORMAL DE INICIATIVA LEGISLATIVA POPULAR Y DEL DERECHO DE PETICIÓN .....</b>	<b>35</b>
102. EJERCICIO INFORMAL DE INICIATIVAS Y PETICIONES VÍA ELECTRÓNICA .....	38
<b>TIC, TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA POR EL PÚBLICO.....</b>	<b>39</b>
103. EL DERECHO ACCESO A LA INFORMACIÓN PÚBLICA, UN NUEVO DERECHO FUNDAMENTAL .....	39
104. OBLIGACIONES DE TRANSPARENCIA ACTIVA Y OBLIGACIÓN DE INFORMACIÓN PÚBLICA EN LA RED. LA PROLIJA REGULACIÓN COLOMBIANA.....	40
105. CALIDAD DE LA INFORMACIÓN PÚBLICA Y MECANISMOS DE CONTROL DE LA TRANSPARENCIA. INDICADORES Y MEDICIÓN DE LA TRANSPARENCIA EN GENERAL Y EN COLOMBIA.....	43
<b>TIC Y DEMOCRACIA PARTICIPATIVA.....</b>	<b>45</b>
<b>LIBERTADES INFORMATIVAS Y SU DIFÍCIL ADAPTACIÓN A INTERNET .....</b>	<b>46</b>
108. LA LIBERTAD DE EXPRESIÓN E INFORMACIÓN PROTEGE EN GENERAL INTERNET Y A TODOS LOS INTERNAUTAS SIN MAYORES LÍMITES QUE EN OTROS MEDIOS.....	46
109 LA CORTE CONSTITUCIONAL COLOMBIANA HA PROFUNDIZADO EN EL TRATAMIENTO JURÍDICO DE LA LIBERTAD DE EXPRESIÓN EN INTERNET CUANDO LA EJERCEN INDIVIDUOS, MEDIOS DE COMUNICACIÓN Y GRANDES PRESTADORES EN INTERNET.....	47
110 LA CORTE COLOMBIANA AFIRMA LA CONEXIÓN DE LA LIBERTAD DE EXPRESIÓN CON LA ARQUITECTURA DE INTERNET Y EL PRINCIPIO DE NEUTRALIDAD .....	48
111. GARANTÍAS FRENTE AL CIERRE DE WEBS O AL CORTE DE ACCESO O FILTRADO DE CONTENIDOS EN INTERNET .....	48
112. PRECISAMENTE EN COLOMBIA SE AFIRMA LA NO RESPONSABILIDAD DE LOS INTERMEDIARIOS EN INTERNET NI DE GOOGLE PARA EVITAR LA CENSURA EN INTERNET Y AFECTAR A LA NEUTRALIDAD EN INTERNET QUE EXIJE LA LIBERTAD DE EXPRESIÓN...	50
113. PROYECCIÓN DE ALGUNAS CATEGORÍAS Y GARANTÍAS DE LAS LIBERTADES INFORMATIVA A INTERNET.....	51
<i>a) Una clave: la relevancia o interés público de la noticia.....</i>	<i>51</i>
<i>b) La veracidad y la diligencia del informador y el derecho de réplica o rectificación .....</i>	<i>51</i>
<i>c) El secreto profesional del periodista en internet ¿para todos? . De Wikileaks a Mexicoleaks. Una     cuestión importante que va a dejar de serlo .....</i>	<i>52</i>
114. DIFICULTADES DE ATRIBUCIÓN DE RESPONSABILIDAD JURÍDICA EN LA RED .....	54
115. PLURALISMO EN INTERNET Y POSIBLE “CENSURA” POR PODERES PÚBLICOS Y, EN ESPECIAL, POR SUJETOS PRIVADOS.....	55
116. 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. LA SOLUCIÓN EUROPEA .....	56
117 LA SOLUCIÓN DE LA CORTE CONSTITUCIONAL COLOMBIANA RESPECTO DEL DERECHO AL OLVIDO Y GOOGLE. GOOGLE NO TIENE QUE DESINDEXAR, LA WEB DE ORIGEN DEBE UTILIZAR MECANISMOS COMO EL ROBOT.TXT PARA QUE GOOGLE NO INDEXE .....	58
118. OLVIDO Y LÍMITES DE INFORMACIÓN SOBRE COMISIÓN DE DELITOS Y DECISIONES JUDICIALES EN COLOMBIA .....	59

## 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.

Cabe tener en cuenta el concepto amplio del Manual para la implementación de la Estrategia de Gobierno en línea en las entidades del orden nacional de la República de Colombia (en adelante Manual de Gobierno en Línea), (en su versión 3.0 página 7)

*Democracia en línea: comprende todas las actividades para que las entidades creen un ambiente para empoderar a los ciudadanos e involucrarlos en el proceso de toma de decisiones. Con estas actividades se propicia que el ciudadano participe activa y colectivamente en la toma de decisiones de un Estado totalmente integrado en línea. Igualmente, se promueve que las entidades públicas incentiven a la ciudadanía a contribuir en la construcción y seguimiento de políticas, planes, programas, proyectos, la toma de decisiones, el control social y la solución de problemas que involucren a la sociedad en un diálogo abierto de doble vía. Este componente establece las indicaciones para que las entidades lleven a cabo sus ejercicios de participación en línea a través de un proceso ordenado y de realimentación permanente tanto al interior, como hacia sus ciudadanos y/o usuarios. Son 4 los grupos de actividades de democracia en línea que se desarrollan en este componente: 1. Definir la estrategia de participación; 2. Construir de forma participativa las políticas y planeación estratégica; 3. Abrir espacios para el control social; 4. Abrir espacios de innovación abierta.*

Cabe pues tener en cuenta este concepto actualizado.

### **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 cuestión. 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 –destruktiva 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 *excusa* 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.

Esta versión parece disiparse con el paso del tiempo, especialmente en razón de la emergencia del Gobierno Abierto en los últimos años.

Cabe mencionar la iniciativa y Partido Ecodemocracia (<http://partido.ecodemocracia.co/> )

. Se afirma desde este partido o plataforma que:

*“Todos los ciudadanos tienen la opción de votar, proponer y deliberar los proyectos de ley activos en la plataforma. Si la Red obtiene uno o más puestos en una corporación política nacional o regional, los ciudadanos registrados que deseen votar, deberán pasar por un proceso de verificación electrónica y en red.*

*El Partido Red Ecodemocracia tiene como únicos parámetros de acción programática y operativa el diagnóstico de la organización Ecodemocracia y el Decálogo operativo de la misma.”*

*“El antiguo representante, es reemplazado por un consultor y técnico, que tiene la capacidad de dar conceptos sobre los proyectos de ley, pero no la capacidad de votarlos.”*

*“En cada votación o bloque de votaciones en el congreso, todo miembro puede delegar su voto en otro ciudadano o en el partido en línea.*

*La delegación del voto es libre, inmediata y opcional y se hace desde un dispositivo móvil como el celular”*

Así pues, se trataría de la articulación de un sistema de participación electrónica e iniciativa a través de representantes políticos clásicos que quedarían sometidos a las preferencias electrónicas de los miembros del partido.



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 n° 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 suelen identificar.

El concepto de “Democracia en línea” para Colombia que se ha expuesto, parece quedar más próxima a esta versión “débil” de democracia y cercana al gobierno abierto que ahora se expone.

### 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*

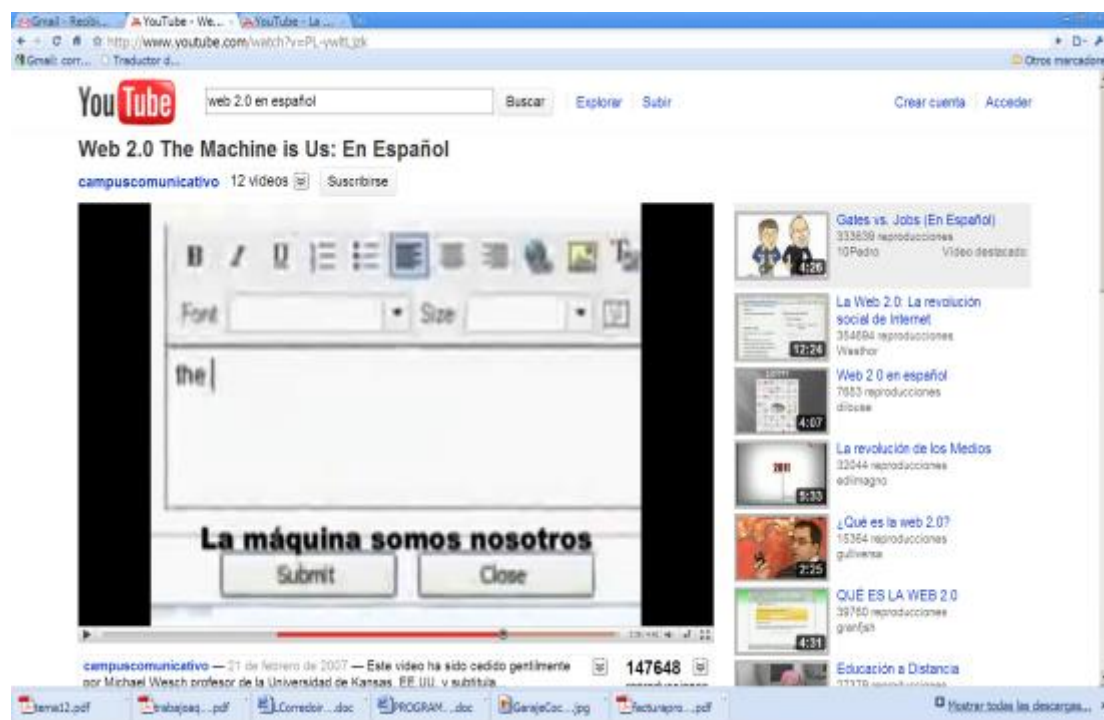


Las TIC facilitan el empoderamiento del ciudadano, la construcción desde abajo arriba, el control de la información así como “la e-democracia debe permitir más participación del ciudadano en establecer la agenda, el análisis y la formulación, ejecución y seguimiento de la política.” (Directriz nº 7 Recomendación 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 y el “Estado abierto” en Colombia

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](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, Venezuela, 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.

Puede seguirse la información de Colombia en  
<http://www.opengovpartnership.org/es/node/271>

Colombia forma parte de la Alianza, como España, en la segunda oleada, desde 9.11.2011 como puede verse en la imagen:



Libertad y Orden

Ministerio de Relaciones Exteriores  
República de Colombia

DM-DVRE-DIA-GEUCA No. 55177

Bogotá, D. C., 9 de septiembre de 2011

Señora Secretaria de Estado:

Tengo el honor de dirigirme a Su Excelencia con ocasión de su amable invitación al Gobierno de Colombia a adherir a la iniciativa *Open Government Partnership* (OGP), la cual es coliderada por los Gobiernos de los Estados Unidos de América y la República Federativa del Brasil.

Me complace anunciar a Su Excelencia que, por compartir los ideales de lograr gobiernos más transparentes, eficaces y responsables, con instituciones que les ofrezcan más poder a los ciudadanos y que responda a sus aspiraciones, Colombia desea participar en esta iniciativa.

Hago propicia la ocasión para reiterar a Su Excelencia las seguridades de mi más alta y distinguida consideración.

**MÓNICA LANZETTA MUTIS**

Viceministra de Relaciones Exteriores  
Encargada de las Funciones del Despacho de la  
Señora Ministra de Relaciones Exteriores

Su Excelencia la señora  
**HILLARY RODHAM CLINTON**  
Secretaria de Estado  
Estados Unidos de América  
Washington, D.C.

Colombia ha presentado su segundo plan de acción, vinculado al proceso de paz, como se puede ver en la imagen.

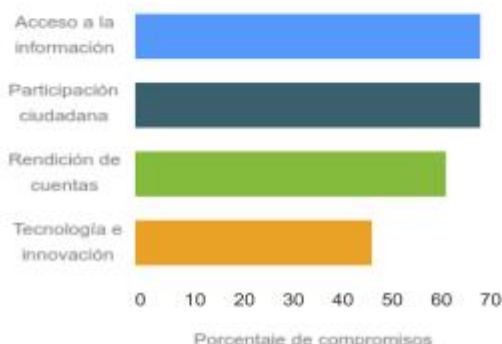


Existe, en el segundo plan de acción, una sinergia más activa entre sociedad civil y gobierno. El desafío a futuro será armonizar planes de acción con los esfuerzos de diálogo para la construcción del proceso de paz.

## Rendimiento de compromisos



## Contenido



## Recomendaciones Clave

- ✓ Reformar mecanismos de control externo incentivando el monitoreo social
- ✓ Incorporar a las regiones y estimular la participación de actores diversos de sociedad civil
- ✓ Avanzar la participación y la transparencia en temas ambientales

## Proceso de consulta



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.

Cabe añadir para Colombia que la expresión ha sido recogida en el Decreto 2573 de 2014, art 1 se afirma el “fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la

sociedad.” Es más, se regula la estrategia “TIC para el Gobierno abierto” (art. 4): “Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones. [...] comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto pero no los cubre en su totalidad.”

## **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 interacción 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](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 información de relevancia jurídica a través de internet en los portales corporativos o sedes electrónicas institucionales se está generalizando en América Latina y, recientemente, en Colombia y España.

## **ACCESO A LAS TIC, BRECHA DIGITAL Y SU TRATAMIENTO JURÍDICO**

### 90. Acceso a internet en Latinoamérica y España. El relevante acceso y conectividad de Colombia

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 conectados.

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
<a href="#">Africa</a>	1,158,355,663	16.0 %	330,965,359	28.6 %	7,231.3%	9.8 %
<a href="#">Asia</a>	4,032,466,882	55.5 %	1,622,084,293	40.2 %	1,319.1%	48.2 %
<a href="#">Europe</a>	821,555,904	11.3 %	604,147,280	73.5 %	474.9%	18.0 %
<a href="#">Middle East</a>	236,137,235	3.3 %	123,172,132	52.2 %	3,649.8%	3.7 %
<a href="#">North America</a>	357,178,284	4.9 %	313,867,363	87.9 %	190.4%	9.3 %
<a href="#">Latin America / Caribbean</a>	617,049,712	8.5 %	344,824,199	55.9 %	1,808.4%	10.2 %
<a href="#">Oceania / Australia</a>	37,158,563	0.5 %	27,200,530	73.2 %	256.9%	0.8 %
<b>WORLD TOTAL</b>	<b>7,259,902,243</b>	<b>100.0 %</b>	<b>3,366,261,156</b>	<b>46.4 %</b>	<b>832.5%</b>	<b>100.0 %</b>

Por países, en América Latina (<http://www.internetworldstats.com/stats10.htm>), y con referencia a usuarios más avanzados con interacción 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%).

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

En perspectiva mundial y en junio de 2016 el grado de penetración de internet en el mundo es del 50,1%, con 3.675.813 usuarios, de los que América Latina –Caribe supone el 10,5% del total. En Europa hay 614,979,903 usuarios de internet, con un grado de penetración del 73.9 %, representando el 16,7% mundial. En el caso de la Unión Europea<sup>1</sup> hay 402,937,674 usuarios, con un grado de penetración –algo superior- de 79.3 %. En España, se cifran los usuarios de internet en 35,705,960, un 76.9 % de la población<sup>2</sup>.

En Colombia en 2015 un 82% de ciudadanos interactuaron por medios electrónicos con el Estado y un 79% de las empresas. Se ha pasado de 2 millones de conexiones en 2010 a 12,4 finalizando 2015. El 59% de los colombianos accede a redes sociales al menos diez veces al día, mientras que el 8.1% ingresa más de 50 veces<sup>3</sup>.

Desde el punto de vista regional, cabe recordar que en Suramérica sobre una población de 415,413,166 personas hay 277,023,754 usuarios de internet que representan el 66.7 % de la

<sup>1</sup> <http://www.internetworldstats.com/stats9.htm>

<sup>2</sup> <http://www.internetworldstats.com/stats4.htm>

<sup>3</sup> Datexco Company, “Estudio uso y apropiación de las TIC en Colombia- Cultura digital”, realizado por para el Ministerio de Tecnologías de la Información y las Comunicaciones. Datos de campo: 1 de noviembre a 4 de diciembre de 2015. Acceso completo en [http://www.mintic.gov.co/portal/604/articles-15296\\_recurso\\_3.pdf](http://www.mintic.gov.co/portal/604/articles-15296_recurso_3.pdf)

población en junio de 2016<sup>4</sup>. En Colombia se estiman 28,5 millones de usuarios <sup>5</sup>, que representan un 58,6% de la población<sup>6</sup>.

De acuerdo con un informe de indicadores básicos de las tecnologías de la información y las comunicaciones del Departamento Nacional de Estadística (Dane), en el 2014 un 38 por ciento de los hogares colombianos tenía acceso a internet, cifra que subió a 41,8 por ciento el año pasado.

Igualmente, la proporción de hogares que poseía un computador de escritorio, un portátil o una tableta alcanzó un 45,5 por ciento cuando en el 2014 alcanzó un 44,5 por ciento. Así mismo, un 56 por ciento de las personas usaba internet.

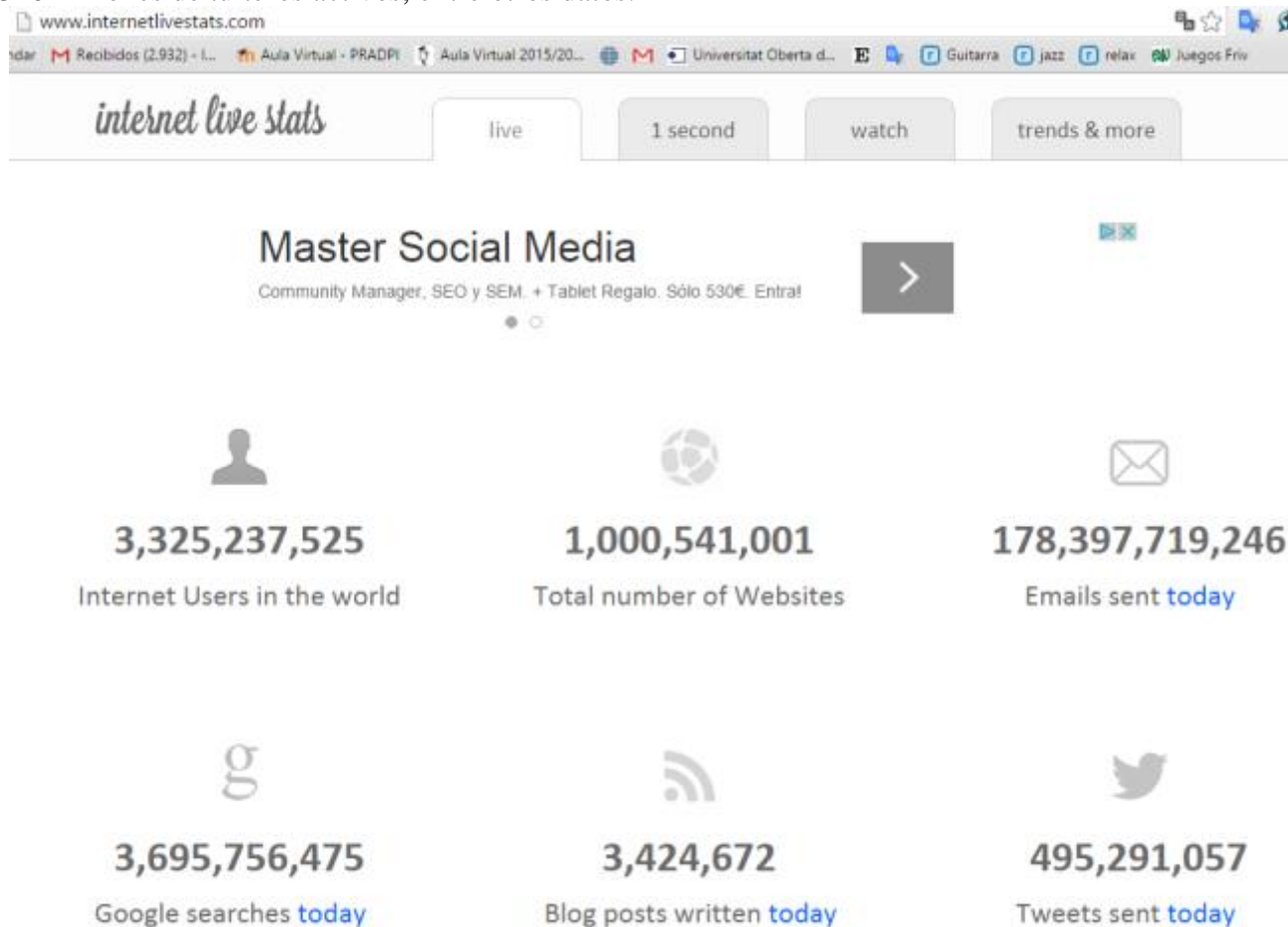
En el 2015, un 67,7 por ciento de los colombianos de 5 o más años que usó internet, lo hizo para acceder a las redes sociales.

De acuerdo con el reporte del Dane, en el 95,6 por ciento de los hogares al menos una persona poseía teléfono celular en 2015, mientras que en 2014 la proporción fue de 95,3 por ciento. Al mismo tiempo, el 86 por ciento de las personas manifestó haber utilizado ese dispositivo.

Colombia fue uno de los países de mejor desempeño en términos de conectividad a internet en 2014, según el 'Affordability Report', en el que el país ocupa la segunda posición entre una lista de 51 economías emergentes y en desarrollo a nivel mundial.

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.



<sup>4</sup> <http://www.internetworldstats.com/stats2.htm>

<sup>5</sup> <http://www.internetworldstats.com/stats15.htm>

<sup>6</sup> Ídem.



### **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 *“en 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.

En Colombia, en principio la Ley 1437 no permite la imposición de la relación electrónica, si bien ya se perciben diversos supuestos de comunicaciones obligatorias.

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 interacción 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 interacción 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 interacción electrónica.

-garantías materiales: las normas que fijan la interacción obligatoria, deberían determinar con una certeza mínima el colectivo de personas u organizaciones a los que se obliga a la interacción 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 de 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 communicationis*, 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 mi juicio destaca por su calidad 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&IID=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”, creación de “puntos de acceso público”, asegurar “el acceso equitativo a Internet para personas con discapacidad y los sectores menos favorecidos” y para todo ello, “adoptar planes de acción detallados”).

También en 2011, destaca el Informe del Relator Especial a la Asamblea de Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, uno de los autores del documento anterior, 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](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”.

En Colombia hubo una propuesta de reconocimiento por los congresistas Gaviria y Galvis en 2011 a través de una propuesta legislativa que finalmente no prosperó. En 2014 un senador (Pedraza) propuso un acto legislativo para modificar al artículo 20 de la Constitución y reconocer el acceso a banda ancha de internet como derecho fundamental, decayendo en 2014.

La Ley 1341 de 2009 en su artículo 2 regula unos “Principios orientadores”, incluyendo el acceso a las TIC:

*“1. Prioridad al acceso y uso de las Tecnologías de la Información y las Comunicaciones. El Estado y en general todos los agentes del sector de las TIC y las Comunicaciones deberán colaborar, dentro del marco de sus obligaciones, para priorizar el acceso y uso a las TIC y las comunicaciones en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad.*

*“7. El derecho a la comunicación, la información y la educación y los servicios básicos de las TIC: en desarrollo de los artículos 20 y 67 de la Constitución Nacional el Estado propiciará a todo colombiano el derecho al acceso a las Tecnologías de la Información y las Comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos: la libertad de expresión y de difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la educación y el acceso al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. Adicionalmente, el Estado establecerá programas para que la población de los estratos menos favorecidos y la población rural tengan acceso y uso a las plataformas de comunicación, en especial de Internet y contenidos informáticos y de educación integral.”*

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 communicationis* 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](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 teoría, 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](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*)<sup>7</sup> 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 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<sup>9</sup>.

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 precondition de un debate y deliberación libres a través de la red. No hay una respuesta unívoca.

---

<sup>7</sup> 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”.

<sup>8</sup> 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.

<sup>9</sup> 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 transparencia y la participación política en la red como garantía de la libertad de expresión, reconocido en Colombia

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.

Hay que llamar la atención sobre la posibilidad del anonimato en un ámbito afín como es el acceso a la información pública. En este sentido, la Ley Modelo Interamericana sobre Acceso a la Información<sup>10</sup> contempla expresamente en su apartado 5 d) que se podrán “realizar solicitudes de información en forma anónima”.

Y la Ley 1712 de transparencia de Colombia, regula expresamente las solicitudes anónimas en su artículo 4º párrafo: “Cuando el usuario considere que la solicitud de la información pone en riesgo su integridad o la de su familia, podrá solicitar ante el Ministerio Público el procedimiento especial de solicitud con identificación reservada.” Y el Decreto 103 de 2015, de 20 de enero, que

---

<sup>10</sup> [http://www.oas.org/es/sla/ddi/docs/AG-RES\\_2607\\_XL-O-10\\_esp.pdf](http://www.oas.org/es/sla/ddi/docs/AG-RES_2607_XL-O-10_esp.pdf)

desarrolla parcialmente la Ley 1712 en su artículo 18 señala que cabrán las peticiones anónimas “siempre que existan medios probatorios suficientes que permitan adelantar la actuación de oficio.” La Resolución 3333 del 22 de diciembre de 2015 en su artículo 22 reglamenta expresamente las “peticiones anónimas” e incluye los medios electrónicos .

#### 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-Whatsapp 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 depuración 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 candidatos. Ello facilita, por ejemplo, tratamientos específicos por candidatos o partidos de los votantes según su carácter más 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 redes sociales, con centenares de miles de “amigos” en *Facebook* por ejemplo, fue un elemento más para su victoria<sup>11</sup>. 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 Minnesota 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](http://en.wikipedia.org/wiki/Tea_Party_movement)), que en ocasiones parece dominar la agenda y la elección misma de candidato por el Partido Republicano. El nuevo presidente de los EEUU Donald Trump parece haber superado y mucho en las redes sociales a la derrotada Hillary Clinton, no sólo en número (cuatro millones más de seguidores en Twitter y cinco millones más en Facebook) sino en captación de afectos y movilización. También parece que superó y mucho a la candidata derrotada en la transmisión de información cierta y en el manejo de robots que generaban la información falsamente (La página de internet Twitter Audit halló que el 39% de los seguidores de Trump en Twitter (comparado con el 5% de Clinton) eran robots generados por computador).

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<sup>12</sup>, desde 2011 hasta la fecha, denominado “Mesa Administrada Electrónicamente”<sup>13</sup>. 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

---

<sup>11</sup> A texto completo, puede seguirse <http://dialnet.unirioja.es/servlet/articulo?codigo=3172502>

<sup>12</sup> <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.

<sup>13</sup> Puede seguirse una explicación sencilla virtual en:

[http://elecciones.mir.es/generales2011/Visitas\\_virtuales/Mesa\\_Administrada\\_Electronicamente\\_\(MAE\)/Mesa\\_Administrada\\_Electronicamente\\_\(MAE\).htm](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>



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 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, como Colombia una semana previa a los comicios. 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 estúpido alguno en reenviar a la información del sondeo electoral prohibido.

**el Periódico**  
**POLÍTICA**

PORTADA | INTERNACIONAL | POLÍTICA | ECONOMÍA | SOCIEDAD | BARCELONA | DEPORTES | OCIO Y CULTURA

Pulso por la independencia | Artur Mas | CUP | Barómetro | Resultados 27 S | Elecc

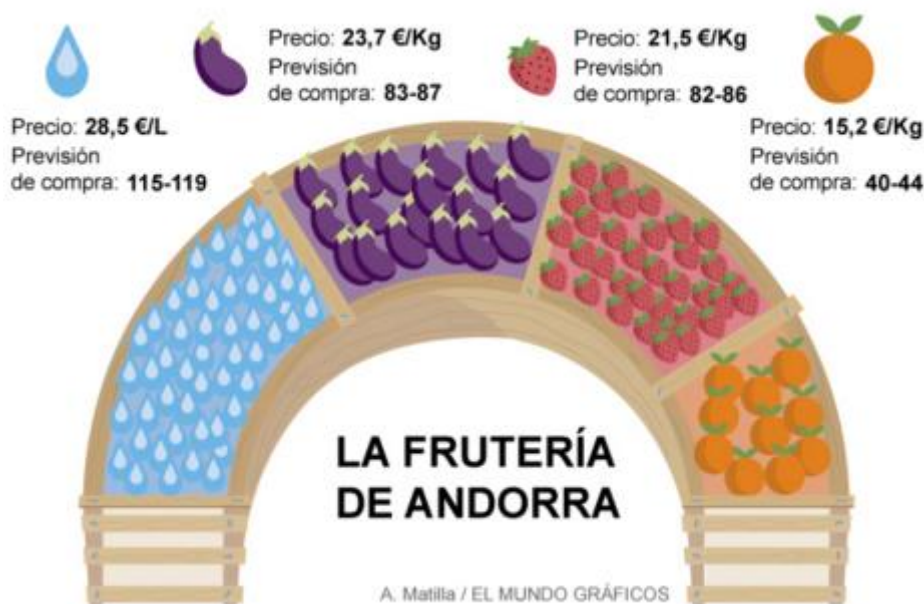
**20D**

**La encuesta prohibida: sondeo definitivo**

'El Periòdic d'Andorra' difunde la sexta entrega del barómetro del GESOP sobre el 20-D

Primer sondeo | Segundo sondeo | Tercer sondeo | Cuarto sondeo | Quinto sondeo

Incluso con cierto humor, en las elecciones de junio de 2016, los sondeos transmitidos desde Andorra se difundían ya por toda la prensa española con la metáfora de los precios de la fruta y verdura, según los colores que identificaban a los cuatro partidos más importantes (agua, Partido Popular, berenjena Podemos, Fresa, P. Socialista, Naranja, Ciudadanos)





#### 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 referendo 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).

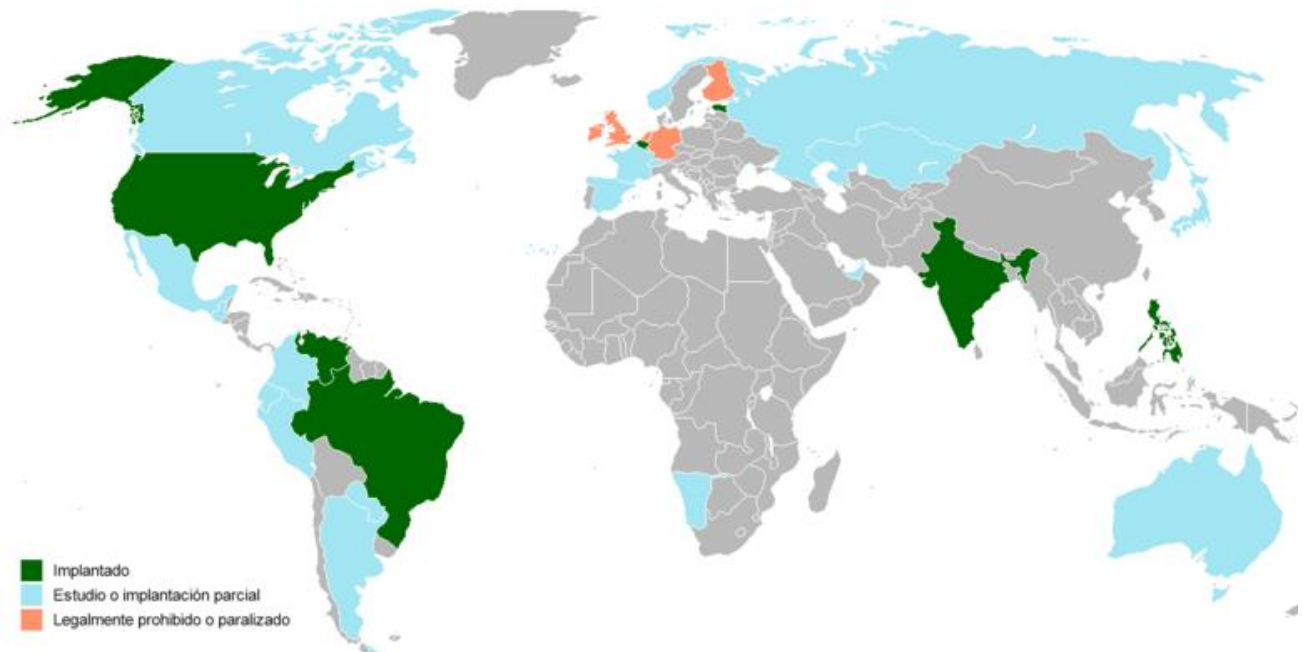
Entre las modalidades, cabe señalar el voto por computadora, con al menos un dispositivo para elegir la candidatura y otro para emitir el voto. Se necesita la conexión entre la mesa electoral y el votante tanto para asistirle como para evitar fraudes de este último. Como recuerda Barrat:

“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 proporcionan 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 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](http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_impl_c.htm)

**Países con implantación**



**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 *Whatsapp* 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 regularon 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.

### c) La regulación del e-voto de 2011 en Colombia... a la espera de su tardía implantación

En Colombia en razón de la Ley 1475 de 2011 se imponía el uso de TIC para el voto y se creó la comisión Asesora para la Implementación del Voto Electrónico

<http://www.registraduria.gov.co/-Comision-asesora-.html>

La misma no parece tener actividad desde 2014 y las últimas experiencias parece que son de 2012

<http://www.registraduria.gov.co/-Experiencias-colombianas-.html>

En Colombia, en la Sentencia de la Corte Constitucional C-490 de 2011 sobre la ley 1475 de 2011, por la cual se adoptan reglas de organización y funcionamiento de los partidos y movimientos políticos, la Corte no vio impedimentos para el e-voto, “La Corte declarará la exequibilidad de esta norma, habida consideración que la posibilidad de implementar el voto electrónico está admitida de manera explícita por la Constitución, a condición de que en su ejercicio se respeten los atributos esenciales del derecho al sufragio, fundamentalmente su carácter secreto, libre de coacción, igualitario, y que suministre garantía de transparencia y efectividad.” (127). Tampoco aprecia problema alguno en el uso de identificadores biométricos (128).

Así, la ley 1475 de 2011 dedica un Capítulo IV (arts. 39 y 40 ) al voto electrónico. Básicamente se afirma que la identificación del elector podrá darse con “medios tecnológicos y/o sistemas de identificación biométricos” y que la identificación “podrá ser independiente de la utilización de mecanismos de votación electrónica”. Se impone la propiedad de los programas y derechos de uso en los contratos para la implementación del voto electrónico. Se afirma asimismo la obligatoriedad de dotar de recursos necesarios y la obligatoria implantación de la “identificación biométrica” y el inicio del desarrollo del sistema de voto electrónico de conformidad con un plan piloto, nunca más tarde de las “elecciones para Congreso que se realizarán en el año 2014.”

Tales obligaciones y plazos fueron ignorados desde 2014. En el marco del proceso de paz en 2016 parecía que el tema recobraría interés, sin embargo se ha admitido por las instituciones que no hay fecha para dar cumplimiento a normativa. En mayo de 2016 un grupo de senadores anunció acciones legales para exigir que se cumpla con la Ley, amenazando con una acción de incumplimiento.

El artículo 6 de esta ley 1475 de 2011 también dispone el suministro de tarjetas electorales o instrumentos de votación electrónica respecto de las consultas populares. En esta dirección, la Ley estatutaria 1757 de 2015 (julio 6) que en su artículo 37 hace referencia al “Contenido de la tarjeta electoral o del mecanismo electrónico de votación” imponiéndose que la tarjeta electoral o el

mecanismo electrónico de votación deberá garantizar que se presente a los ciudadanos la posibilidad de manifestar libremente su decisión sobre la respectiva pregunta del plebiscito, referendo, revocatoria del mandato o consulta popular.

El artículo 38 fija algunos requisitos específicos para el “mecanismo electrónico de votación”. Así, en la letra c) se dispone que “c) La tarjeta electoral o el mecanismo electrónico de votación para la consulta sobre la convocatoria a una asamblea constituyente deberá ser diseñado de tal forma que los electores puedan votar con un sí o un no la convocatoria y, separadamente, los temas que serán competencia de la Asamblea.”

### ***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.<sup>14</sup>

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

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

#### Garantía de voto universal

Se afirman cuatro exigencias:

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

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

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

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

#### Garantía de voto igual

Se afirman cuatro directrices:

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

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

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

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

---

<sup>14</sup>

### 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 Paper 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”<sup>15</sup>. Si el escrutinio manual puede hacerlo incluso un analfabeto, el escrutinio electrónico requiere de conocimientos. Señala Jones<sup>16</sup> 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)<sup>17</sup> 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

---

<sup>15</sup> BARRAT I ESTEVE, Jordi, “Observación electoral y voto electrónico”, en *Revista catalana de dret públic*, n.º. 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>

<sup>16</sup> 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>

<sup>17</sup> El texto en alemán en [http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303\\_2bvc000307.html](http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html) en inglés, en [http://www.bundesverfassungsgericht.de/en/decisions/rs20090303\\_2bvc000307en.html](http://www.bundesverfassungsgericht.de/en/decisions/rs20090303_2bvc000307en.html)

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<sup>18</sup>. Una de las posibles ventajas del e-voto es la celeridad del recuento, que no es manual. No obstante, esta ventaja se hace muy relativa en sistemas con listas cerradas y bloqueadas, como suele ser el caso español, en donde el recuento es bastante sencillo y rápido. En el caso español que el sistema electrónico no puede dar la transparencia que aquí se da, pues como se ha visto se cuenta con una potencial y real capacidad de auditar el proceso de escrutinio y recuento por cualquier ciudadano y, sobre todo, por los representantes, partidos y candidatos.

Ahora bien, tampoco hay que cerrar la puerta al e-voto y las ventajas que trae consigo siempre que se consiga la suficiente confianza social. Y es que, todo se hace depender de la confianza ciudadana pues como afirma Barrat “el voto electrónico sería compatible con los principios electorales de cualquier democracia, siempre y cuando las medidas garantistas generaran la suficiente confianza ciudadana”<sup>19</sup>. 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.poueva.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](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>

---

<sup>18</sup> Al respecto destaca la obra de DRIZA MAURER, Ardita y BARRAT, Jordi, *E-voting Case Law: a Comparative Analysis*, Publishing House, 2015.

<sup>19</sup> Ob cit. pág. 10 versión electrónica.



*Videos –parodia contra el e-voto*

Movimiento antibelga:

<http://www.youtube.com/watch?v=4g0zbaIQL90>

Homer Simpson tries to vote for Obama

[https://www.youtube.com/watch?v=EV\\_c1-YTk8M](https://www.youtube.com/watch?v=EV_c1-YTk8M)



## 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, especialmente reconocido en Colombia**

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.



*Por primera vez puedes cambiar las cosas. Con tu firma*

**Recogemos firmas**  
aptas legalmente

**Cambiamos las cosas**  
con el voto de todos

Novedades:

[Noticias y información útil](#)

Te imaginas poder firmar desde el móvil? [Va a ser posible](#). Síguenos en [Twitter](#) y [Facebook](#)

Iniciativas en curso:

*No hay iniciativas activas en este momento.*

*¿Tienes alguna propuesta? [Envíanosla](#)*

[¿Para qué utiliza Mifirma.com el dinero de los donativos recibidos?](#)

**Donar**

[¿Quieres recibir información sobre nuevas iniciativas y novedades?](#)

Email\*

**¿Cómo funciona?**



Posibilitamos la recogida de firmas. Cualquier ciudadano puede firmar online nuestras iniciativas legislativas populares (ILP).



Cuando alcanzamos el número de firmas necesario, seguimos los trámites legales para que la iniciativa se debata en el Congreso.



Súmame a Mifirma.com y difunde estas iniciativas entre tus amigos, a través de las redes sociales.

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/>

En Colombia cabe tener en cuenta la Ley estatutaria 1757 de 2015 (julio 6) que en su artículo 6 parágrafo 2º dispone que “La inscripción de iniciativas [iniciativas para la revocatoria del mandato] podrá realizarse a través de medios electrónicos, en cuyo caso deberá utilizarse lenguaje estándar de intercambio de información en el formulario”. De igual modo, según se ha visto, el artículo 6 de la ley 1475 de 2011 así como la Ley estatutaria 1757 de 2015 (julio 6) prevén el uso de identificación y votación electrónicos en el ámbito de las consultas.


El derecho de petición, de importancia extraordinaria en Colombia (art. 23 Constitución) puede ejercerse sin duda alguna a través de medios electrónicos con una enorme flexibilidad. Así lo prevé expresamente el ordenamiento jurídico colombiano.


En este sentido el artículo 5 de la Ley 1437 del Código de Procedimiento Administrativo toda persona podrá presentar peticiones, quejas, reclamaciones, mediante cualquier medio tecnológico o electrónico disponible en la entidad, aun por fuera de las horas de atención al público y sin someterse a requisitos como el registro previo del correo electrónico. También se dispone la solicitud electrónica de información en la Ley 1712 de 2014 y la la Ley 1755 del 30 Junio de 2015 de petición. De manera concreta para el MINTIC la Resolución 3333 del 22 de diciembre de 2015 dispone como “Canales oficiales de registro” de peticiones la “Virtual:Cuenta Facebook y de Twitter, además de la Página Web: [www.mintic.gov.co](http://www.mintic.gov.co) en el link Atención al Público - Peticiones. Por su parte la Resolución 3564 del 31 de diciembre de 2015 sobre peticiones de información regula en su artículo 6 el formulario electrónico de solicitud de información pública. Y de modo muy concreto el Anexo N°. 1 hace referencia al “Correo electrónico institucional destinado por el sujeto obligado para la recepción de solicitudes de información. y al “Link al formulario electrónico de solicitudes, peticiones, quejas, reclamos y denuncias.” Y ya en particular, el Anexo N°. 2 regula los “Lineamientos sobre el formulario electrónico para la recepción de solicitudes de información pública.”

### ***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](http://www.change.org) ). Que se trate de un ejercicio informal de derechos no resta el valor político que puedan tener estas iniciativas o movimientos.

**change.org**

 Inicia una petición

 Más peticiones

 Buscar

 Entrar

# La mayor plataforma de peticiones del mundo

139.595.695 personas han pasado a la acción. [Victorias cada día.](#)

**Inicia una petición**

## **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.

Como ya señalara la Corte Constitucional colombiana en la Sentencia C-141/10 de control de la ley de refrendo (4.1.3):

“La transparencia en el ejercicio de las funciones públicas constituye un elemento de la moderna democracia institucional, que aunque de amplia tradición, se ha renovado con las nuevas concepciones fruto del avance en las comunicaciones, que facilitan la concreción de principios como el de publicidad a través de herramientas como las páginas web, los correos electrónicos o los mensajes de texto a celulares. Este resulta un aspecto trascendental y que redondea el sentido democrático del órgano legislativo, pues carecería de sentido el carácter representativo derivado de la escogencia de los miembros del Congreso si la actividad que realizan como representantes no pudiera ser seguida por sus electores.

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).

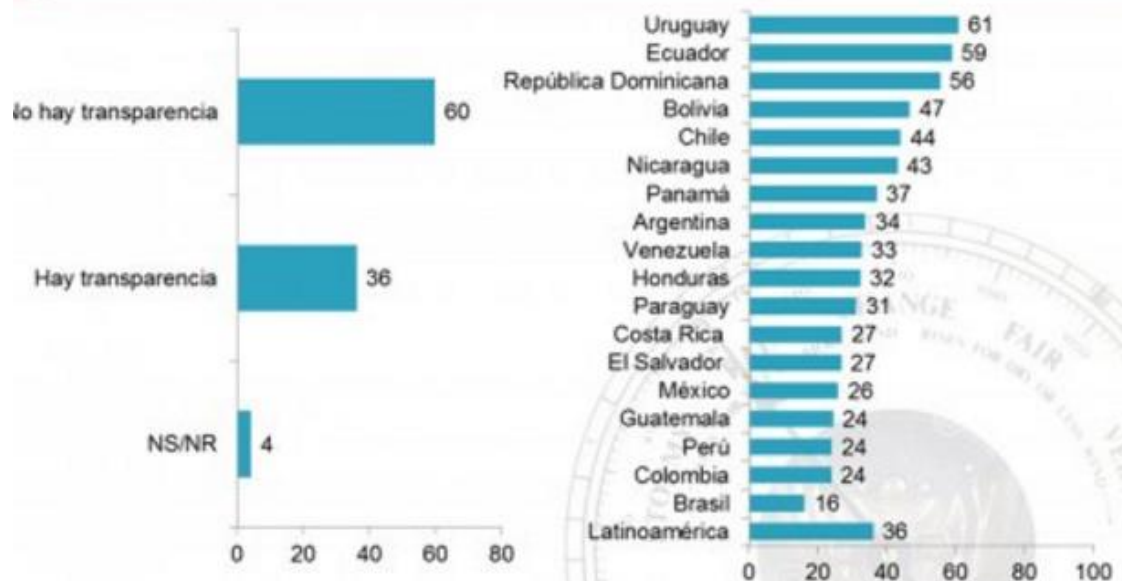
La percepción de transparencia en Colombia, como puede apreciarse se sitúa en la cola.

# PERCEPCIÓN DE TRANSPARENCIA EN EL GOBIERNO

## TOTAL AMÉRICA LATINA 2015 - TOTALES POR PAÍS 2015



P. ¿Cuánta transparencia cree Ud. que hay en el gobierno? ¿Cree Ud. que hay mucha, poca, algo o nada de transparencia? \*Aquí "Poco" más "nada" y "mucho" más "algo". \*\*Aquí solo "Mucha" más "algo".



Fuente: Latinobarómetro 2015

ranking de Latinobarómetro sobre transparencia de gobierno en América Latina

Colombia aprobó la Ley 1712 de 2014 y cabe tener en cuenta especialmente la Corte Constitucional colombiana en Sentencia C-274 del 9 de mayo de 2013 sobre la ley. De igual modo cabe tener en cuenta la Ley 1755 de 2015 (Junio 30), que regula el Derecho Fundamental de Petición.

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 prolija regulación colombiana***

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.

The screenshot displays the INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) website. At the top, there is a navigation menu with links for 'Directorio', 'Contrataciones', 'Concesiones', 'Subsidios', and 'Más'. The main header features the INAI logo and the title 'Portal de Obligaciones de Transparencia'. Below this, a search bar is present with a 'Buscar' button. The search results are filtered by 'Tema: XIII - CONTRATACIONES' and 'Institución: INSTITUTO MEXICANO DEL SEGURO SOCIAL EN PROCESO DE REESTRUCTURA'. The search results show 3,637,599 results found in the 'XIII - CONTRATACIONES' fraction. The first result is titled 'Contratos - CFE' and describes the acquisition of dry chemical powder by the Comisión Federal de Electricidad (CFE) through a direct adjudication process.

Además, no sólo se trata de poner a disposición 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.



Seguendo el ya citado Manual para el Gobierno en línea colombiano, se define la política de Información en línea:

*“comprende todas las actividades a desarrollar para que las entidades dispongan para los diferentes tipos de usuarios de un acceso electrónico a toda la información relativa a su misión, planeación estratégica, trámites y servicios, espacios de interacción, ejecución presupuestal, funcionamiento, inversión, estructura organizacional, datos de contacto, normatividad relacionada, novedades y contratación, observando las reservas constitucionales y de Ley, cumpliendo todos los requisitos de calidad, disponibilidad, accesibilidad, estándares de seguridad y dispuesta de forma tal que sea fácil de ubicar, utilizar y reutilizar. Las actividades de este componente están concentradas principalmente en dos aspectos: 1. Publicación de información y 2. Publicación de datos abiertos.”*

Cabe seguir las págs. 22 y ss. en las que se determinan las políticas concretas y los indicadores para su medición.

En todo caso, jurídicamente en Colombia hay que seguir en especial el “principio de transparencia” (art. 3 Ley 1712) los poderes públicos tienen “el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios”. Especialmente en virtud del “Principio de la divulgación proactiva de la información” expresamente la publicidad activa forma parte del contenido del derecho de acceso a la información, pues éste “no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de [...] publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros.”

Asimismo, la Ley 1712 en el artículo 4 “Concepto del derecho” afirma que: “El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública lo que a su vez conlleva la obligación de producir o capturar la información pública.”

En Colombia, la Ley 1712 de transparencia incluye determinados ítems de información obligatoria. Además, a diferencia de España, en Colombia es muy amplio desarrollo de las obligaciones de publicidad activa. El Decreto 103 de 2015, de 20 de enero, que desarrolla parcialmente la Ley 1712 describe la información obligatoria mínima en razón de la ley. Y muy especial mención merece por el grado de concreción que introduce en la información que debe publicarse la Resolución 3564 del 31 de diciembre de 2015 por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública. La tipología de la información obligatoria se ha agrupado la Resolución 3564 en distintos ítems, con una muy concreta regulación respecto de cada uno:

1. Mecanismos de contacto con el sujeto obligado (art. 1).
2. Información de interés (art. 2).
3. Estructura orgánica y talento humano (art. 3).
4. Normatividad (art. 4).
5. Presupuesto (art. 5).
6. Planeación (art. 6).
7. Control (art. 7).
8. Contratación (art. 8).
9. Trámites y servicios (art. 9.1).
10. Instrumentos de gestión de información pública (art. 10).

Cabe señalar que el detalle más concreto de la información obligatoria a publicar se contiene en el Anexo I de dicha Resolución.

También cabe destacar el “Deber de información al público” del artículo 8 del Código del Procedimiento administrativo, Ley 1437. Dicho precepto obliga a disponer “en el sitio de atención y en la página electrónica” y se indica que “para obtener estas informaciones en ningún caso se requerirá la presencia del interesado”. Se trata de información sobre normas, funciones, procedimientos, trámites, actos documentos que deben presentarse según la actuación, dependencias, localización y horarios<sup>20</sup>. También hay obligaciones de información activa en el Decreto 124 de 2016, de 26 de enero, relativo al Plan Anticorrupción y de Atención al Ciudadano<sup>21</sup>

### ***105. Calidad de la información pública y mecanismos de control de la transparencia. Indicadores y medición de la transparencia en general y en Colombia***

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

---

<sup>20</sup> “1. Las normas básicas que determinan su competencia.

2. Las funciones de sus distintas dependencias y los servicios que prestan.

3. Las regulaciones, procedimientos, trámites y términos a que están sujetas las actuaciones de los particulares frente al respectivo organismo o entidad.

4. Los actos administrativos de carácter general que expidan y los documentos de interés público relativos a cada uno de ellos.

5. Los documentos que deben ser suministrados por las personas según la actuación de que se trate.

6. Las dependencias responsables según la actuación, su localización, los horarios de trabajo y demás indicaciones que sean necesarias para que toda persona pueda cumplir sus obligaciones o ejercer sus derechos.

7. La dependencia, y el cargo o nombre del servidor a quien debe dirigirse en caso de una queja o reclamo.

8. Los proyectos específicos de regulación y la información en que se fundamenten, con el objeto de recibir opiniones, sugerencias o propuestas alternativas. Para el efecto, deberán señalar el plazo dentro del cual se podrán presentar observaciones, de las cuales se dejará registro público. En todo caso la autoridad adoptará autónomamente la decisión que a su juicio sirva mejor el interés general.”

<sup>21</sup> El mismo impone la publicación del Plan Anticorrupción y de Atención al Ciudadano y el Mapa de riesgos de corrupción en su artículo 2.1.4.8 y se impone la publicación de los anexos (art. 2.1.4.7) .

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: Reconoscibilidad 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 patrimonial 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/](http://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](http://www.agpd.es)) y un Consejo de la Transparencia ([www.consejodetransparencia.es](http://www.consejodetransparencia.es)).

En Colombia, el acceso a la información se ha considerado derecho fundamental por la vía del derecho a la petición y cuenta con el control jurisdiccional inmediato que corresponde a la tutela ante la jurisdicción.

Y en este ámbito de la transparencia activa no debe desconocerse que los indicadores habituales de transparencia. Colombia, durante muchos años los indicadores de Transparencia Internacional quedaron desfasados, si bien, desde 2015 se cuenta con unos de los más actualizados. Así puede seguirse en [www.indicedetransparencia.org.co](http://www.indicedetransparencia.org.co) <sup>22</sup> El Índice de Transparencia de las Entidades Públicas cuenta con tres instrumentos de evaluación Nacional, Departamental y Municipal<sup>23</sup>. Se trata de un índice muy desarrollado y positivo. Por lo que ahora interesa, en el mismo no se distingue expresamente si los indicadores de publicidad activa cuyo cumplimiento valora son los de la ley u otras normas o se va más allá de lo que es obligatorio normativamente .

---

<sup>22</sup> Los documentos metodológicos pueden seguirse en <http://www.indicedetransparencia.org.co/Documentos> Según se afirma, para obtener información detallada sobre el proceso de cálculo del Índice, hay que remitirse al documento Metodológico Índice de Transparencia Municipal y Departamental 2013 – 2104 en [www.transparenciacolombia.org.co](http://www.transparenciacolombia.org.co)

<sup>23</sup> 1. El Índice de Transparencia Nacional que evalúa entidades de las tres ramas del poder público, los órganos de control y el Ministerio; 2. El Índice de Transparencia Departamental, el cual evalúa la gestión centralizada de las gobernaciones y las contralorías departamentales y 3. El Índice de Transparencia Municipal, diseñado para evaluar la gestión central de las alcaldías.

## 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.

En Colombia, hay experiencias importantes de “Urna de cristal”, bien valoradas internacionalmente. Asimismo el ya varias veces referido Manual del Gobierno en línea 3.0 tiene su política 6 de “Democracia en línea”, siendo que se detallan no pocas acciones concretas en la línea participativa (ver págs. 67 y ss.) El planeamiento es excelente, si bien, la regulación e imposición jurídica del uso de medios electrónicos ha sido bastante mejorable. En esta dirección cabe recordar que la reciente Ley estatutaria 1757 de 2015 (julio 6) de participación es más que tímida, sino anacrónica por su casi inexistente referencia al uso de TIC para la participación.

Así, el artículo 2 señala los medios electrónicos y la utilización de TIC “cuando sea posible” para “discusiones que se realicen para la formulación de la política pública de participación democrática”. El artículo 53 afirma el compromiso de “realizar y generar espacios y encuentro presenciales, y a complementarlos con espacios virtuales, o a través de mecanismos electrónicos, siempre y cuando existan condiciones para ello, para la participación ciudadana, tales como foros, mesas de trabajo, reuniones zonales, ferias de la gestión o audiencias públicas, para que los ciudadanos y las organizaciones sociales evalúen la gestión y sus resultados.” El artículo 6. 2º hace una mera referencia del uso de medios electrónicos para la inscripción de iniciativas y el 73 la inscripción “ante la Secretaría de la respectiva Corporación para que le sean remitidos vía correo electrónico los proyectos de normas radicados y los cuestionarios de control político como sus respuestas atinentes al tema de su interés.”

Una norma tan reciente sin duda que podría haber sido más innovadora en estas cuestiones.

## **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&IID=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 aquella (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. Así 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 6°).

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" (n° 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" (n° 122).

Pues bien, lo cierto es que la Corte Constitucional colombiana es posiblemente el tribunal que más se ha centrado en la importancia de esta cuestión.

### ***109 La Corte Constitucional colombiana ha profundizado en el tratamiento jurídico de la Libertad de expresión en internet cuando la ejercen individuos, medios de comunicación y grandes prestadores en internet***

La libertad de información y expresión no sólo protege a Google, sino también a los usuarios de las redes sociales. Ya en la Sentencia T-550 de 2012 la Corte recordó la referida Declaración Conjunta Sobre la Libertad de Expresión en Internet, de la Relatoría Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión del 1° junio 2011 que reconoce la libertad de expresión a medios de comunicación y usuarios de internet.

Así, en la Sentencia T-050/16 (mujer se negó a retirar de la red social Facebook una publicación acompañada con una foto, relacionada con el no pago de una obligación dineraria a cargo de la accionante ) se recuerda que "lo publicado en redes sociales está amparado por la libertad de expresión, pero también está sujeto a los límites [...]el amparo de dicha garantía y sus respectivos límites, se aplica a internet y las redes sociales de la misma manera que a los demás medios de comunicación". Y hay que subrayar que se afirma también el carácter prevalente de la libertad de expresión también ejercida por los individuos en internet, si bien "a pesar de su carácter prevalente no carece de límites".

En todo caso, en esta Sentencia T-050/16 se proyecta la prevalencia de la libertad de expresión ya sea de un medio de comunicación o de un individuo en internet: "dado que la libertad de expresión guarda primacía frente a ciertos derechos, debe estudiarse en cada caso concreto si las circunstancias fácticas se enmarcan o no dentro de los límites establecidos para tal garantía y no realizar una censura previa de manifestaciones como las aquí estudiadas, pues, como se observó, tal actuación se encuentra expresamente prohibida por nuestra Carta Política."

Y en esta Sentencia T-050/16 se profundiza en la diferencia entre medios de comunicación y usuarios individuales en libertad de expresión y responsabilidades, para señalar que respecto de "la evaluación del correcto ejercicio de la libertad de expresión las reglas aplicables son las mismas para ambos":

"si bien puede existir distinción entre las redes sociales y los medios de comunicación como herramientas para el ejercicio de la libertad de expresión, por ejemplo: en términos de acceso en el entendido de que es mucho más sencillo acceder a la plataforma de una red social que a un medio de comunicación, también en materia de controles institucionales que son mucho menores en las primeras, o en aspectos de atribución de responsabilidad; lo cierto es que en la evaluación del correcto ejercicio de la libertad de expresión las reglas aplicables son las mismas para ambos, lo que

implica que si existe vulneración, se le atribuirá responsabilidad a quien vulnere otros derechos fundamentales a través de estos, ya sea individualmente a quien realizó la publicación vía red social o al medio de comunicación, como al autor del mensaje transgresor, según sea el caso.”

### ***110 La Corte colombiana afirma la conexión de la libertad de expresión con la arquitectura de internet y el principio de neutralidad***

Como se dirá, fue importante la sentencia inicial sobre estos temas de la Corte constitucional colombiana, la sentencia T-040 de 2013 que hizo referencia a cuestiones de libertad de expresión en internet y derecho al olvido. No obstante, más importante es la Sentencia T-277/15 pues además de no hacer responsable a los intermediarios como Google “Adicionalmente, estima necesario señalar que la razón para no acceder a la desindexación consiste en la protección del principio de neutralidad de la red que, como ya se mencionó, solo puede ser restringida en situaciones excepcionales”. Y es que se afirma la íntima conexión de la “arquitectura de internet” con la libertad de expresión y el derecho de acceso a la información de la ciudadanía del artículo 20 de la Constitución. Se vincula la neutralidad de la red y la libertad de expresión, de modo que una restricción a la neutralidad exige el escrutinio tripartito de esta libertad:

“una afectación de la neutralidad de la red implica a su vez una intromisión con el derecho fundamental a la libertad de expresión e información de todos los usuarios de la red que, por lo tanto, ha de estar sujeta a la prueba tripartita antes mencionada”. La desindexación de la información por Google “representa una afectación quizá más gravosa al derecho a la libertad de expresión que la misma eliminación de contenidos”.

### ***111. Garantías frente al cierre de webs o al corte de acceso o filtrado de contenidos en internet***

En su momento se abordó el “ius communicationis” 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<sup>24</sup>, pese a que parece que se está generalizando en la red.

---

<sup>24</sup> 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).

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 ejercicio 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.

***112. Precisamente en Colombia se afirma la no responsabilidad de los intermediarios en internet ni de Google para evitar la censura en internet y afectar a la neutralidad en internet que exige la libertad de expresión***

Respecto de la responsabilidad de los intermediarios, la Corte Constitucional colombiana en su Sentencia T-277/15 deriva la no responsabilidad general de los intermediarios por los contenidos, en razón de la libertad de expresión: “La libertad de expresión [...] protege que el contenido expresado se difunda y llegue a otros [...] imponer responsabilidades a los intermediarios de Internet por los contenidos transmitidos limitaría de forma importante la difusión de ideas por este medio de comunicación, pues les daría el poder para regular el flujo de información en la red.

Respecto del caso particular de Google, la Corte Constitucional colombiana ya en su sentencia relativa a un problema de derecho al olvido de Google respecto de información de un medio de comunicación, ya en su sentencia T-040 de 2013:

*“el responsable de la información emitida, y por ende de su posible rectificación, es el medio de comunicación que recolectó, analizó, procesó y divulgó la noticia, es decir, la casa Editorial El Tiempo, a través de su página electrónica oficial. En ese orden a quien procede realizar la rectificación [...] Google Colombia S.A. no es responsable de la noticia*

*es un simple motor de búsqueda al cual no se le puede endilgar la responsabilidad* (Sentencia T-040 de 2013, MP. Jorge Ignacio Pretelt Chaljub, AV. Alexei Egor Julio Estrada).

En cualquier caso, en la Sentencia T-277/15 entiende que no puede hacerle responsable pues ello lo convertiría en un “censor o controlador de contenidos”, afectando a la arquitectura misma de internet desconociendo sus principios. Ello comprometería el derecho a la información de la ciudadanía:

*“Además de hacerle responsable [a Google] por una información que aquel no generó y por la que no debe endilgársele responsabilidad, esta medida entraña la posibilidad de convertir al motor de búsqueda en un censor o controlador de los contenidos publicados por los usuarios que acceden a la red. Esto, a juicio de la Sala, y como lo advierten varios de los intervinientes, puede afectar la arquitectura de Internet por la vía de desconocer sus principios rectores de acceso en condiciones de igualdad, no discriminación, y pluralismo. A su vez, se declara que una intervención de este tipo no solo tiene una mera influencia técnica en el funcionamiento de un medio de comunicación sino que compromete, además, el derecho a la información de las personas que acceden al servicio, es decir, todos los ciudadanos.”*

Se considera que obligar al bloqueo de resultados sería un control previo contrario al principio de neutralidad que debe cumplirse:

*“ordenar al motor de búsqueda Google.com que bloquee de sus resultados el portal de Internet del medio de comunicación donde se informa de la captura e investigación penal en contra de*

Gloria, supondría implementar una modalidad de control previo contraria al principio de neutralidad.”

### ***113. Proyección de algunas categorías y garantías de las libertades informativa a internet***

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

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

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

En general, los tribunales no han querido ser severos y restrictivos en la consideración de si una información no era objetivamente de interés público. Es muy posible que hasta ahora los tribunales implícitamente considerasen que la información tenía interés público sólo por el hecho de que la noticia se recogiera en los medios tradicionales. Los medios de comunicación clásicos eran un filtro *material* –no jurídico- para determinar qué información gozaba de interés público

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

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](http://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.

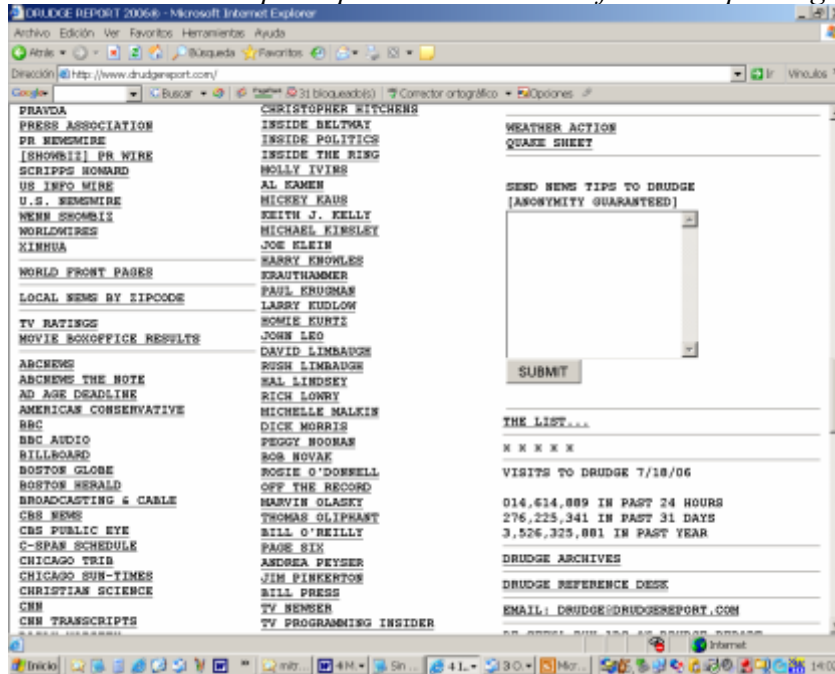
[http://en.wikipedia.org/wiki/Obsidian\\_Finance\\_Group,\\_LLC\\_v.\\_Cox](http://en.wikipedia.org/wiki/Obsidian_Finance_Group,_LLC_v._Cox)

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](http://www.drudgereport.com) uno de los más visitados del mundo, “garantizaba” hasta hace pocos años el anonimato para quienes le remitan información privilegiada “tip”



[www.filtrala.org](http://www.filtrala.org) (como [www.mexicoleaks.mx](http://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.



#### ***114. 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 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 responsable 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 mismo 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 exenciones legales de responsabilidad. 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 improprios 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).*

En Colombia no tuvo éxito la ley Lleras que imponía responsabilidad a los intermediarios en internet y la cuestión queda huérfana de regulación, sin perjuicio de lo ya expuesto respecto de la regla general de neutralidad y no responsabilidad en razón de la libertad de expresión marcada por la Corte Constitucional.

### ***115. 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 unilateralmente restringir contenidos de un usuario por entenderlos contrarios a las condiciones de uso. El tribunal francés 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 libertad 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.

Según se ha expuesto en la doctrina de la Corte Constitucional, en Colombia se ha adoptado con claridad la necesidad de evitar que los intermediarios privados pasen a ser censores, de modo

que no se les imponga el control obligatorio. Más allá de que *deban*, la cuestión es la posibilidad de que *puedan* hacerlo.

***116. 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. La solución europea***

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 afeción 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](https://support.google.com/legal/contact/lr_eudpa?product=websearch)

The screenshot shows the Google 'Ayuda de Legal' (Legal Help) page. The main heading is 'Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea' (Request for removal of search results under European data protection law). Under 'Antecedentes' (Background), it explains that since May 2014, a European Court of Justice ruling (C-131/12) allows users to request removal of search results if their privacy rights outweigh the public interest. It also notes that Google will balance individual privacy against the public's right to know. A note states that a digital ID document is required, and fields marked with an asterisk are mandatory. A dropdown menu for selecting a country is visible, with 'Seleccionar uno' (Select one) as the current selection. The 'Información personal' (Personal information) section is partially visible at the bottom.

*Resultados desde mayo de 2014 del ejercicio del derecho al olvido en Google en la Unión Europea*

<https://www.google.com/transparencyreport/removals/europeprivacy/>

## Número total de solicitudes de retirada de URLs

En el gráfico siguiente se muestran los datos sobre los porcentajes de URL que hemos revisado y procesado. Las cifras de la derecha se basan en la cantidad total de solicitudes recibidas. Estos datos se remontan al lanzamiento del proceso de solicitudes oficial el 29 de mayo de 2014.



## Sitios más afectados

En la lista siguiente se destacan los dominios en los que hemos retirado la mayoría de las URL de los resultados de búsqueda.

Estos diez sitios principales suman el **8%** del total de URLs que se ha solicitado que se retiren de los resultados de búsqueda.

www.facebook.com URL retiradas: 15375	profileengine.com URL retiradas: 10313	annuaire.118712.fr URL retiradas: 8469	www.youtube.com URL retiradas: 7802	groups.google.com URL retiradas: 7678
twitter.com URL retiradas: 6594	plus.google.com URL retiradas: 6375	badoo.com URL retiradas: 5189	www.wherevent.com URL retiradas: 4808	www.192.com URL retiradas: 4015

### ***117 La solución de la Corte Constitucional colombiana respecto del derecho al olvido y Google. Google no tiene que desindexar, la web de origen debe utilizar mecanismos como el robot.txt para que Google no indexe***

En la Sentencia T-260 de 2012 la Corte ya afirmó el especial peligro para los derechos de la personalidad que implican las nuevas tecnologías y redes sociales, se indicó que, si bien en estos espacios deben regir normas similares a los medios no virtuales, acceder a estos implica un riesgo mayor para las garantías fundamentales pues, la posibilidad de hacer pública información y datos personales a través de perfiles creados por quienes las utilizan, implica un más alto grado de vulnerabilidad de los derechos antes mencionados. Se afirmaron los peligros de que *“Los datos personales pueden ser utilizados por terceros usuarios malintencionados de forma ilícita. Existe la posibilidad de que traten y publiquen en la red información falsa o sin autorización del usuario, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho.”*

En la Sentencia T-277/15 se deja claro que el origen de la información en la web, el responsable de la web debe utilizar los mecanismos como el robot.txt que indica a Google que no indexe la información. Y ésta solución sí que es proporcional:

*“por medio del uso de estas herramientas técnicas [robots.txt” y “metatags] es factible mantener la publicación de la noticia, sin que se corra el riesgo de alterar la verdad histórica y evitando, en todo caso, que el dato negativo que afecta los derechos de la accionante resulte accesible de manera indiscriminada a partir de la mera digitación de su nombre en un buscador de internet. [...] recursos técnicos que permiten encontrar un balance entre el derecho del medio de comunicación a publicar la noticia que informa sobre la captura de la accionante y del derecho de la señora Gloria a proteger su intimidad”*

*“debe ordenarse al medio de comunicación que proceda a hacer uso de una herramienta técnica como “robots.txt”, “metatags” u otra similar”*

*“Si bien esta medida representa una limitación al derecho a la libertad de expresión de la Casa Editorial El Tiempo, esta es menos lesiva que aquella que ordena la eliminación de la información de red, por cuanto al menos permite que el suceso que dio lugar a la noticia sea publicado”*

### ***118. Olvido y límites de información sobre comisión de delitos y decisiones judiciales en Colombia***

Ya hubo un caso de olvido respecto de sentencias judiciales de carácter penal en sentencia T-020 de 2014, fallado a favor del amparo solicitado (M. P. Luis Guillermo Guerrero Pérez. S. V. Gabriel Eduardo Mendoza Martelo). Esta situación suponía “una carga desproporcionada en su contra, creando una nueva fuente de consulta de antecedentes judiciales, por fuera de los controles limitados circunstancia ha generado una situación de estigmatización por virtud de la cual ha visto frustradas oportunidades laborales y comerciales!

A partir de esta solución la Sentencia T-277/15 formula los elementos respecto de la difusión de información judicial penal. “la publicación del fallo, que hizo accesible los datos a través de internet, desconocía los principios de finalidad y circulación restringida de los datos personales”. Se recuerda en este sentido las condiciones que deben darse:

-“noticias referidas a procesos de naturaleza penal o que den cuenta de la comisión de delitos por parte de personas determinadas”

-“la posibilidad de consultar la noticia permanece de forma constante e ininterrumpida en el tiempo”.

-“que si se trata de un personaje con notoriedad pública o un servidor público, o los hechos que registra la noticia responden a la comisión de delitos de lesa humanidad o que hayan lesionado de forma grave los derechos humanos, el acceso a la información generada no debe restringirse”.

-“el derecho de la persona a que se restrinja el acceso a la información relativa a la conducta que quebrantó las normas penales se origina desde el momento mismo en que el procedimiento penal concluye a su favor”.

-debe actualizarse la información judicial penal para ajustarse a la veracidad: “Debe entonces, reportarse en forma completa el desenlace del proceso al cual fue vinculada la actora.”