### Comunicación 7

## EMBATES JURÍDICOS Y RUMORES ÉTICOS EN LA RED

LORETO CORREDIRA Y ALFONSO Universidad Complutense de Madrid

Embate. (De embatirse)

- 1. m. Golpe impetuoso de mar.
- 2. m. Acometida impetuosa. U. t. en sent. fig.
- 3. m. Mar. Viento fresco y suave que reina en el verano a la orilla del mar.
- 4. m. pl. Mar. Vientos periódicos del Mediterráneo después de la canícula.

Ya que estaremos en el Mediterráneo hablaremos de los embates que hoy sufre la Red. Son "vientos periódicos" –como el afán de control sobre la información–, a veces "golpes impetuosos de mar" –leyes anti-informativas o acciones delictivas insoportables-. También son "vientos frescos y suaves" que nos obligan a todos a pensar más y mejor sobre la Información.

Hay rumores, que no formulaciones expresas, sobre una ética en Internet. Trataremos al menos uno de los principales retos y riesgos jurídicos que plantea Internet: la protección de los menores frente a contenidos ilícitos y/o nocivos, y las verdades y mentiras de algunas maneras de defenderlo.

Aunque citaremos algunos casos extremos que incumplen la regla, la tendencia general en los países occidentales, en lo que se refiere a contenidos en Internet, es sin duda mostrar preocupación por determinadas conductas (como el crecimiento de la pedrastia o algunas otras formas de cibercriminalidad), ofreciendo como solución a los problemas la autorregulación y la co-regulación. Se fomenta así la responsabilidad social y ética de los proveedores de acceso y contenido de Internet, así como de los usuarios, educadores y políticos.

# Modelos de regulación, co-regulación y autorregulación en Internet: comparativa internacional

Tomando como "problema", o reto jurídico la protección de menores, veamos cómo se ha resuelto. Tal ejemplo, como ocurre en el Derecho, nos sirve de "caso" para ver qué está pasando en el Derecho de Internet.

Algunos países han adoptado medios de "censura", es decir de supervisión y supresión de contenidos, bien por medios administrativos —como era la *Communication Decency Act* de los EEUU, que fue declarada inconstitucional en 1997 precisamente por eso-, bien por medios judiciales. También hay que incluir aquí las disposiciones de países totalitarios como China, y otros como Corea o Sudáfrica.

En otro orden de cosas, aunque en el marco de este Congreso sobre el derecho a la información, hay que citar sin duda la polémica *Ley de Servicios de la Sociedad de la Información* española¹ de 2002, que prevé la apertura de expedientes administrativos por incumplimiento de determinadas cuestiones (como la no inscripción en el registro de proveedores), si bien reserva sólo a los jueces aquellas materias que por la Constitución o por ley se les había encomendado². Se trata de otro embate jurídico que sufre ahora mismo Internet: se aprueba una ley de máxima responsabilidad para lo que deberían ser principios de autorregulación o al menos de co-regulación.

Otro ejemplo de país que ha establecido disposiciones concretas es el de Australia, que lo que ha hecho es modificar la legislación de televisión<sup>3</sup> y remitir al sistema de autocontrol de la Autoridad Audiovisual.

En la línea de fomentar la autorregulación está también la Unión Europea desde

<sup>&</sup>lt;sup>1</sup> Aprobada el 27 de junio de 2002.

<sup>&</sup>lt;sup>2</sup> En concreto el artículo 8 llamado "restricciones a la prestación de servicios" establece que: "1. En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes: a) la salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional, b) la protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores, c) el respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social, y d) la protección de la juventud y de la infancia.

En la adopción y cumplimiento de las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el Ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión y el derecho a la libertad de información, cuando éstos pudieran resultar afectados.

En todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo..

<sup>2.</sup> Si para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un servicio o la retirada de datos procedentes de un prestador establecido en otro Estado, el órgano competente estimara necesario impedir el acceso desde España a los mismos, podrá ordenar a los prestadores de servicios de intermediación establecidos en España, directamente o mediante solicitud motivada al Ministerio de Ciencia y Tecnología, que tomen las medidas necesarias para impedir dicho acceso. (...)."

<sup>&</sup>lt;sup>3</sup> Se trata de la Broadcasting Services Act de 1999, disponible en el url: www.aba.gov.au/legislation/bsa/index.htm

que adoptó la *Decisión sobre el buen uso de Internet, de 25 de enero de 1999*, que vino precedido del *Libro Verde*<sup>4</sup> *de protección de menores y de la dignidad humana en servicios audiovisuales y de la información*. Ambos documentos, al menos en lo que al análisis de la situación se refiere, han servido de base al desarrollo del Internet Action Plan. Una política de fomento y financiación de iniciativas de "hotlines", software de filtrado y acciones de sensibilización.

Las hotlines, o líneas directas, repertorios o guías de trucos, son –dentro de lo discutible que uno las pueda encontrar- un medio voluntario de autocontrol que ha cobrado fuerza en Internet. Como afirman Machill y Rewer<sup>5</sup> "son un elemento esencial para eliminar contenido ilícito en la red. Estos medios pueden tener un papel central en el sistema de autorregulación que aúne a los estados, los consejos audiovisuales y a los usuarios".

En todo caso conviene diferenciar el contenido "ilegal" del contenido no estrictamente pornográfico pero relacionado con menores. Las líneas divisorias son difíciles de trazar, pero lo cierto es que la Unión Europea también distingue lo "ilegal" de lo "nocivo", siendo lo primero delictivo y por tanto perseguible por los tribunales y, lo segundo, evitable.

Las líneas de trabajo que sugiere este Documento, así como la *Decisión del 2000 relativa* a la lucha contra la pornografía infantil en Internet<sup>6</sup>, tienen que ser aplicadas por los proveedores, así como por las empresas. También la UNESCO lanzó en 1999 un Plan de Acción contra el abuso sexual de los niños, la pornografía y la pedofilia<sup>7</sup> apostando por una conducta responsable en el sector.

Las respuestas de otros gobiernos como el australiano o el británico, han creado respectivamente, <u>NetAlert</u><sup>8</sup> y R3-Safety net<sup>9</sup>, iniciativas para promover el uso seguro de Internet.

EE.UU tiene varias normas específicas, la mayoría del mandato de Clinton, alguna de ellas, como la *Child Online Protection Act* (COPA), impugnadas y aún en proceso de apelación. La que sí está en vigor es la *Children On line Privacy Protection Act* (COPPA), aprobada en 1998, que se refiere sobre todo a la recogida de datos en la web. Dado que EEUU no tiene ley de protección de datos, al menos ha considerado importante "limitar" la obtención y tratamiento de información sobre menores.

### Respuestas sociales y de la industria: filtros, etc.

Son muchas las iniciativas de todo tipo para promover un uso razonable y educativo para los menores. Además de los organismos públicos hay un sinfín de entidades no lucrativas y empresas que se dedican especialmente a esto.

<sup>&</sup>lt;sup>4</sup>COM (96) 483 accesible en el url: europa.eu.int/en/comm/dg10/avpolicy/new\_srv/comlv-en.htm

<sup>&</sup>lt;sup>5</sup>Machill, Marcel y Rewer, Alexa, Internet Hotlines, Evaluation and self-regulation of Internet content, Gütersloh, 2001.

<sup>&</sup>lt;sup>6</sup>Decisión del Consejo de 29.5.2000, DOCE 9.6.200, L 138.

<sup>&</sup>lt;sup>7</sup>URL: www.unesco.org/webworld/child\_screen/conf\_index\_2.html

<sup>8</sup> URL: www.netalert.net.au

<sup>9</sup> URL: dtiinfo1.dti.gov.uk/safety-net/r3.htm

Por ejemplo, <u>Childnet International</u><sup>10</sup>, es una organización sin ánimo de lucro que busca promover los intereses de los niños en las comunicaciones internacionales; tiene su sede en Gran Bretaña.

Son más conocidas otra iniciativas: la norteamericana para la difusión de filtros y sistemas de clasificación, la *Internet Content Rating Association*<sup>11</sup> y la europea, INHOPE Association<sup>12</sup>, que reúne a responsables de "hotlines" europeas o asociaciones de ellas, de varios países europeos, así como de EEUU, Australia e Islandia.

Esta última asociación es el prototipo de acción política que se propone la Unión Europea en el *Internet Action Plan*, y dedica como es el caso, recursos a financiarlo. Sus objetivos son "facilitar la cooperación entre las diferentes líneas directas contra la pornografía infantil en Internet de Europa".

### Los programas de "bloqueo"

Los grandes de la red, al menos en lo que se refiere a portales y proveedores de acceso, American On Line (AOL), Microsoft Network (MSN) y Yahoo aplican desde hace meses ya filtros en los contenidos, aunque en junio del 2002 han anunciado conjuntamente una nueva herramienta para la protección de menores, en el marco de un encuentro promovido por la ya citada IRCA, el más importante consorcio para los contenidos en Internet.

Previamente al filtrado es necesario que los contenidos, ya sea de la red, como de la televisión, estén "clasificados". Según ese "rating" o conjunto de criterios se puede proceder al "etiquetado" de cualquier material (texto, imagen o sonido), de modo que —por ejemplo-conociendo que tal web o programa es de la escala 2- la etiqueta sobre la que opera el filtro pueda frenar su acceso.

Indudablemente el sistema de "etiquetado" es voluntario. Con el ICRA filter, que es gratuito, como con otros que ofrece el mercado de programas (Cyber Patrol, Cybersitter 2000, Cyber Snoop, Internet Guard Dog, Net Nanny and Norton Internet Security 2001) o de consorcios como Optenet o Zanox, o con los que tienen los propios navegadores (el Vigilante de Contenidos del Internet Explorer, o el de AOL, por ejemplo), cabe que algún material ilícito pueda no ser visto por los usuarios que lo han instalado.

Lo que es así de sencillo de explicar es muy complejo y de dudosa eficacia en la práctica. Sin duda contenidos extremos o muy explícitos pueden ser bloqueados, pero tanto el software<sup>13</sup> como la cultura y uso de la red en esto tienen aún que cambiar mucho.

<sup>10</sup> URL: www.childnet-int.org

<sup>11</sup> URL: www.icra.org

<sup>&</sup>lt;sup>12</sup>URL: www.inhope.org. También en esta web se encuentra el Informe elaborado en Mayo del 2002 sobre la situación.

<sup>&</sup>lt;sup>13</sup> Hay un interesante estudio sobre "Which Internet Filters Protect The Best?" en www.consumerreports.org/Special/ConsumerInterest/Reports/0103fil0.html. También hay información www.getnetwise.org o www.safekids.com.