

Pornografía, pedofilia y control de contenidos en Internet

Dr. Oscar Jaramillo Castro

Centro de Estudios Mediales (CEM), Facultad de Ciencias de la Comunicación e Información de la Universidad Diego Portales.

Mayo 2003.

"Acceso a pornografía por Internet en colegios pone en tela de juicio Red Enlaces"¹. Titulares de prensa como el que acabamos de citar y que apareció durante el mes de marzo de 2003 en el diario La Tercera, constituyen la punta de iceberg de un problema mucho mayor. Desde que a mediados del año pasado el programa Contacto de Canal 13 denunció la existencia de una red de pedofilia que operaba en Chile y que distribuía el material a través de Internet, éste es un tema que ha acaparado la atención no sólo de la prensa, sino que también de las autoridades del gobierno, del Ministerio de Educación, parlamentarios, la policía, la Iglesia y del público en general.

Esta creciente preocupación tiene su origen en factores internos y externos a la red. En primer lugar está la gran cantidad de material pornográfico que existe en la red. Una simple consulta a través de los motores de búsqueda más populares de la web, como Google² o Yahoo³, dejan en evidencia que este tipo de sitios se cuentan por miles y cientos de miles. En segundo lugar está facilidad con la que los niños pueden acceder a este tipo de contenidos. A diferencia con lo que sucedía con los medios tradicionales, no existen restricciones de horario como sucede en la televisión, ni se puede limitar la venta sólo a los mayores de edad, como ocurre con las revistas o libros de esas características. En la web sólo basta con hacer un click o con teclear la dirección electrónica deseada.

Por otra parte, hay que considerar una serie de problemas con los que se han topado quienes han querido solucionar este problema. La existencia de vacíos legales y la dificultad para determinar responsabilidades en Internet, ha dificultado la acción de la justicia y de los organismos policiales. A eso hay que sumar el hecho de que Internet es una red de carácter internacional, que no guarda ninguna relación con las fronteras geográficas del "mundo real", por lo que los tribunales de justicia se ven enfrentados constantemente a dificultades para fijar la jurisdicción. Asimismo la red ofrece una serie de posibilidades que le permite a los responsables de producir material pornográfico o pedofílico de evadir cualquier intento de control o de limitar la difusión de ese tipo de contenidos.

Pero el principal motivo de preocupación, tal como lo señala la Directiva del Parlamento Europeo 97/36/CE de Televisión sin Fronteras, es que la exposición de los niños a material pornográfico y a las redes de pedofilia atenta contra su desarrollo físico, síquico y moral.

Los resultados obtenidos por las iniciativas legales desarrolladas por países como Estados Unidos y Australia, han sido cuestionadas por su efectividad y por dañar la libertad de expresión. Uno de los ejemplos más clásicos dentro de esta área fue la declaración de inconstitucionalidad del Acta de la Decencia en las Comunicaciones (CDA, en inglés) por la Corte Suprema de los Estados Unidos.

¹ Diario La Tercera. 09/03/2003. Badilla, Luisa. Acceso a pornografía por Internet en colegios pone en tela de juicio Red Enlaces. p.17.

² www.google.com

³ www.yahoo.com

En esa oportunidad, la Corte señaló que Internet requiere un nivel de protección de la libertad de expresión similar a la prensa y los libros, debido a su naturaleza no intrusiva⁴. No obstante, el fallo adverso de la Corte Suprema de los Estados Unidos, Australia creó una ley que incluso contempla penas de cárcel para todos los adultos que busquen o bajen desde Internet material pornográfico. Según Luis Escobar la Serna eso transgrede el derecho a la información, porque penaliza una conducta que fuera de la red es absolutamente legal⁵. Lo que ocurre en Australia es equivalente a encarcelar a todos los lectores o suscriptores de la revista Play Boy.

El problema está en cómo compatibilizar la libertad de expresión con la efectiva protección del desarrollo físico, síquico y moral de los niños, frente a la pornografía y la pedofilia. Más aún cuando la principal solución frente a este problema, como ha sido la utilización de programas o software de filtrado y etiquetado, ha demostrado bajos niveles de efectividad. De acuerdo a Edelman los programas de filtrado tienden a bloquear contenidos absolutamente inocuos y a dejar pasar una gran cantidad de material pornográfico de naturaleza cruda⁶.

Además en investigaciones previas, hemos concluido que las iniciativas de etiquetado de sitios llevadas a cabo por la World Wide Web Consortium (W3C) y la Asociación de Clasificación de Contenidos de Internet (ICRA, por sus siglas en inglés), presentan los mismos problemas que los programas de filtrado⁷.

Por lo tanto, tenemos un problema real que afecta el desarrollo de los menores de edad y que además tiene consecuencias sobre el derecho a la información de las personas. Porque en este momento, el desafío está en cómo proteger a los niños sin limitar el acceso a contenidos inocuos, porque en ese instante se cae en la censura. Como podemos observar, este es un problema complejo, porque no ha podido ser solucionado desde un ámbito legal, ni tecnológico. Pero lo principal es que sus consecuencias se viven día a día cada vez que un niño se conecta a Internet. Es por eso que vale la pena preguntarse cómo solucionar este problema de manera efectiva y real, sin caer en la censura. O al menos vislumbrar las posibles soluciones.

La preocupación por el “Ciberporno”

Al igual que lo que sucedió en Chile, la preocupación por la posibilidad de que los menores accedan a contenidos pornográficos a través de Internet, comenzó en 1995 en los Estados Unidos después de un artículo de la revista Time, sobre lo que en esa oportunidad se denominó como "cyberporno".

Dicho reportaje causó un impacto a tal punto que según la Human Rights Watch (HRW), se tradujo en la creación de la CDA o Acta de la Decencia en las Comunicaciones por parte del gobierno de

⁴ Sentencia de la Corte Suprema de los Estados Unidos, Reno contra ACLU, Nº 96-511, del 16 de junio de 1997.

⁵ Escobar de La Serna, Luis. Derecho de la Información. Editorial Dykinson. Madrid, España. 1998. p. 523.

⁶ Edelman, Ben. Sites Blocked by Internet filtering programs. Edelmexpert report, november 30, 2001, for Multnomah County Public Library et. Al., vs United States of America, et. Al. <http://cyberlaw.harvard.edu/people/edelman/mul-y-us/>

⁷ Jaramillo, Oscar. Derecho a la información en los portales y buscadores de la web. Tesis para obtener el grado de Doctor en Ciencias de la Información de la Universidad Complutense de Madrid. 2002.

Bill Clinton⁸. Esta fue la primera ley creada específicamente para tratar de regular la red. Básicamente dicha norma penalizaba la difusión a través de Internet de cualquier tipo de contenidos que pudiera ser considerado como "indecente". Además establecía que todos los sitios que desearan publicar contenidos de corte erótico o pomográfico, debían implementar un sistema de verificación de edad, a través del uso de los números de la tarjeta de crédito.

No obstante, en 1997 la Corte Suprema de los Estados Unidos declaró como inconstitucional la CDA, debido a que consideró que la norma atentaba contra la Primera Enmienda, al restringir la libertad expresión de todos los usuarios de Internet.

Tanto la creación de la CDA como su posterior declaración de inconstitucionalidad marcan un hito en el campo de la protección de menores en los espacios digitales, debido a que marcan la lógica del debate. Desde ese momento en adelante, se mantendrá una fuerte discusión entre distintos sectores para tratar de armonizar el respeto del derecho a la información y la protección de los menores.

Según Pilar Cousido el origen de esa disputa está en el hecho de que al referirse sobre los menores de edad, la legislación informativa adopta dos posiciones básicas: protectora o fomentadora⁹. La primera posición establece límites, sanciones y responsabilidades en contra de quienes difundan mensajes que dañen o atenten en contra de los niños. Mientras que la segunda postura tiene como objetivo la creación de premios, subvenciones o programas infantiles. El conflicto se genera entre quienes detentan la postura protectora y los grupos que defienden la libertad de expresión a nivel mundial.

Un claro ejemplo de ello es que la declaración de inconstitucionalidad de la CDA se origina en una serie de acciones legales interpuestas por la ONG norteamericana American Civil Liberties Union (ACLU). La ACLU junto a otras ONG's dedicadas a la defensa de las libertades civiles como la HRW, Global Internet Liberty Campaign (GILC), Amnistía Internacional y Electronic Frontiers, han manifestado su abierto rechazo a la implementación de cualquier tipo de leyes que intenten controlar los contenidos por Internet, incluyendo las que intentan proteger a los menores de los contenidos pornográficos.

El principal problema es que tanto la postura protectora como la fomentadora no han podido solucionar el problema. Pese a la dureza de algunas leyes como la Broadcasting Service Amendment (Online Services) Act de 1999 de Australia, no se ha logrado disminuir la exposición de los niños a los contenidos pornográficos y a las redes de pedofilia. Esta ley autoriza a la Autoridad de Difusión Australiana para retirar material pornográfico desde servidor web. Incluso una reforma efectuada en el año 2002 penaliza la lectura y búsqueda de material pornográfico por parte de los mayores de edad.

En tanto las iniciativas de autorregulación que han sido desarrolladas por la World Wide Web Consortium (W3C) y la Internet Content Rating Association (ICRA), tampoco han podido lograr un impacto significativo, pese a que ambas organizaciones se han creado a partir de un amplio

⁸ Human Rights Watch (HRW) Report. Silencing the Net: The threat to freedom of expression online. 1996. p. 8.

⁹ Cousido, Pilar; Bel, Ignacio; Corredoira, Loreto. Derecho a la Información (I): Sujetos y medios. Madrid, España. Ed. Colex. 1992. p. 123.

consenso entre organizaciones de padres, educadores, académicos, junto a los productores de contenido y de servicios en línea, como Microsoft, Yahoo y America Online - Time Warner.

Mientras que la Unión Europea¹⁰ junto con el Consejo Pontificio para las Comunicaciones Sociales de El Vaticano¹¹ han mantenido una postura intermedia, que toma aspectos de las posturas protectora y fomentadora. Ambos organismos han discutido el tema y elaborado líneas de acción, que ponen énfasis en la educación y en la posibilidad de utilizar algunos softwares de filtrado.

En Chile el tema no ha tenido el mismo desarrollo que en países como Estados Unidos o Gran Bretaña, pese al impacto que ha tenido en la opinión pública. Hasta este momento la atención ha estado más que nada en el ámbito policial, a través de la acción de la Brigada de Cibercriminales de la Policía de Investigaciones, que se ha dedicado a desarticular las redes de pedofilia.

Desde un ámbito legislativo sólo se han elaborado dos proyectos de ley que tangencialmente abordan el problema creado por la pornografía desde una perspectiva protectora. Se trata de los proyectos 3004-19 que Establece la responsabilidad por los contenidos de Internet y 2395-19 que Establece un sistema de regulación de Internet. En el primero de los proyectos se afirma que los ISP (Internet Service Provider)¹² sólo podrán operar en Chile si establecen un sistema de filtrado de contenidos, mientras que en el segundo, se disponen penas para quienes difundan contenidos de carácter ilegal a través de Internet. Sin embargo, ambos proyectos son de carácter general y en ningún momento se aclara cómo deberán funcionar los sistemas de filtros o cuáles son las acciones concretas que se deberán seguir. En el caso concreto del proyecto de responsabilidad en Internet, el articulado se limita a fijar penas, sin hacer referencia a los problemas creados por la “extraterritorialidad” de la web y por las dificultades que existen para fijar las responsabilidades, sobre todo cuando los contenidos son publicados de manera anónima.

Lo que sucede es que el tema de la pornografía en Internet es nuevo en nuestro país, razón por la cual no se ha producido un gran debate. Asimismo hay una falta de comprensión y de conocimiento, que se ve reflejada en los proyectos de ley que se están discutiendo en el Congreso Nacional.

No obstante, siguen la misma lógica que los proyectos que se han elaborado en Estados Unidos y Australia, al penalizar la producción de contenidos pornográficos y al establecer mecanismos de carácter tecnológico para controlar los contenidos.

Pero cuál es la razón que justifica que hablemos de una falta de comprensión del problema, cuando se copian las soluciones que se han ensayado en Estados Unidos y Australia. Para comprender dicha afirmación, debemos analizar más en detalle dichas soluciones para ver cuáles son sus principales problemas.

¹⁰ Com (96) 487 Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos en Internet. 1998. <http://europa.eu.int/ISPO/legal/es/es1396.htm>

¹¹ Foley, John; Pastore, Pierfranco. Ética en internet. Pontificio Consejo para las Comunicaciones Sociales. 2002. http://www.vatican.va/roman_curia/pontifical_councils/pcacs/documents/rc_pc_pcacs_doc_20020228_ethics-internet_sp.html

¹² Proveedores de acceso a Internet, como Terra, Entel o America Online.

La búsqueda de soluciones

Dentro de la búsqueda de soluciones se han seguido tres caminos básicos: la creación de leyes que penalicen la producción y tenencia de material pornográfico, impedir que los niños accedan a este tipo de material a través del uso de programas de filtro o del etiquetado de sitios y el impulso de iniciativas de corte educativo.

Sin embargo, antes de poder analizar más en detalle estas tres vías que se han ensayado hasta este momento es necesario referirnos brevemente al derecho a la información, para poder situar el problema dentro del marco de los derechos humanos.

Si bien es cierto que el desarrollo del concepto de derecho a la información tiene su fuente principal en el trabajo desarrollado por Francisco de Vitoria hacia el año 1539¹³, es a partir de la Declaración Universal de los Derechos Humanos de 1948, donde adquiere su actual significado. A partir del trabajo de Vitoria y de dicha declaración, Desantes define el derecho a la información como los derechos o facultades para difundir, recibir e investigar mensajes a través de los medios de comunicación¹⁴.

Vitoria establece que la comunicación forma parte de los derechos naturales que tienen todos los hombres. Según él, el simple acto de hablar es natural en todos los hombres y tiene como finalidad comunicar sentimientos, información o pensamientos a otras personas. El objetivo de este proceso de comunicación sería la creación o mantención de vínculos sociales. Es por eso que para Vitoria no es posible que exista una comunidad sin comunicación, razón por la cual los considera como sinónimos¹⁵.

Desde esa perspectiva, el derecho a la información adquiere una vital importancia para la mantención de la vida en comunidad y, en especial, para el desarrollo y fortalecimiento del sistema democrático. El actual Secretario General de la ONU, Kofi Annan, manifestó que las sociedades dependen de los medios de comunicación para que estos difundan las ideas de los distintos partidos políticos y de esa manera, los ciudadanos puedan votar con conocimiento de causa¹⁶. Los medios de comunicación y la comunicación en general, jugarían un rol clave dentro de uno de los axiomas de la democracia: el voto informado. Esa es una de las razones por las cuales los dictadores acostumbran intervenir la prensa y establecer sistemas de censura después de tomar el control del gobierno. Los ejemplos abundan y sólo basta con ver países como Cuba o China.

¹³ Desantes - Guanter, José María. Francisco de Vitoria, precursor del derecho a la información. Fundación de la Comunicación Social. Madrid, España. 2002. P. 41.

¹⁴ Desantes - Guanter, José María. Información y Derecho. 1ª Ed. Santiago, Chile. P. Universidad Católica de Chile. 1990. p. 31.

¹⁵ Desantes - Guanter, José María. Francisco de Vitoria, precursor del derecho a la información.

¹⁶ Annan, Kofi. Discurso del Secretario General de la ONU en la Conferencia Internacional de las Democracias Nuevas o Restauradas. Cotonú, Benin, 4 de diciembre de 2000. www.un.org/spanish/docs/democraciasnuevas.htm

El problema comienza cuando surgen conflictos entre la información y otros derechos humanos. En el caso que estamos estudiando, el conflicto se genera entre el derecho a la información y la preocupación por proteger a los menores frente a la pornografía y la pedofilia en Internet.

A partir de la doctrina desarrollada por Desantes, lo que corresponde es recurrir a lo que él denominó como la coordinación de los derechos humanos, para ver qué derecho se debe contraer para dar paso al otro¹⁷. Según este autor la coordinación se debe hacer en función de los principios de personalidad y comunidad.

Lo que plantea el primer principio es que el derecho que esté más cerca del núcleo de la personalidad, debe contraerse para dar paso al que esté más lejos. Desantes plantea que los derechos que están más cerca del núcleo que la personalidad que el derecho a la información, son los derechos a la vida, el honor y la intimidad¹⁸.

Y a partir de lo planteado por Vitoria, Desantes explica el significado del principio de comunidad. La finalidad última de la comunicación sería la creación y mantención de la comunidad, por lo que la información deberá contraerse frente al derecho a la paz, que tienen todas las personas¹⁹.

De acuerdo a su doctrina sólo en aquellos casos en los que en que se afecte a uno de esos casos, el derecho a la información deberá contraerse. En otras palabras, el incitar a la guerra o la violencia, queda fuera de la protección del derecho a la información debido a que va en contra del derecho a la vida.

No obstante, hay que aclarar que el hecho de que Desantes hable de "contracción" y no de límites no es casual. Tal como lo explica la Convención Americana Derechos Humanos de 1969, la aplicación de responsabilidades en materia informativa deber realizarse con posterioridad a la difusión de los contenidos. De lo contrario, se estaría frente a una medida de censura "previa".

Otro aspecto que hay que considerar es la diferencia que hace la Unión Europea entre los contenidos que define como "nocivos" e "ilegales". Por ilegales define como aquellos contenidos que pueden ser considerados como delictivos, por parte de la legislación de los Estados miembros²⁰. Pese a lo vaga que puede parecer dicha definición, adquiere un sentido mayor si se lo relaciona con la coordinación de los derechos humanos. Desde una perspectiva desantiana un contenido ilegal no sólo sería aquel que va en contra de una norma o ley, sino que transgrede los derechos a la vida, el honor, la intimidad y el derecho a la paz.

Mientras que un contenido "nocivo" es aquel que puede constituir una ofensa a los valores o sentimientos de otras personas²¹. Es decir, son contenidos que no van en contra de ninguna norma o ley, pero que debido a su naturaleza potencialmente ofensiva, necesitan de una mayor cuota de criterio para ser entendido y puestas dentro de un contexto.

El objetivo de hacer una diferencia entre los contenidos nocivos e ilegales, se relaciona directamente con la necesidad de respetar la coordinación de los derechos humanos en función de

¹⁷ Desantes - Guanter, José María. Información y derecho. Op. cit.

¹⁸ Idem

¹⁹ Idem

²⁰ Com(96) 487. Op. cit. p. 8.

²¹ Idem

la naturaleza propia de la pornografía y la pedofilia. La pornografía puede considerarse como no apta u ofensiva para los menores de edad. Lo que se plantea es que se requiere tener un criterio formado, por lo que podría ser dañino para los menores de edad.

Tal como lo señala la Directiva de Televisión sin Fronteras de la Unión Europea, la pornografía no es un contenido que quebrante la ley. Pese a ello, lo adecuado es que sólo llegue a manos de personas mayores con un criterio formado, ya que de lo contrario puede afectar el desarrollo físico, síquico y moral de los niños. Es por eso, agrega, que deben tomarse medidas para impedir el acceso a los menores de edad, sin que eso signifique una medida de censura para el resto de las personas.

En cambio, la pornografía infantil o pedofilia no sólo es una conducta penada por la ley, sino que además atenta de manera directa en contra de los derechos a la vida y el honor de los menores de edad, debido a que los mecanismos para obtener ese tipo de material implican abiertamente un abuso físico, psicológico y moral de los menores de edad. Cabe recordar que gran parte de las fotos y videos que comercializan ese tipo de sitios son obtenidos a través de la filmación de violaciones o de lo que la ley chilena denomina como abusos deshonestos.

El objetivo de hacer esta diferenciación entre contenidos nocivos e ilegales, junto con abordar la coordinación de los derechos humanos, es que tanto la pornografía como la pedofilia necesitan de soluciones distintas debido a su naturaleza.

Sin embargo, al ver las leyes como la australiana (a la cual ya hicimos alusión) y la CIPA (Children's Internet Protection Act) de los Estados Unidos, veremos que esa diferencia no es realizada con claridad. Una situación similar ocurre con los principales mecanismos de control de contenidos de carácter tecnológico, como lo son los sistemas filtrado y etiquetado de sitios.

Además debemos analizar con más detalle los programas de filtrado y etiquetado, debido a que tanto los proyectos de ley chilenos, como la CIPA de los Estados Unidos establecen la obligatoriedad de los programas de filtrado para proteger a los menores de edad. No obstante, dicha solución deja abierta una serie de interrogantes que se centran sobre todo en su efectividad y en el respeto a la coordinación de los derechos humanos.

El filtrado y etiquetado

Antes de poder comenzar un análisis más detallado es necesario especificar en qué consiste el filtrado y etiquetado. Pese a que normalmente se confunde o se habla de ambas técnicas como si fueran una sola, es necesario hacer la diferencia por razones metodológicas. Hacemos esta aclaración, porque en estricto término, en la mayoría de los casos se utiliza una mezcla de ambos y su funcionamiento es parecido. Pero lo que hay que tener en cuenta, es que en la práctica se traducen en iniciativas distintas. Además se requiere de un análisis más detallado, debido a que son la principal solución por la que se aboga en Chile, a partir del ejemplo norteamericano.

En términos generales, el filtrado es realizado a través de un programa computacional que bloquea o niega el acceso a distintas páginas web, a partir de una categorización predefinida por el autor del software.

De acuerdo a la información entregada por los fabricantes de los principales programas de filtrado como Surfcontrol de Cyber Patrol²², N2H2 Internet Filtering²³, Secure Computing SmartFilter²⁴ y Websense²⁵, este tipo de software funciona a través de dos mecanismos básicos. El primero de ellos consiste en la elaboración de una base de datos o lista negra, con los sitios "prohibidos". Esta base de datos es realizada "a mano" por un grupo de personas contratadas por la empresa, quienes están revisando constantemente la web.

Además la mayoría de los softwares de filtrado complementan sus listas negras con una búsqueda por palabras claves. Como el número de sitios que puede visitar un grupo de personas es reducido, se han implementado unos *robots* o *web crawler*, similares a los que utilizan los motores de búsqueda. Un *robot*, *spider* (araña) o *web crawler* es un programa computacional que recorre la web de manera autónoma, sin la intervención de ninguna persona. El robot lo que hace es entrar a una página web y clasificarla en función de una detección de palabras claves. Es decir, ve qué palabras tiene en el título y cuáles son las que se repiten más dentro del texto. Una vez que termina de clasificar la página, envía una copia a su servidor y entra a todos los links tenga esa página, en donde vuelve a repetir el mismo proceso.

Como podemos observar la función principal del robot es realizar una lista negra, pero sin la intervención humana. La principal ventaja frente a la confección de listas negras por parte de personas, es que el robot puede hacer una lista mucho más extensa que lo podría hacer un verdadero ejército de personas, contratadas para tal efecto.

En cambio, tal como lo manifiesta la ACLU, los sistemas de etiquetado pretenden crear un método uniforme de clasificación de contenidos²⁶. El etiquetado consiste en que cada página que existe en la web, debe ser catalogada o autodefinida. Lo que se quiere es que cada página tenga una especie de etiqueta que diga "sexo", "deportes" o "niños", que sea elaborada por el mismo autor del sitio. De esa manera, al entrar en una página el navegador que ocupa el usuario, verá la etiqueta y dará o negará acceso al sitio, a partir de las preferencias que el mismo usuario predefinió en el browser, sea este Internet Explorer o Netscape Navigator.

La diferencia con el filtrado es que no existe una búsqueda por palabras claves, ni una lista negra. Lo que sucede es que cada sitio se autoclasifica, poniéndose una "etiqueta" que lo identifica claramente. La gracia está en que esta "etiqueta" queda puesta de tal manera que es visible para los navegadores o browsers. Además las instituciones que han fomentado el desarrollo del etiquetado, el World Wide Web Consortium (W3C) y la Internet Content Rating Association (ICRA), esperan que esto se transforme en una norma estándar, válida para todos los contenidos y páginas existentes en la web.

El etiquetado no es realizado a través de un software especial, como sucede con el filtrado. Es realizado por el mismo programa navegador o browser que ocupa el usuario para visualizar las páginas web, por lo que está disponible para cualquier usuario sin necesidad de contar con un equipamiento adicional.

²² www.cyberpatrol.com

²³ www.n2h2.com

²⁴ www.securecomputing.com

²⁵ www.websense.com

²⁶ Beeson, Ann; Hansen, Chris. Fahrenheit 451 20: Is cyberspace burning? American Civil Liberties Union (ACLU). 1997.p.3.

Y a diferencia de los softwares de filtrado, que cada uno de ellos tiene su propia categorización de contenidos, el etiquetado se basa en la creación de una norma estándar. Tanto la iniciativa desarrollada por la ICRA como por el W3C, se basan en la norma PICS (Platform for Internet Content Selection²⁷), que fue desarrollado por éste último organismo. Sin embargo, a partir del año 2000 PICS dio paso a una nueva norma conocida como RSACi (Recreational Software Advisory Council), que fue desarrollada por la ICRA. Cabe señalar que entre las dos normas no existen grandes diferencias y que en el fondo, la RSACi no es más que un desarrollo o evolución de PICS.

El W3C explica que PICS fue diseñado originalmente para ayudar a los padres y maestros a controlar a qué tipo de contenidos acceden los niños en la Internet, a través de la utilización de etiquetas²⁸. Las etiquetas son definiciones sobre el contenido de la página que se incluyen dentro del código HTML, de manera tal que éste pueda ser reconocido por el browser.

Las etiquetas tienen dos niveles de información. El primero de ellos se refiere a las valoraciones del sitio, según cuatro categorías básicas: desnudez, lenguaje, sexo y violencia. El objetivo de este nivel (valoraciones) es determinar si el sitio contiene material que puede ser colocado dentro de alguna de esas categorías. Mientras que el segundo nivel, llamado indicadores, se refiere al grado o "crudeza" con el que son presentadas cada una de las categorías anteriores. A partir de ellas se determina quién puede ver ese contenido en función de las categorías del primer nivel²⁹. Si se compara con la calificación cinematográfica, este segundo nivel dirá si ese contenido sobre sexo es apto para todo espectador, mayores de 14 años o mayores de 18 años.

²⁷ Plataforma de Selección de Contenidos de Internet.

²⁸ W3C. Platform for Internet Content Selection (PICS). World Wide Web Consortium 1997. www.w3.org/PICS

²⁹ Dempsey, James; Weitzner, Daniel. . Sin limitación de fronteras: La protección del derecho a la libertad de expresión en una Internet global. Global Internet Liberty Campaign (GILC). 1998. <http://www.arnal.es/fee/info/regard-index.html> p. 13.

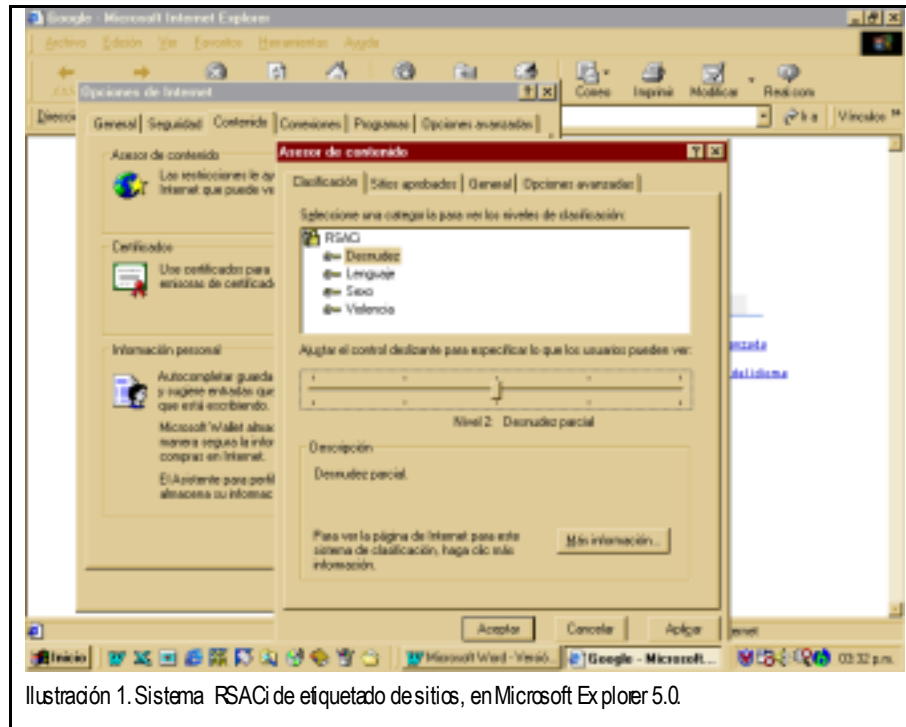


Ilustración 1. Sistema RSACi de etiquetado de sitios, en Microsoft Explorer 5.0.

Por ejemplo, si analizamos la página de la revista Play Boy, el primer nivel dirá sexo. Pero el segundo, especificará si éste se refiere a "besos apasionados", "roce sexual con ropa puesta", "roce sexual no explícito" y "actividad sexual explícita". Entonces, sólo será mostrada una página cuando la etiqueta que contiene el sitio coincide, con los parámetros predefinidos por el usuario dentro de las preferencias de su browser.

Como podemos observar, existen grandes diferencias entre el filtrado y etiquetado, lo que se traduce en distintas consecuencias sobre el derecho a la información. En primer lugar, el filtrado se centra en la facultad de recibir información, mientras que el etiquetado, en la de difundir. A partir de allí se crean grandes diferencias, debido a que en función de la facultad afectada - junto a otras variables como el grado de obligatoriedad, el nivel de aplicación y la definición de los contenidos prohibidos - se puede marcar la diferencia entre una medida de censura y la coordinación racional de los derechos humanos.

Claramente, el etiquetado de sitios se inscribe dentro de un ámbito autorregulatorio, que funciona bajo una lógica similar al sistema de calificación cinematográfica, al señalar cuáles son los contenidos que debieran quedar fuera del alcance de los niños para proteger su desarrollo en los términos de la Directiva de Televisión sin Fronteras. No obstante, la naturaleza autorregulatoria del filtrado limita su campo de acción a los contenidos nocivos.

En cambio, los softwares de filtrado tiene la capacidad para actuar sobre los contenidos nocivos e ilegales, debido a su carácter externo. Desde esa perspectiva, son útiles para limitar el acceso a los niños tanto a la pornografía, como a la exposición a las redes de pedofilia. Cabe señalar que al igual que la norma PICS, los programas de filtrado se limitan a impedir el acceso a los contenidos cuestionados. En ningún momento actúan o pueden ser utilizados para buscar responsabilidades por

parte de los productores de contenidos, por lo que no pueden ser usados para actuar en contra de una red de pedofilia, una vez que ha sido detectada.

Otro de los puntos que han sido cuestionados y que dio pie a la demanda de la ACLU en contra de CIPA en los Estados Unidos, es el nivel en el que deben ser aplicados los programas de filtrado. Según la organización hay una gran diferencia cuando el filtrado es realizado de manera obligatoria por el gobierno o si su aplicación queda sujeta a la decisión de los padres de los menores de edad³⁰. En el primer caso se trataría de una medida de censura, mientras que en el segundo, no. La razón principal está en el hecho de que limitaría el acceso a los contenidos nocivos, sin afectar o impedir que otro tipo de usuarios (adultos) acceda a ellos.

Pero una de las principales críticas que realiza la ACLU se centra en la efectividad de los sistemas de filtrado y en el hecho de que en muchos casos "censuran" una serie de contenidos inofensivos, como diarios, revistas e incluso sitios de organizaciones que defienden los derechos de los niños o que prestan ayuda a las víctimas de delitos sexuales.

Cabe recordar, que el uso obligatorio de los programas de filtrado es ampliamente utilizado por países como Arabia Saudita o China, como una forma de censurar contenidos que desde un punto de vista políticos no son aceptables para dichos gobiernos.

La efectividad del filtrado y el etiquetado

Pese al temor que causa entre los defensores de los derechos civiles, por la posibilidad que se utilicen con fines políticos, uno de los aspectos más cuestionados es la efectividad real del etiquetado y, más específicamente, del filtrado. Lo que se critica es que estos sistemas tienen grandes huecos o vacíos que dejan pasar una gran cantidad de material que de verdad es nocivo o ilegal, fenómeno que es conocido como no bloqueado. Pero lo que más ha generado preocupación, es que finalmente terminan censurando una gran cantidad de sitios que son absolutamente inofensivos, como páginas de noticias o de temas de salud. Esto es lo que ha sido llamado como sobrebloqueado. Tanto el no bloqueado como el sobrebloqueado han llegado a tal punto, que han tenido la fuerza suficiente como para cuestionar todo el sistema.

Un ejemplo de ello es la lista de los diez mayores errores cometidos por los programas de filtrado, que elaboró Tracy Zawaski³¹. Entre los sitios filtrados y que son absolutamente inofensivos se encuentran: la web del Instituto Smithsonian³², el Zoológico de San Diego³³, la Cruz Roja de los Estados Unidos³⁴, la Revista Online de Exploración Submarina (Explore Underwater Magazine Online)³⁵ y la página del Superbowl del fútbol norteamericano³⁶. Un caso aparte es el bloqueo que

³⁰ American Civil Liberties Union (ACLU). Report. Censorship in a box: Why blocking software is wrong for public libraries. 1998. p. 8.

³¹ Zawaski, Tracy. Rating, filtering, and blocking systems. Law School, Wayne University. 2000. www.law.wayne.edu/litman/classes/cyber/zawaski.html

³² www.si.edu

³³ www.sandiegozoo.com

³⁴ www.redcross.org

³⁵ www.exploreuw.com

sufrió el sitio de noticias de la CNN³⁷ por parte del software Sentinel, debido a que dentro del título de un artículo estaba la palabra "erótica".

Entre los sitios no bloqueados, se encuentran las páginas web: "Do you need a cheap gun?" (¿Necesita usted un arma barata?)³⁸, "Animal Juice - Extreme Animal Sex"³⁹ y "How to make Ecstasy" (¿Cómo llegar al éxtasis?)⁴⁰.

Durante el juicio en contra del filtrado obligatorio en las bibliotecas públicas de los Estados Unidos, Ben Edelman afirmó que los problemas producidos por este tipo de software tienen su origen en cuatro razones básicas⁴¹. La primera de ellas es la incapacidad de los programas de filtrado para bloquear sólo imágenes. Lo que sucede es que los robots de búsqueda de estos programas funcionan sobre la base de la detección de palabras. Entonces, como las imágenes son sólo bytes, no pueden diferenciar entre una foto pornográfica y una de un auto.

En segundo lugar, son incapaces para bloquear todos los contenidos que se topan con ciertas definiciones. Esto se debe a que no tienen la capacidad para distinguir las distintas sutilezas del lenguaje, lo que da origen principalmente al sobrebloqueo. Según la ACLU esto se debe a que los robots de los programas de filtrado buscan ciertas palabras claves en el texto de la página, pero son incapaces para analizar el contexto en que éstas son utilizadas⁴². Generalmente buscan palabras como "sex" o expresiones como "xxx" (triple x). Es por eso que a veces bloquean páginas con palabras "sexto" o "sexton". Por otra parte, algunos operadores de sitios pornográficos han aprendido a evitar el bloqueo ocupando expresiones "sess" o "sezz" en vez de "sex", con lo que se aumentó el número de sitios no bloqueados.

Ben Edelman asegura que también hay problemas en la elaboración de las "listas negras", que son confeccionadas por el personal trabaja en las empresas que fabrican los programas de filtrado⁴³. Esto se debe a discrepancias de criterio, incluso entre los mismos empleados de una empresa, los que clasifican con distinta dureza o permisividad un mismo tipo de contenidos.

Un tercer problema radica en la incapacidad de los programas del filtrado para bloquear contenidos que están basados en protocolos distintos del html. A lo que nos referimos es a lo que es conocido como "streaming video". Generalmente son archivos de video o música que están en los formatos de RealNetworks, RealPlayer o Microsoft Media Player. También se aplica este mismo problema a los documentos que están en el formato PDF (Adobe Acrobat Reader).

Un cuarto problema detectado por Edelman es que estos sistemas son ineficientes para bloquear el acceso a un sitio específico durante un período de tiempo a un usuario dado. Si un padre descubre a uno de sus hijos navegando en un sitio pornográfico o de otra naturaleza y no quiere que el niño

³⁶ www.nfl.com/sb34/

³⁷ www.cnn.com

³⁸ www.guns-unlimited.com/default.cfm

³⁹ www.animaljuice.com

⁴⁰ <http://members.tripod.co.uk/~proogs/craig/bomb.htm>

⁴¹ Edelman, Ben. Sites Blocked by Internet filtering programs. Edelm expert report, november 30, 2001, for Multnomah County Public Library et. Al., vs United States of America, et. Al. <http://cyber.law.harvard.edu/people/edelman/ml-v-us/>

⁴² American Civil Liberties Union. Censorship in a box. Op. cit. p. 5.

⁴³ Edelman, Ben. Op. cit. p. 29.

vuelva a visitarlo, se enfrentará a grandes problemas si la web no figura dentro de la base de datos o lista negra o cabe dentro de los vacíos que enumeramos con anterioridad.

Y a los problemas detectados por Edelman hay que sumar que la gran cantidad de páginas que existen en la actualidad, que según el último conteo realizado por Google llega a la cifra de 3.083.324.652 páginas web. A eso hay que sumar el hecho de que esa cifra sólo representaría un 16% del total de páginas que existen en la web, de acuerdo al estudio de Steve Lawrence y Lee Giles⁴⁴. Desde esa perspectiva los dos métodos utilizados por los programas de filtrado demuestran sus limitaciones. Por un lado es casi improbable que la elaboración de las listas negras de manera manual tenga un gran impacto. Más aún, si los mismo robots, que también utilizan estos programas, no logran revisar más allá del 16% del material existente en la web.

El etiquetado también se ve enfrentado al problema del no bloqueado y sobrebloqueado, aunque por razones distintas. Pese a que el sistema de etiquetado de la ICRA se puede activar desde los dos programas navegadores más ocupados, como lo son el Microsoft Explorer y Netscape Navigator, son muy pocos los usuarios que saben de la existencia de él y de cómo ocuparlo.

Este desconocimiento se suma al que existe entre los productores de contenidos y operadores de sitios. La composición pluralista de la W3C y de la ICRA y el hecho de que incluya a los productores de contenidos, no ha sido suficiente como para convertir esta medida de autorregulación en una costumbre dentro de la web.

Eso ha llevado a la ICRA a tomar medidas que están al borde de la ética. Al preguntarse "¿por qué molestarse en etiquetar un sitio?" la respuesta que da esta organización es: "Los sitios comerciales, con poco o ningún material censurable querrán etiquetar su sitio para que no sea bloqueados por defecto"⁴⁵. Lo que plantea el equivalente a decir "etiquete su sitio o al activar el sistema de filtrado será censurado", ya que por defecto se entiende como toda configuración estándar con la que viene un programa computacional.

Con esa simple medida la ICRA va en contra del espíritu mismo de la autorregulación y lo único que hace es aumentar la cifra de sitios sobrebloqueados. Lo que al final se traduce en un cuestionamiento a todo el sistema en general, al producir el mismo fenómeno de censura previa que los sistemas de filtrado.

Asimismo dentro del marco de una investigación anterior, pudimos comprobar que al activar el sistema RSACi desde el *browser* Internet Explorer 5.0 ó 5.5 se producen grandes inconvenientes a la hora de navegar⁴⁶. El sobrebloqueo adquiere tal nivel de repetición que impide la navegación de manera normal, debido a que la tendencia es a bloquear por defecto a todos los sitios que no están etiquetados y como la mayoría no lo están, es casi imposible pasar de un sitio a otro.

Lo que se cuestiona de estos dos sistemas de control parental es que junto con ir en contra del derecho a la información al censurar contenidos inofensivos, no cumplen su cometido al dejar pasar una gran cantidad de sitios nocivos y abiertamente ilegales, como lo vimos en los casos que enumeramos con anterioridad.

⁴⁴ Lawrence, Steve; Giles, Lee. Searching the World Wide Web. Science, Volume 5360, 1998. p.98 -100.

⁴⁵ ICRA. Op. cit. p. 3.

⁴⁶ Jaramillo, Oscar. Op. Cit.

¿Deben implementarse o sirven para algo los sistemas de filtrado y etiquetado? Como una forma de evitar que los niños accedan a contenidos nocivos se justifican, pero los problemas que crean al sobrebloquear y dejar pasar una gran cantidad de material, hacen que sea poco aconsejable su implementación. Aunque en el caso del etiquetado se advierte una mejor alternativa, debido a que lo que necesitan es un mayor apoyo por parte de los mismos productores de contenidos, para convertirse en una alternativa real que respete al derecho a la información. El desafío está en la creación de políticas claras y representativas de la comunidad de Internet, junto con dejar de lado la tentación de hacer las cosas por defecto.

Conclusiones

Como podemos observar, la difusión de contenidos pornográficos y pedofílicos por Internet tiene numerosas aristas que deben ser consideradas a la hora de buscar soluciones. Una de las principales conclusiones es que tanto las posturas protectoras como las fomentadoras, no han sido capaces de encontrar soluciones efectivas.

En un segundo nivel surge la necesidad de coordinar en los términos de Desantes, la protección de los menores con el derecho a la información, debido al peligro que se corre al caer en la censura. Con respecto a este tema, la aplicación de mecanismos de control, tales como el filtrado y el etiquetado abren un nuevo debate sobre el real significado de la censura en Internet.

Al centrarse sólo en la posibilidad de que los usuarios puedan acceder a los contenidos, dejando de lado el establecimiento de responsabilidades para los autores de los contenidos, ¿estamos legitimando un sistema de censura? ¿Cuándo es censura y cuándo no lo es?

Lo interesante de ese tema, es que de su respuesta también depende la posibilidad de encontrar soluciones efectivas. En primer lugar exige que se haga una diferencia clara entre la pornografía y la pedofilia, a través de los conceptos de contenidos nocivos e ilegales.

Desde esa perspectiva, la aplicación de los sistemas de filtrado sólo sería lícito utilizarlos, cuando se siga la lógica establecida por la Directiva de Televisión sin Fronteras de la Unión Europea. Es decir, cuando la decisión sobre su aplicación quede en manos de los padres, como una forma de evitar el acceso por parte de los niños a contenidos nocivos. De otra manera se corre el peligro que estos programas sean aplicados con fines políticos, como sucede en China o Arabia Saudita.

No obstante, los softwares de filtrado no solucionan por sí solos el acceso a la pornografía por parte de los niños. Tanto el sobrebloqueado como el no bloqueado, convierten en peligrosa la alternativa seguida por los proyectos de ley chilenos que sólo descansan en la tecnología para resolver el problema. La falsa sensación de seguridad junto con la complacencia podrían llevar a olvidar la importancia que juega la educación en este problema, tal como lo señala el Pontificio Consejo para las Comunicaciones Sociales del Vaticano. Según este organismo la tecnología sólo debe ser considerada como un apoyo, porque el eje central que permitiría resolver el problema está en una formación ética y moral, que debe comenzar por el hogar. Cabe señalar que ésa es una función que incluso, no puede ser delegada a otros entes como la escuela, la Iglesia o la misma tecnología.

Cabe señalar que el único rol que debiera jugar la tecnología es el de monitoreo o vigilancia por parte de los padres. Si bien es cierto que los programas de filtrado no pueden evitar que un niño entre a un sitio pornográfico, a través del manejo de las *cookies*, *snifers* o programas de espionaje (*spyware*) se puede detectar el acceso a ese tipo de contenidos. Es decir, la tecnología permite saber cuándo, por cuánto tiempo y con qué frecuencia un niño visita un sitio pornográfico. De esa manera los padres podrán tomar las medidas que estimen convenientes y educarlo para que ello no vuelva a ocurrir.

Desde el punto de vista del derecho a la información, se produce una absoluta consecuencia con la necesidad de establecer responsabilidades posteriores al hecho, ya que de lo contrario se cae en la censura. Mientras que los sistemas de filtrado y etiquetado partiría de la base contraria, ya que aplicaría el castigo antes que se produjera el hecho (que el niño entrara a un sitio pornográfico). La lógica de la prevención exacerbada (que ha proliferado en materia internacional a través de los ataques “preventivos”) no sólo instaura la censura como algo aceptable y necesario, sino que también estigmatiza a los niños. Parte de la base de que son culpables o que visitarán sitios pornográficos.

Como podemos observar, a través de las fallas de los sistemas “preventivos” se crea una serie de problemas tanto o más importante que lo que se pretende solucionar y tampoco se logra el objetivo primario: mantener a los niños fuera del contacto con la pornografía.

El punto está en que si se aplica el enfoque contrario (de las responsabilidades ulteriores), se pueden tomar las medidas necesarias para que ello no vuelva a ocurrir, desde las perspectivas fomentadoras y protectoras.

Tal vez el problemas más difícil de solucionar, es que esta perspectiva requiere de una mayor preocupación por parte de los padres y en interesarse en lo que hagan sus hijos. Por simple que esto parezca, es el eslabón más débil del problema.

Cabe señalar que este mismo enfoque es el también permitiría actuar de una manera efectiva en contra de los contenidos ilegales, como la pedofilia. El filtrado y el etiquetado no sirven para controlar ese tipo de contenidos, ya que actúan únicamente sobre la facultad de recibir de los usuarios. No impiden que los autores sigan generando contenidos ilegales y que corrompan o violen niños para obtener fotos o videos, que con posterioridad son comercializados a través de Internet.

En este mismo caso, la tecnología también puede ser utilizada para monitorear, vigilar y rastrear a los productores de los contenidos ilegales. Si bien es cierto que es posible publicar contenidos de manera anónima, a través del uso de programas que reparten los bytes que componen un sitio web en 20 ó 15 servidores host (de alojamiento de páginas web) distintos o de servidores tipo “Islas Caimán”, siempre es posible rastrear los mensajes que envían por correo electrónico o los mecanismos de pago en línea. Nuevamente, la función de la tecnología sería la rastrear e identificar, para que los autores de los contenidos puedan ser responsabilizados por sus acciones. Como vemos, lo único que se buscaría es el establecimiento de responsabilidades ulteriores, tal como lo señala la Convención Americana de Derechos Humanos.

Por lo tanto, lo que se requiere para encontrar soluciones efectivas para que los niños no accedan a la pornografía a través de Internet y para erradicar la pedofilia, es que se termine con el enfoque

“preventivo”, no sólo porque no es efectivo para resolver el problema, sino que por el serio peligro que encierra para el desarrollo del derecho a la información en Internet, al legitimizar la censura. También supone una utilización más racional de la tecnología, al limitar su campo de acción sólo a la detección para que sean las personas, sean padres o jueces, quienes solucionen este problema.

Bibliografía:

Monografías y artículos de revistas científicas:

1. American Civil Liberties Union. Censorship in a box: Why blocking software is wrong for public libraries. American Civil Liberties Union Freedom Network. 1998. www.aclu.org/issues/cyber/box.html
2. Annan, Kofi. Discurso del Secretario General de la ONU en la Conferencia Internacional de las Democracias Nuevas o Restauradas. Cotonú, Benin, 4 de diciembre de 2000. www.un.org/spanish/docs/democraciasnuevas.htm
3. Beeson, Ann; Hansen Chris. Fahrenheit 451.2: Is cyberspace burning. American Civil Liberties Union. 1997. www.aclu.org/issues/cyber/burning.html
4. Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones. (1998) Contenidos ilícitos en Internet. <http://europa.eu.int/ISPO/legal/es/es1396.htm>
5. Cousido, Pilar; Bel, Ignacio; Corredoira, Loreto. Derecho de la información (I): Sujetos y medios. Madrid, España. Editorial Colex. 1992. p. 123.
6. Cozac, David. Internet censorship report: The challenges for free expression on-line. Canadian Committee to Protect Journalist (CCPJ). 1998. www.ccpj.ca/publications/internet/index.html
7. Dempsey, James; Weitzner, Daniel. Sin limitación de fronteras: La protección del derecho a la libertad de expresión en una Internet global. Global Internet Liberty Campaign (GILC). 1998. <http://www.arnal.es/free/info/regard-index.html>
8. Desantes Guanter, José María; Información y Derecho. 1ª Ed. Santiago, Chile. Pontificia Universidad Católica de Chile, 1990, p. 38.
9. Desantes, José María. La información como deber. Editorial Abaco. Colección de la Facultad de Ciencias de la Información de la Universidad Austral, Argentina. Primera ed. Buenos Aires, Argentina. 1993. P. 132.
10. Desantes - Guanter, José María. Francisco de Vitoria, precursor del derecho a la información. Fundación de la Comunicación Social. Madrid, España. 2002
11. Edelman, Ben. Sites Blocked by Internet filtering programs. Edelm expert report, november 30, 2001, for Multnomah County Public Library et. Al., vs United States of America, et. Al. <http://cyber.law.harvard.edu/people/edelman/mul-v-us/>
12. Fernández Esteban, María Luisa. Nuevas tecnologías, Internet y derechos fundamentales. Ed. Mac GrawHill. Madrid, España. 1998.
13. Foley, John; Pastore, Pierfranco. Ética en Internet. Pontificio Consejo para las Comunicaciones Sociales. 2002. http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_sp.html
14. Foley, John; Pastore, Pierfranco. Ética en las comunicaciones sociales. Pontificio Consejo para las Comunicaciones Sociales. Jornada Mundial de la Comunicaciones Sociales, Jubileo de los Periodistas. Ciudad del Vaticano. 2000.

- http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_2000053_0_ethics-communications_sp.html
15. Giordano, Philips. Invoking law as a basis for identity in Cyberspace. Stanford Technology Law Review. 1998. http://stlr.stanford.edu/STLR/Articles/98_STLR_1
 16. Human Right Watch (1996) Silencing the net: The Threat to freedom of expresion on-line. Electronic Privacy Information Center. 1996. http://www.epic.org/free_speech/intl/hrw_report_5_96.html
 17. Internet Watch Foundation. Rating and filtering Internet content: A United Kingdom perspective. Internet Watch Foundation. March 1998. www.internetwatch.org.uk/label/rating_r.htm
 18. Lessig, Lawrence. El Código: y otras leyes del ciberespacio. Trad. Alberola, Ernesto. Ed. Taurus. España. 2001.
 19. Libro Verde sobre la Convergencia de los sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus consecuencias para la reglamentación: En la perspectiva de la Sociedad de la Información. COM (97) Versión 3, del 3 de diciembre, de la Comisión Europea. p. 43.
 20. Morales, Fermín; Morales, Oscar (editores). Contenidos ilícitos y responsabilidades de los Prestadores de Servicios de Internet. Ed. Aranzadi. España. 2002.
 21. Resnick, Paul. Special Report: Filtering information on the Internet. Scientific American. Marzo 1997. www.sciam.com/0397issue/0397/resnick.html
 22. Sommer, Joseph. Against cyberlaw. Berkeley Technology Law Journal. Fall 2000 v 15 i3 p. 1145.
 23. Volokh, Eugene. Freedom of speech, cyberspace, Harassment Law, and Clinton Administration. Stanford Technology Law Review. 2000. http://stlr.stanford.edu/STLR/Working_Papers/00_Volokh_1
 24. W3C. Platform for Internet Content Selection (PICS). World Wide Web Consortium. 1997. www.w3.org/PICS
 25. Zawaski, Tracy. Rating, filtering, and blocking systems. Law School, Wayne University. 2000. www.law.wayne.edu/litman/classes/cyber/zawaski.html

Jurisprudencia y cuerpos legales

26. Ley de Protección Infantil de la Privacidad en Línea (Children's Online Privacy Protection Act) de los Estados Unidos del 3 de noviembre de 1999. 16 CFR Part 312. RIN 3084-AA84. Sección 312.2. N°6.
 27. Ley N° 19.733 de Chile Sobre Libertades de Opinión e Información y Ejercicio del Periodismo.
 28. Sentencia de la Corte Suprema de los Estados Unidos, Reno contra ACLU, N° 96-511, del 16 de junio de 1997. <http://www.aclu.org/court/renovacludec.html>
 29. Proyecto de 3003-19 del Congreso Nacional de Chile que Establece la privacidad de los datos recolectados a través de Internet.
 30. Proyecto de ley 3004-19 del Congreso Nacional de Chile que Establece la responsabilidad por los contenidos de Internet.
- Proyecto de ley del Congreso Nacional de Chile que establece un sistema de regulación de Internet.