CENSURA EN LA RED: RESTRICCIONES A LA LIBERTAD DE EXPRESIÓN EN INTERNET

Ángel L. Rubio Moraga
Universidad SEK de Segovia

Resumen

El control de la información ha constituido siempre la base del poder del Estado a lo largo de la historia. En este contexto, los medios de comunicación son vistos como el gran enemigo del régimen, más aún si éste se viste de colores autoritarios. Sin embargo, este modelo de control se ve en la actualidad ante una encrucijada: ¿Cómo se puede vigilar y controlar la universal, escurridiza e intangible Internet?. Tal y como ocurre con el resto de medios de comunicación, Internet también es objeto de prohibiciones, cortes, omisiones, etc. y es que la censura también existe en la Red. Ver la situación actual y posible evolución de esta peligrosa herramienta contra el derecho a la información y la libertad de expresión será el objeto del presente estudio.

Palabras Clave: Internet, Censura, Autoritarismo, Democracia, Libertad de Expresión

1. Introducción

Internet siempre ha supuesto una pesadilla para los gobiernos. Por un lado no pueden dejar de fomentar su desarrollo e implantación masiva para no quedar descabalgados de la Sociedad de la Información; por otro, la libertad y el anonimato que corre por las redes se ven como una amenaza. Así, son muchos los Estados que censuran de un modo u otro los contenidos que perjudican sus intereses. Algunos incluso pueden castigar a quienes expresan en el ciberespacio sus opiniones contrarias al "interés nacional" o a lo "políticamente correcto". Si ninguna de estas dos medidas alcanza el objetivo deseado, las restricciones se mueven hacia lo seguro: vetar el contenido y dificultar el acceso haciendo de Internet un lujo al alcance de unos pocos. Así, millones de ideas quedan silenciadas y otras tantas escondidas. Mientras, la libertad de expresión y el derecho a la información, protegidos por el artículo 19 de los Derechos Humanos, quedan reducidos a una mera anécdota en cuanto a Internet se refiere.

Los atentados del 11 de septiembre de 2001 en las ciudades de Nueva York y Washington han supuesto la línea de inflexión en cuanto a la lucha por la libertad de la Red y gran parte de los derechos conquistados están a punto de perderse tal y como reflejan dos informes publicados a finales de 2002, uno de *Reporteros sin Fronteras (RSF)*[1] y otro realizado conjuntamente por *Privacy International* y el *Electronic Privacy Information Center*[2].

La cruzada antiterrorista iniciada tras los atentados por EE.UU. y en la que en mayor o menor medida se encuentra inmerso medio planeta ha conducido a una serie de medidas de control masivo sobre la Red. Según el estudio de *RSF:*

[1] Reporteros sin Fronteras, "Los enemigos de Internet" (http://www.rsf.fr/article.php3?id_article=3669)
[2] Electronic Privacy Information Center (EPIC): http://www.epic.org

"Cuando se cumple un año de los trágicos acontecimientos de Nueva York y Washington, la Red puede muy bien figurar en la lista de "daños colaterales" de la deriva generalizada de la seguridad. A causa de ello, se han amputado las libertades digitales fundamentales" [3].

En esta ocasión, sin embargo, y a diferencia de lo que suele ocurrir en el mundo físico, la necesidad de controlar el medio no se limita a los países con regímenes autoritarios, sino que son también las democracias occidentales, baluartes de la libertad de expresión, las que pretenden ejercer algún tipo de control sobre la Red desde el marco legislativo como consecuencia del temor que genera un medio incontrolable, en el que los tradicionales papeles de emisor-receptor se difuminan e invierten para convertir a todo ciudadano en intermediario entre la información y su difusión al gran público. De este modo, la censura, practicada sobre la Red adquiere una doble vertiente, la explícita, llevada a cabo por los gobiernos de los regímenes más autoritarios, y la implícita o encubierta que sería la practicada en los países democráticos. Si bien la única diferencia entre ambas es que este último tipo de censura es aún más insidioso que la censura explícita, puesto que se practica sin que los ciudadanos sean conscientes muchas veces de ella y la justifican con fórmulas de protección de la infancia de contenidos pornográficos y dañinos, o de lucha contra información ilícita o xenófoba. El resultado es la elaboración de leyes restrictivas que ponen en peligro el derecho a la libertad de expresión.

2. Formas de Censura en la Red o "Cómo poner vallas al campo".

Los métodos para censurar la Red son múltiples y variados, dependiendo del tipo de control que el gobierno en cuestión quiera ejercer, por lo que se han desarrollado diferentes estrategias que van desde las más a las menos restrictivas. Sin embargo, la mayoría de los países utilizan una combinación de las mismas para ejercer su censura. Ahora bien, frente a ellos, existen otros modos, éstos dedicados a su combate, es la denominada contracensura.

- La forma más directa de censura en los países autoritarios es la prohibición de acceso a Internet, tal y como ocurrió en Afganistán con el gobierno talibán o como ocurre en Corea del Norte donde Internet es inexistente, a pesar de los tímidos intentos del régimen de aquel país.
- Un segundo grado de censura es el que ejerce, por ejemplo, el gobierno comunista de Fidel Castro, cuyo caso analizaremos más adelante, y que en vez de prohibir Internet, hace que el acceso a la Red pase por un restrictivo control basado en la expedición de autorizaciones exclusivas a personas "de confianza".
- La monitorización sería el siguiente escalón, sin embargo, el país que mejor lo ejemplifica es uno de los más autoritarios y restrictivos. Es el caso de China, que aunque permite el acceso a Internet, los ciudadanos de este país se encuentran vigilados por una brigada policial encargada de monitorizarlos. Rusia, Singapur, India y algunos países de África del Norte y de Oriente Medio practican también la censura mediante la monitorización de contenidos.
- El filtro de contenidos y el bloqueo de *sites*, por último, serían las categorías menos restrictivas. El método consiste en obligar a los proveedores de servicio de Internet del país (ISP[4]) a instaurar filtros en sus servidores con el fin de bloquear los web "indeseables". Arabia Saudí es uno de los países que lo practica.
- La clasificación hecha por CEIP (Carnegie Endowment for International Peace[5]), organización norteamericana sin ánimo de lucro que estudia el fenómeno de la

[3] Reporteros sin Fronteras. *Op. Cit.*
[4] Internet Service Provider (Servidor de Servicio de Internet).
[5] CEIP, Carnegie Endowment for International Peace: http://www.ceip.org

globalización, destaca además de los métodos mencionados, considerados reactivos, otras formas proactivas que ayudan a los gobiernos a imponer su control sobre la información. Campañas de propaganda en Internet, obligación encubierta a los ISP para que pertenezcan al estado, creación de intranets nacionales sustitutivas de la Red global, implementación de servicios de *e-government* que aumentan la satisfacción de los ciudadanos con el gobierno y el uso de la preponderancia informativa para luchar contra la oposición al poder son algunas de ellas.

- Por último, destacar las estrategias, más difíciles de definir, puestas en práctica por los gobiernos occidentales para ejercer sus formas de control de contenidos en la Red. La creación de leyes o propuestas de regulación son sus cauces bajo el pretexto de la lucha contra el crimen o la protección de la infancia para lo que se consiente el uso de software de filtrado como *Net Nanny*, *Cybersitter* o *X-stop*, aplicaciones basadas en imperfectas "listas negras" de web por palabras clave que prohíben en ocasiones el acceso a *sites* inofensivos.
- Relacionado con el control de la Red, sin llegar a ser censura propiamente dicha, pues no interfiere el derecho a la información y la libre opinión, pero sí a otro íntimamente ligado como es el derecho a la intimidad de las comunicaciones, el uso de redes de espionaje como *Echelon* o programas como *Carnivore* pueden considerarse otras formas legítimas de control.

Frente a estas medidas, Internet se presenta igualmente como plataforma de combate contra los controles ejercidos. Así, medios alternativos de información[6], grupos de *ciberderechos*, sistemas de anonimato o el llamado *hacktivismo ético* son algunas de las formas de frenar el control desmedido de los gobiernos. La idea es burlar la censura de la Red porque si la libertad de expresión en Internet es evidentemente peligrosa los obstáculos a dicha libertad son más peligrosos aún.

3. La censura del ciberespacio en los regímenes autoritarios.

El control de la Red está a la orden del día en los países con regímenes autoritarios, que ni siquiera respetan derechos tan básicos como el de la vida. No es una medida nueva: es la extensión lógica del control informativo que este tipo de gobiernos ejercen en los medios tradicionales de comunicación, pues no hay nada más peligroso para su 'estabilidad' que la libertad de expresión, especialmente si se realiza a través de una plataforma de alcance mundial como Internet.

Estas naciones mantienen una relación dual con Internet, ya que por un lado animan su desarrollo para la propaganda estatal o con fines económicos, mientras que por otro controlan la "contaminación" que pueda penetrar del exterior y las contestaciones internas. Esa política se ha acentuado con la campaña antiterrorista internacional iniciada tras el 11-S y los "enemigos de Internet" han reforzado sus dispositivos policiales y legislativos para cercar la Red, a la vez que han aumentado la presión sobre los ciberdisidentes[7].

---

[6] SHAPIRO, A. L.. *El mundo en un clic: cómo Internet pone el control en sus manos (y está cambiando el mundo que conocemos),* Barcelona, Grijalbo Mondadori, 2001. Este autor afirma que los primeros activistas que utilizaron la Red como plataforma de denuncia fueron los demócratas serbios seguidores de la emisora *Radio B92* (http://www.b92.net). Los creadores de esta popular cadena de radio comenzaron a emitir a través de la Red tras ver cómo las autoridades del entonces presidente de Serbia, Slobodan Milosevic, cerraban sus puertas. Este intento frustrado de censura, no obstante, permitió descubrir el poder de Internet: en pocas semanas el mundo entero conocía los movimientos de los activistas serbios contrarios al régimen de Milosevic y en pocas semanas *Radio B92* volvía a emitir por las ondas hertzianas como consecuencia de la presión internacional.

[7] El 20 de junio de 2002, el gobierno tunecino condenó a Zouhair Yahyaoui a dos años y cuatro meses de cárcel por haber creado un sitio de Internet (*Tunezine.com*) demasiado crítico para con el régimen establecido.

El caso más palpable de violación de los derechos en la Red lo representa China, para cuyo gobierno el control de la información que fluye por Internet es una de las principales preocupaciones. Y es que, con casi 30 millones de internautas y el potencial de convertirse en el país asiático con la mayor audiencia de Internet en este miso año, China, que se conectó en 1993 y permite disponer de cuentas privadas desde 1995, considera al medio una herramienta clave para modernizar su economía. Por ello, en lugar de prohibir el acceso, lo ha impulsado pero limitando los contenidos mediante el control de los ISP, el bloqueo de *sites*, el cierre de cibercafés y la aplicación de penas durísimas a los ciberdisidentes pues, desde enero de 2002, el envío de material "secreto" o "reaccionario" a través de la Red se castiga con la pena capital.

Las autoridades chinas obligan a los usuarios de Internet a inscribirse en el registro de un cuerpo especial de la policía. Más allá de bloquear sitios espinosos para el régimen de Jiang Zemin, como los relacionados con los derechos humanos o la independencia del Tíbet, prohíben el acceso a las páginas de *The New York Times, The Wall Street Journal* o la *CNN*. Protegido el espionaje del correo electrónico por ley (los ISP están obligados a rastrear las cuentas de correo y a cortar la conexión e informar a la policía de cualquiera que introduzca un mensaje "subversivo"), resulta sencillo cazar a ciberdisidentes para proceder a su inmediata encarcelación[8].

Además de las críticas al régimen del presidente Jiang Zemin, la censura china se extiende sobre cualquier contenido de carácter sexual y religioso, con especial hincapié en el movimiento espiritual *Falun Gong* y las web que lo promueven como *Clearwisdom.com*, tildado por el Partido de "culto demoníaco". A todo ello habría que sumar quizá el caso más sonado de la historia censora de China y que fue llevado a cabo por la administración sobre los portales nacionales con motivo del X aniversario de la matanza de estudiantes en Tiananmen.

A pesar de ello, el número de internautas no ha parado de crecer en China. Casi 30 millones de ciudadanos, sobre una población total de 1.300 millones, se conectan a Internet. De los usuarios habituales de la Red, cerca de 4,5 millones se conectan en cibercafés. Razón esta por la que el gobierno chino, en previsión de no poder controlar el crecimiento de este tipo de establecimientos, decidió cerrar 17.488 cibercafés el 20 de noviembre de 2001, medida que se ha repetido con posterioridad si bien ha afectado a un menor número de establecimientos. El gobierno chino justificó la medida afirmando que estaban relacionados con páginas web pornográficas o consideradas "subversivas". Otros 28.000 cibercafés fueron obligados a instalar sistemas de vigilancia que permitieran al poder controlar a sus internautas. Ante esta situación resulta chocante la existencia de la web *Derechos Humanos en China*[9] a través de la cual se pretende informar "completa y objetivamente al mundo entero sobre el desarrollo de los derechos humanos en China". Lo más sangrante es que dicha página ha sido creada por la ONG *Comité de Estudios de Derechos Humanos*, cuya vinculación directa con el gobierno chino ha sido sobradamente demostrada.

---

[8] En Mayo de 2001, el gobierno chino detenía a Wang Jinbo por haber exigido la revisión del veredicto oficial sobre el movimiento democrático de 1989, así como por reclamar la liberación de prisioneros políticos a través de Internet. En diciembre fue condenado a 4 años de prisión por subversión (Más información: http://www.dfn.org/focus/china/luxinhua-sentence.htm). En abril de 2001 la policía detuvo al veterano activista Chi Shouzhu, que en 1999 quedó libre tras 10 años en prisión por haber participado en las revueltas pro-democráticas del 89, por el simple hecho de descargar material pro-democracia desde Internet e imprimirlo (*The Guardian*, 19 de Abril de 2001). Un mes antes, un ingeniero había sido detenido por colgar en su web ensayos políticos sobre la situación de Taiwán, a la vez que hacía una vehemente crítica del "alma del comunismo". En Enero de 2002 la *BBC* se hacía eco de dos nuevos ciberdisidentes encarcelados (*BBC News Online,* "Chinese internet dissidents jailed", 14 de Enero de 2002).

[9] *Human Right in China*: http://www.hrichina.org

Otros países asiáticos, como Singapur[10], Malasia o Vietnam, bloquean el acceso a un centenar de páginas sin ningún tipo de pudor a la vez que, irónicamente, fomentan el uso de Internet entre su población.

Sin embargo, hay casos más extremos, como ocurre con Corea del Norte. El régimen comunista y dictatorial de Kim Jong-Il ha mantenido al país totalmente cerrado al exterior. Debido a ese afán de aislamiento, Internet no existe en todo el país. No hay ni un solo ISP, ni siquiera estatal, aunque empiezan a surgir las primeras páginas web oficiales, eso sí, albergadas en Japón.

Más directa y sin duda eficaz es la medida adoptada por los gobiernos cubano y marroquí consistente en encarecer el servicio de conexión. De esta forma se restringe el acceso y se limita la navegación, hasta el punto de que en Cuba tan sólo existen unas 40.000 cuentas de correo electrónico (de las cuales sólo 3.600 son consideradas legales por las autoridades cubanas) y se calcula que hay unos 50.000 internautas en toda la isla[11], una cifra que se debe en parte al altísimo precio de las telecomunicaciones (de baja calidad y sin apenas líneas telefónicas) y a la pobreza causada por el embargo norteamericano, y, en parte, al férreo control sobre el acceso que ejerce el gobierno, ya que el acceso a Internet es proporcionado por un único proveedor de servicios y los usuarios de Internet han de registrarse ante las autoridades y justificar su necesidad de uso. Si éstas aceptan su petición, les hacen firmar un contrato de utilización con cláusulas restrictivas. El fruto de esta regulación es que sólo la nomenclatura cubana tiene acceso a la Red: políticos del régimen, altos funcionarios, intelectuales y periodistas afines al poder, las embajadas y las empresas extranjeras.

Igualmente significativo es el hecho de que en todo el país sólo haya un cibercafé público –hay otro restringido a artistas del sindicato oficial-, abierto a raíz de la afluencia de turismo, y cuyo precio en 2003 era de 5 dólares/hora, la mitad del salario mensual medio de los cubanos.

En 1996 el gobierno de Castro adoptó el Decreto-Ley 209 "Acceso desde la República de Cuba a la red informática global" que, además de montar conexión directa con EE.UU. (antes la había con Canadá) instauró que la utilización de Internet no debía hacerse "violando los principios morales de la sociedad cubana ni los textos de las leyes del país" así como que los correos electrónicos no deben "comprometer la seguridad nacional". En el 2000, Castro creó un Ministerio de Informática y Comunicaciones con el objetivo de "transformar Cuba en una Sociedad de la Información"[12], a pesar de que el dirigente cubano considera la Red como un "instrumento de manipulación del capitalismo, en el que la mayor parte de la información está disponible en inglés".

Como consecuencia de esta represión, ha surgido un verdadero mercado negro de direcciones de correo electrónico que sirve a los pocos cubanos que disponen de un ordenador, mientras que los periodistas independientes, para burlar la censura, han de enviar sus artículos a los responsables de los *sites* que operan desde el exilio donde luego los publican. Una actividad que ha llevado a la cárcel a muchos, como es el caso de José Orlando González Bridón, condenado a dos años por una información publicada en *Cuba Free Press*.

---

[10] En las últimas elecciones presidenciales celebradas en Singapur tan sólo se autorizó a las webs de los partidos inscritas en la *Singapore Broadcast Authority (SBA*, http://www.sba.gov.sg/internet.htm) a que pudieran hacer campaña por Internet, el resto debían ser retiradas bajo penas de cárcel de un año.

[11] *The Chicago Tribune*, "Bleak Future for Cuban Internet", 1 de Marzo de 2001.

[12] Para conseguir este objetivo el gobierno cubano cuenta con numerosos *sites* oficiales, además de los diarios *Granma* (http://www.granma.cu), *Juventud Rebelde* o *Trabajadores*, y la Agencia Nacional de Información *Prensa Latina*

En parecidas circunstancias, aunque con un menor control por parte de las autoridades, se encuentran los internautas de países como Kazajstán y Kirziguistán , donde se cobran sumas auténticamente prohibitivas por el simple acceso a la Red.

Otros países prefieren recurrir al uso de filtros que hacen las veces de pre-censor y que impiden el acceso a sitios "nocivos" y mantienen alejado aquello que sería negativo para la mente de sus ciudadanos en función de las tradiciones culturales o religiosas de cada país. Entre estos se encuentran Irán, Irak, Arabia Saudí, Bahrein, Emiratos Árabes, Jordania, Kuwait o Egipto.

En Irán, por ejemplo, los ISP se ven obligados por el monopolio estatal de telecomunicaciones a bloquear los *sites* "peligrosos" por ser inmorales o contrarios a la seguridad del Estado. Además, los jóvenes menores de 18 años tienen prohibido conectarse o entrar en cibercafés –razón por la cual en la capital, Teherán, se cerraron 400 de los 1500 existentes-, extendiendo la censura en la Red hasta un nivel similar al del resto de medios de comunicación, abarcando temas tan dispares como la sexualidad, las críticas a los regímenes islámicos o la simple mención de los Estados Unidos o Israel.

En Irak, en los meses previos al último ataque norteamericano, los internautas sólo contaban con un ISP (*Uruklink*[13]) y escasos cibercafés en la capital donde sólo podían conectarse a las páginas que no contradijeran los "preceptos de la religión islámica".

En Egipto, las autoridades han establecido un sistema de vigilancia sobre cualquier contenido de carácter nocivo y perjudicial para las creencias religiosas del país, persiguiendo todo tipo de "perversiones", entre las cuales la homosexualidad juega un papel destacado y es, ante los ojos de las autoridades religiosas de dicho país, una desviación imperdonable[14].

El gobierno Saudí, por su parte, ha construido un sistema de filtración de direcciones y contenidos (*Djeddah*) para controlar el flujo de información. Incluso los Emiratos Árabes Unidos, el país mejor conectado del Golfo Pérsico, y con una legislación que permite la libertad de expresión, en la práctica controla los contenidos que no interesan al régimen mediante su único ISP *Etisalat*[15], por supuesto de carácter estatal.

En cuanto a Afganistán –conocido por la violación sistemática de los derechos humanos a cargo del régimen talibán-, es otro de los grandes censores de Internet, un medio al que se opone radicalmente por albergar contenidos "obscenos, inmorales y anti-islámicos".

Sin apenas infraestructuras de telecomunicaciones, mermadas por más de dos décadas de guerra, y tras la prohibición impuesta por el régimen talibán al llegar al poder en 1996, para los afganos es literalmente imposible acceder a la Red. Tan sólo pueden hacerlo los dirigentes y los exiliados. Los primeros conectándose a través de las líneas de teléfono proporcionadas por su vecino Pakistán (hasta este último conflicto, colaborador) donde también se encontraba alojada la web oficial del movimiento talibán *afghan.ie.com* (actualmente inaccesible), y los segundos a través de satélite o de redes de otros países, como el caso de Abdullah Qazi, exiliado a EE.UU. y creador del web *Afghanistan Online*[16].

Por último, en Europa, destacan las antiguas repúblicas soviéticas como las más restrictivas de Internet. Quizá el caso más notorio sea el de Bielorrusia, en cuyas últimas elecciones presidenciales, de las que salió vencedor su anterior presidente Alexandr Lukashenko, se bloquearon los *sites* de la oposición y de los medios de comunicación críticos con el régimen de Lukashenko, así como la versión digital del diario independiente *Belaruskaya Delovaya Gazeta* y el extracto de noticias enviado diariamente por el grupo

[13] *Uruklink*, ISP oficial de Irak: http://www.uruklink.net

[14] En diciembre de 2001 un tribunal egipcio condenó a prisión a dos jóvenes por incluir contenidos homosexuales en su página web y ofrecerse para mantener relaciones sexuales con otros chicos

[15] *Etisalat*, ISP oficial de los Emiratos Árabes Unidos: http://etisalat.co.ae

[16] *Afghanistan Online (privada)*: http://www.afghan-web.com

antigubernamental *Charter 97*, tarea fácil pues el país sólo cuenta con un ISP, *Beltelecom*[17], que es de carácter estatal.

4. La censura de la Red en los países democráticos

La actitud de los diferentes estados vistos hasta ahora, sin ser justificada, no es exclusiva de los regímenes totalitarios. Bien es cierto que en los países democráticos no se puede hablar de la existencia de "censura" dada la consideración que el derecho a la libertad de expresión suele tener en la mayoría de textos constitucionales democráticos. Sin embargo, se aprecia cada vez con mayor frecuencia un gran interés por controlar los contenidos de la Red mediante la legislación. En los países democráticos, la Red es considerada como un icono de modernidad e instrumento de desarrollo económico, pero, a la vez se genera una profunda desconfianza respecto al uso que puedan hacer los ciudadanos de esa potencialidad de libre comunicación, de ahí los continuos intentos de regulación, legislación e instauración de mecanismos de control, siempre al amparo de la protección necesaria de los niños, los principios democráticos y los consumidores.

Sin embargo, tras los atentados del 11 de septiembre en Estados Unidos, estos intentos de control se han intensificado en los países occidentales de forma manifiesta. Así lo demuestra el cierre, por parte de las autoridades norteamericanas y británicas, de numerosos *sites* de musulmanes integristas por considerarlos herramienta propagandística del terrorismo, y la elaboración en EE.UU. y Francia de una normativa para regular la vigilancia de las telecomunicaciones y de Internet con el objetivo de prevenir futuros actos terroristas.

Ahora bien, el control de Internet por parte estatal no se inició a raíz de los sucesos del 11 de septiembre. Ya en 1996 el gobierno norteamericano propuso la denominada *Communications Decency Act* mediante la que se pretendían controlar los contenidos de la Red que pudieran dañar la sensibilidad de los niños y contra la que se levantaron millones de defensores de los ciberderechos hasta que finalmente fue declarada inconstitucional por el Tribunal Supremo del Gobierno Federal. Otro ejemplo lo tenemos en septiembre del 2000, cuando un tribunal francés ordenó a *Yahoo!* que impidiera la compra de artículos nazis sin importar el país de procedencia de dicho material, una sentencia que sería recurrida más tarde por la empresa norteamericana al considerar que dicho dictamen sentaría el precedente negativo de que los *sites* debieran adaptarse a las leyes específicas de cada país.

Al margen de estos casos, será a partir de finales del 2001 y como consecuencia de los atentados de Nueva York y Washington cuando la mayoría de los países democráticos se sumarán a estos intentos de controlar la libertad de expresión en la Red. Este control, en principio, se orienta hacia la conservación generalizada de las informaciones relativas a los correos electrónicos recibidos y enviados y a los sitios consultados en la Red, lo cual supone que los ISP y los operadores de telefonía se convertirán en una especie de agentes de policía, mientras que las fuerzas del orden tendrán pleno acceso a toda esa masa de informaciones[18].

---

[17] *Beltelecom*, ISP estatal de Bielorrusia: http://www.beltelecom.by

[18] En este sentido se han adoptado algunas medidas en diferentes países e instituciones de carácter internacional, como por ejemplo la *Resolución 1373* relativa a la lucha contra el terrorismo y aprobada por el Consejo de Seguridad de la ONU el 28 de septiembre de 2001; la *USA Patriot Act*, aprobada en EE.UU. el 24 de octubre de 2001, así como los decretos presidenciales de George W. Bush que precedieron y siguieron a ese texto; la *Revisión de la Directiva Europea* sobre protección de datos de telecomunicaciones, aprobada el 30 de mayo de 2002; las recomendaciones del G8 y de la *Europol*; o los numerosos proyectos de ley aprobados o presentados en los diferentes Parlamentos Nacionales, entre los que se encontraría la controvertida *Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico* (LSSI), una ley elaborada por el Ministerio de Ciencia y Tecnología español con el fin de adaptar la directiva sobre comercio electrónico 2000/31/CE de la Comisión

Pero sin duda el país más activo en la carrera por el control de la Red ha sido Estados Unidos, amparándose para ello en la lucha contra la amenaza terrorista. Así, tanto el Gobierno como el FBI han redoblado sus esfuerzos para perseguir el cibercrimen y han convertido Internet en una amenaza por donde pueden penetrar los enemigos de la patria. Sin embargo, y hasta la fecha, ni la utilización del programa *Carnivore*[19], empleado para la interceptación de datos pero poco útil para su análisis y aprovechamiento, ni la actuación de la *National Infraestructure Protection Center* (NIPC) o ciberpolicía, han tenido escaso éxito.

El 24 de octubre de 2001, la *USA Patriot Act* legalizaba definitivamente la vigilancia de la información de Internet. Mediante esta ley antiterrorista, el FBI puede fiscalizar los mensajes electrónicos y conservar y analizar el rastro de la navegación de los sospechosos. Para dotar de mayor eficacia a su *Carnivore*, el FBI planeó reorganizar la arquitectura de Internet para conducir el tráfico a unos servidores centrales donde "pinchar" sus equipos[20].

Por otra parte, y habida cuenta que la mayor parte de las comunicaciones de Internet transitan por canales situados en EE.UU., el Departamento de Justicia se siente con todo el derecho a perseguir a los ciberdelincuentes allá donde se hallen, sean o no estadounidenses, de tal forma que las autoridades norteamericanas se han convertido en una policía mundial de Internet, capaz de aplicar su ley en todo el planeta y perseguir el cibercrimen en cualquier parte del globo.

Mientras tanto, en Europa se empieza a aplicar el modelo de seguridad en Internet copiando el patrón estadounidense. Y ello, a pesar de que las democracias europeas se han opuesto tradicionalmente a todo tipo de vigilancia electrónica sobre los ciudadanos. Sin embargo, la presión norteamericana ha sido permanente desde que dio comienzo la "Cruzada Antiterrorista", dando sus frutos el 30 de mayo de 2002, cuando el Parlamento Europeo aprobó la nueva Directiva que impone a los gobiernos europeos legislar para obligar a los ISP y operadores de telecomunicaciones a conservar todos los datos de las comunicaciones (correos electrónicos, Internet, telecopias, teléfonos), así como garantizar el acceso a los mismos a las autoridades.

Con esta medida se pretenden establecer normas comunes con el objetivo de uniformar el panorama legislativo europeo en el ámbito de Internet y poder definir así el cibercrimen y armonizar las penas contra los ciberdelitos, para así poder perseguir con criterio el racismo y otra serie de contenidos ilícitos de Internet.

Así, a finales de 2001 el Parlamento de Alemania aprobó las medidas propuestas por el Ministro del Interior, Otto Schily, entre las que se encontraban el garantizar a las fuerzas de seguridad el pleno acceso a los datos de las telecomunicaciones almacenadas en soporte digital (contenidos de las comunicaciones, informaciones relativas a los intercambios de correos electrónicos, etc.).

En Dinamarca, y dentro de la denominada "Batería de Medidas Antiterroristas", de octubre de 2001, el gobierno estableció una serie de disposiciones para legalizar la retención de datos relativos a las telecomunicaciones, navegación, correos electrónicos, así como

---

Europea, en vigor desde el pasado 13 de octubre de 2002, y que desde su nacimiento ha provocado multitud de reacciones tanto a favor como en contra

[19] *Carnivore* es un programa cuya existencia se conoció públicamente en julio de 2000. Desde entonces ha sido utilizado por el FBI para monitorizar el tráfico de Internet y el correo electrónico a través de los proveedores de acceso. La utilización de este programa tras los atentados del 11-S necesitaba de una autorización judicial, pero, tras la aprobación de la *Combating Terrorism Act*, el 13 de septiembre, los servicios de seguridad ya no necesitaban de dicho permiso y se inicio una auténtica cruzada para combatir el cifrado de mensajes.

[20] Acorde con esta línea de actuación, la Oficina de Influencia Estratégica, perteneciente al Departamento de Defensa, propuso difundir falsas informaciones en los medios de comunicación extranjeros, utilizando especialmente sitios de Internet creados con ese objetivo y correos electrónicos dirigidos a las redacciones, aunque afortunadamente esta campaña de "Propaganda Negra" fue rápidamente desmontada tras la manifiesta oposición nacional e internacional a dicha estrategia.

facilitar a la policía acceder más fácilmente a los datos personales. Además, la ley antiterrorista permite a los servicios secretos consultar las informaciones sin permiso judicial.

En Francia, la *Ley de Seguridad Cotidiana* (LSQ), aprobada de urgencia el 15 de noviembre de 2001, obliga a los ISP a conservar durante un año datos relativos a las conexiones a la Red y el correo electrónico[21], mientras que la *Ley de Orientación y Programación de la Seguridad Interior* (LOPSI), aprobada el 31 de julio de 2002, prevé que la policía judicial pueda efectuar rastreos en los servidores de los ISP donde se almacena información sobre la navegación y los correos electrónicos..

Por su parte, en el Reino Unido se aprobaba a mediados de diciembre de 2001 la *Anti-Terrorism, Crime and Security Act*, que también fija en al menos un año la conservación de los datos de conexión por parte de los ISP, datos a los que la policía puede acceder, en muchos casos, sin autorización previa del juez. Además, el Ministro del Interior presentó en Junio de 2002 un proyecto de revisión de la controvertida *Regulation Investigatory Powers Act* (RIPA), según la cual las administraciones locales podrían acceder a la información relativa a la navegación y el envío y recepción de correos electrónicos.

En Italia, el gobierno de Silvio Berlusconi aprobó a mediados de diciembre de 2001 una ley para facilitar la escucha de sospechosos, que además autoriza interceptar datos de comunicaciones, conexiones a Internet y correos electrónicos, misión que ahora cae en manos de un bueno número de funcionarios de los servicios de policía de la capa baja de la jerarquía[22].

Por último, en España la *Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (LSSI), aprobada el 27 de junio de 2002 y en vigor desde el 13 de octubre, obliga a los ISP a retener y conservar los datos de conexiones y tráfico al menos durante un año, aunque, gracias a las enmiendas introducidas, la policía no tendrá acceso a los datos sin permiso judicial. Sin embargo, aún queda por saber qué autoridad –administrativa o judicial- tendrá potestad para clausurar los sitios web que atenten contra una serie de valores, lo cual ha sido sin duda el punto que mayor controversia ha generado, ya que, y en contra de lo que reza el artículo 20 de la Constitución Española sobre la Libertad de Expresión, con esta Ley podrían ser las autoridades administrativas y no las judiciales las que ordenaran el cese de un sitio web.

5. Conclusión

Debido al carácter descentralizado e inabarcable de la Red, la misma Internet censurada ha servido como plataforma de lucha y protesta contra los controles y prohibiciones impuestos. La misma volatilidad de la Red permite que los sistemas de control sean difícilmente asumibles por los estados. Su uso como vía de información alternativa junto al desarrollo de programas que burlan los filtros establecidos preservando el anonimato o el trabajo de los diferentes grupos defensores de los ciberderechos, son algunos ejemplos de esa lucha contra la censura en Internet. Sin embargo, son bien pocos los organismos oficiales que promueven acciones en este contexto.

En ese sentido, podemos afirmar que Internet no es tan libertaria e incontrolable como podemos llegar a pensar. Internet se puede controlar mediante innumerables medidas tal y

[21] Dicha Ley también autoriza a los jueces a recurrir a los "medios del Estado sometidos al secreto de la Defensa Nacional" para descifrar los mensajes, obligando a proveedores de medios de criptografía a entregar a las autoridades sus protocolos de cifrado para que puedan descifrar los mensajes.

[22] Otra ley promulgada a finales del 2001 protege a los agentes de los servicios secretos civiles (SISDE) y militares (SISMI) que cometan delitos –exceptuando matar o herir personas- en el curso de sus misiones, autorizando así el robo, las requisas "secretas" y las escuchas telefónicas y electrónicas.

como hemos visto a lo largo de este artículo. Sin embargo, ya no sólo por las características de la propia Red, sino por las de un mundo cada vez más globalizado, cada vez es más complicado frenar el intercambio de ideas y siempre es posible encontrar una vía para denunciar las injusticias ante los países democráticos y las organizaciones que, como RSF, desarrollan una labor de un valor incalculable para asegurar un derecho inalienable para todo ser humano.

Quedémonos para finalizar con la histórica Declaración de Independencia del Ciberespacio, redactada en 1996 por John Perry Barlow, fundador de EFF, auténtico himno a la libertad en Internet:

"Gobiernos del Mundo Industrial, vosotros, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, os pido en el pasado que nos dejéis en paz. No sois bienvenidos entre nosotros. No ejercéis ninguna soberanía sobre el lugar donde nos reunimos. No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a vosotros sin mas autoridad que aquella con la que la libertad siempre habla. (…) Estamos creando un mundo en el que todos pueden entrar, sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento. Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coaccionado al silencio o el conformismo. (…) Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y hermosa que el mundo que vuestros gobiernos han creado antes".