COMUNICAR 10, 1998; pp. 111-116

Familia y escuela: el miedo a Internet

Antonio R. Bartolomé
Barcelona

Aunque en nuestro país todavía no es un problema de gran magnitud, lo va a ser dentro de muy pocos años, quizás meses. ¿Quién controla Internet? En algunos países como Estados Unidos el tema ya ha llegado hasta la elaboración de leyes que luego han sido anuladas por el Tribunal Supremo. Los padres se preocupan por los materiales a los que sus hijos pueden acceder desde dentro de su casa. Los profesores lamentan que sus alumnos «chatean» en horas de clase. Y en el otro extremo, ¿existe libertad de expresión en Internet? Este artículo pretende presentar algunos aspectos en relación a este tema; más puntos para una discusión que propuestas o respuestas.

1. Control externo a Internet

La verdad es que Internet es bastante resistente a los controles externos. Podemos encontrar dos grandes vías para tratar de controlar la red. Una es la seguida por el gobierno de la República Popular de China y por otros países y se trata de impedir por la fuerza el acceso. Para ello basta controlar-censurar los centros nacionales, impidiendo, por ejemplo, el acceso desde ellos a direcciones consideradas «molestas». Este tipo de soluciones no tiene mucho éxito como bloqueo total, aunque ciertamente dificultan mucho las cosas a los usuarios menos expertos o con menos recursos económicos.

La otra vía es la seguida en países democráticos en donde se trata de utilizar los mecanismos que permite la ley. Ésta es mucho más interesante pues plantea los auténticos retos a una sociedad democrática que se rija por el poder de los acuerdos y las leyes. Vamos a ver algunos casos famosos para analizar elementos clave del problema.

Una persona en California coloca un material en Internet. Este material es legal desde la perspectiva de las leyes californianas, pero no en Texas. Ahora otro individuo en Texas considera que ese material es indecente y lo denuncia. Un sheriff de Texas envía un requerimiento a su colega californiano que detiene al sujeto y lo envía a Texas para ser juzgado. El fondo jurídico es que los delitos contra las «leyes de la decencia» en Estados Unidos tienen el carácter de delito federal, pero las

leyes son dictaminadas por cada Estado. Veamos, aunque la situación jurídica es diferente, el concepto es que un sujeto puede ser juzgado en cualquier lugar del mundo, pues desde cualquier lugar del mundo puede accederse a sus materiales en Internet. Por ejemplo, usted coloca una frase de los «Versos Satánicos» y el gobierno de Irán lo manda ejecutar: ¿cuál es la diferencia conceptual entre este supuesto y el caso de Texas?

Karen Sorensen (1997) señala que la legislación que limita Internet en Estados Unidos (EEUU) o Alemania proporciona una base y una justificación a la que se produce en China, Singapur e Irán, donde el objetivo de los censores no es sólo el material pornográfico sino también las discusiones a favor de la democracia y la educación en los derechos humanos. Desde la perspectiva de una ley como la «Communications Decency Act» en EEUU, ¿qué puede objetarse a que China elimine información que «altera el orden público», o que Nghiem Yuan Tinh, Director del *Vietnam Data Communication Company* afirme que «Internet debe ser controlada no sólo por razones técnicas y de seguridad, sino también desde el punto de vista cultural» (Financial Times, 1995).

Así el problema es más complejo que permitir, o no ver, distribuir escenas pornográficas. Debemos pensar en el control general sobre la libertad de expresión, pero esto nos lleva a la libertad que invade parcelas de otro y finalmente a la agresión a otros.

Algunos países aplican un control sobre el efecto «liberalizador» de Internet limitando el acceso a grandes segmentos de su población, como es el caso de India y Arabia Saudita, por ejemplo, mediante impuestos exorbitantes o limitándolo a las Universidades. Por supuesto, si uno posee suficiente dinero como para pagar un acceso a través de compañías extranjeras puede entonces evitar ese control.

Pero, ¿dónde está el límite? No se trata sólo de «limitar la distribución de cierta información» en Internet. Por ejemplo, es posible rastrear y controlar los mensajes que se envían. Hace ya años se dieron casos en Francia en que utilizaba la información suministrada por los peajes de las autopistas (Agre, 1996). Si los gobiernos no pueden limitar ni controlar Internet, ¿quién puede impedir que alguien utilice esa información?

Y esto nos lleva todavía a otras situaciones. Por ejemplo, ¿qué pasa si alguien envía masivamente publicidad a través de Internet? Bien, si usted está utilizando una línea telefónica va a tener que pagar por recibir una publicidad que no ha pedido: ¡Usted paga por recibir la publicidad que otro le quiere enviar! Y de nuevo nos planteamos si es necesario que alguien supervise esa situación.

Y llegamos a los virus, malignos o benignos. En 1997 corría por Internet la «triste» historia de Jessica Nydek, una niña enferma de cáncer. El mensaje invitaba a ser reenviado –saturando la red– e indicando que una aportación de un centavo de dólar era añadido a la cuenta de una institución de lucha contra la enfermedad. La misma organización, «American Cancer Society», se vio obligada a aclarar que no tenía nada que ver con el tema y que se trataba de un «hoax/virus» que reaparece periódicamente y se propaga, afortunadamente sin dañar discos duros (ver información en http://www.cancer.org/chain.html).

Y terminemos con un caso extremo (NewsCom, 1997). En octubre de 1996 Andrea Lynn Vickery conectó con un grupo *on-line* buscando alguien que quisiera asesinar a su exmarido. Robert E. Lee Smith, un militar retirado le sigue el juego hasta que comprueba que efectivamente le paga mediante una tarjeta de crédito y la denuncia. ¿Y si hubiese sido otro quien hubiese contactado con Andrea?, ¿pode-

mos suponer que así se han concretado y cometido otros asesinatos? El asesino no tiene ninguna relación con la víctima y el autor-instigador del delito puede probar su absoluta inocencia. ¿Justifica este tipo de actos la existencia de organismos que «espíen» los mensajes privados enviados por Internet? Esto nos llevará al tema de los mensajes cifrados y los límites impuestos por el Gobierno Norteamericano a los sistemas de encriptación.

Así el problema es más complejo que permitir, o no ver, distribuir escenas pornográficas. Debemos pensar en el control general sobre la libertad de expresión, pero esto nos lleva a la libertad que invade parcelas de otro y finalmente a la agresión a otros.

¿Deben los gobiernos legislar sobre Internet? En los siguientes apartados veremos que muchos opinan que no.

2. El control desde dentro. Los sistemas automáticos

Se trata de programas que filtran los mensajes de modo que no puedan visitarse en la web materiales considerados inadecuados. Generalmente se refieren a materiales pornográficos y en ocasiones de tipo fascista o violento. Son programas que los padres o maestros pueden instalar en los «browsers» como *NetScape Communicator* o *Microsoft Explorer*.

Existen dos formas de enfocar el control. La más drástica parte del principio de que es mejor filtrar mucho que poco, así que se seeleccionan sitios de dudosa conducta y se filtra todo lo que provenga de ahí. La segunda aproximación desarrolla una lista de términos «peligrosos» y filtra todos los documentos que los incluyan. Este tema está descrito en varios sitios pero citaremos un corto trabajo de Bjorn y Yue Chen (1996).

Un programa que aplica uno o ambos métodos es CyberPatrol, de Compuserve. Este programa fue ofrecido inicialmente para alemán e inglés y luego para español y francés. Sin embargo es obvio que incluso así el programa es insuficiente. Solamente en España sería necesario considerar también los términos en catalán, euskera, gallego...

Pero hay que considerar un problema adicional: las diferencias culturales. Por ejemplo, mientras en USA ciertos films corrientes en Europa, son considerados películas «X» (pornográficas) por contener escenas de sexo explícito, en Europa los contenidos violentos son menos aceptados que allí.

Pero hay que considerar un problema adicional: las diferencias culturales. Por ejemplo, mientras en USA ciertos films corrientes en Europa, son considerados películas «X» (pornográficas) por contener escenas de sexo explícito, en Europa los contenidos violentos son menos aceptados que allí.

Otro problema se refiere a las interferencias entre lenguajes. Como el programa no identifica la lengua trata de aplicar varios filtros, por ejemplo, la palabra «sex» que es un filtro estándar en CyberPatrol, significa «seis» en Sueco, o «sade» significa «dije».

Lo más interesante de este planteamiento es que deja el control de Internet en el otro extremo del hilo, es decir, el emisor de contenidos no es responsable, sino que es el receptor el que debe velar por su seguridad.

Esta perspectiva no debe ser vista únicamente en esos aspectos ante los que los americanos y alemanes parecen tan sensibles, pero que desde una perspectiva latina no se diferenciarían de la posibilidad de que un menor compre una revista porno en un quiosco. También hay que considerar otros aspectos de seguridad como que se nos introduzca un virus, o que alguien ataque o simplemente curiosee nuestros ordenadores a través de Internet. Si no controlamos Internet mediante una legislación universal y compartida, no queda más

remedio que recurrir a programas que protejan «nuestro extremo del hilo». MCalister (1996) se plantea estas preguntas en relación a la seguridad en Internet:

• ¿Qué aparatos de seguridad deben implementarse para controlar lo que se publica en www?

• Muchos conocen los riesgos de los virus, ¿pero conocen otros riesgos potenciales?

• ¿Cuántas organizaciones tienen los recursos para realizar un análisis de riesgos en profundidad?

• ¿Qué salvaguardias existen para frustrar a los «hackers»?

• ¿Qué implicaciones hay en relación a la propiedad intelectual respecto a la protección de los datos, al copyright, patentes y al plagio?

• ¿Qué implicaciones hay para los delitos incluidos robo y pornografía?

• ¿Qué implicaciones hay en los contratos, con respecto a negligencia, entorpecimiento o deformación?

• ¿Qué implicaciones hay en los derechos de los consumidores y usuarios?

La pregunta que nos podemos hacer, en definitiva, es: ¿podemos defendernos de todo esto nosotros, los usuarios, sin acciones externas? Dentro del mismo marco de «autodefensa», pero dejando de lado la perspectiva individual y tomando una visión colectiva, llegamos a nuestro tercer apartado: la autodefensa comunitaria.

3. El control desde dentro. La autodefensa comunitaria

En la primera mitad de los noventa, ésta ha sido la herramienta básica de regulación de actuaciones en Internet. Supongamos que alguien envía un anuncio a una lista automática de distribución que no se lo ha pedido, o que alguien realiza afirmaciones racistas. Basta que uno lo sugiera y que todos los que estén de acuerdo envíen mensajes de protesta. En Internet eso puede querer decir miles de mensajes que bloqueen el servidor. El resultado es que el indeseable se ve privado de su sistema de correo y, si es alquilado, expulsado de él.

> Si hablamos de información, la situación es similar a la existencia de revistas en los quioscos: el que quiera que compre. Si hablamos de delitos como la distribución de virus o la intromisión en áreas privadas, entonces deben actuar las leyes. Pensemos que esto se aplica también a muchas facetas desconocidas hoy pero existentes.

Un ejemplo en nuestro idioma se produjo durante el verano de 1997 a raíz del caso de Miguel Ángel Blanco. Por la red comenzaron a distribuirse mensajes dando a conocer páginas relacionadas con ETA e invitando a enviarles mensajes. Éstos son los argumentos a favor y en contra de acciones como ésta.

A favor están todos una serie de argumentos tradicionales en Internet: no son acciones organizadas desde el poder, sino que sólo funcionan si los individuos se suman; la fuerza viene precisamente de la suma de decisiones individuales. Como el mecanismo es simétrico, demuestra la auténtica fuerza democrática de una idea. Para que alguien participe en una campaña de este tipo no suele bastar con que disienta del otro sino que debe sentirse realmente amenazado. Es, pues, un sistema democrático y autorregulable de acción contra los delincuentes.

No hay demasiados argumentos en contra, pero los recoge Álvaro Ibáñez en *iWorld* (Ibáñez, 1997). El fundamental es esta frase: «Quienes opinen lo contrario deberían confiar en la inteligencia de las personas, para, por un lado, decidir libremente si quieren visitar esas páginas o no, y por otro, interpretar el mensaje que contengan». Pero añade otros: «no vale la pena conseguir cerrar un servidor, porque en

otro lugar aparecerá uno nuevo: la censura es imposible en Internet».

Para complicar más la situación podemos considerar dos elementos más. El primero, el hecho de que una mayoría pueda «linchar» a una minoría. Es obvio que este sistema defiende fundamentalmente los derechos de la mayoría, y que es más difícil de aplicar por una minoría.

El otro elemento me lo sugiere una vieja historia: en 1995 una lista de Internet denominada «alt.religion.scientology» se vio atacada por cientos de mensajes provenientes de un grupo –o secta– también llamada Scientology y que estaba disconforme con los contenidos vertidos en la lista. El tema es que aunque el mecanismo se basa en la suma de decisiones individuales, éstas pueden aunarse no sólo como resultado de una reflexión personal o libre o por la influencia de un estado de opinión creado por los medios. También puede darse el caso de organizaciones que pueden «recomendar» acciones determinadas a sus miembros. Por ejemplo, en 1997 una importante rama de cristianos no católicos en Estados Unidos invitó a sus miembros a no comprar ni utilizar productos Disney por considerar que la actitud de la empresa de no discriminación de homosexuales entre los empleados era contraria a sus creencias. ¿Qué pasaría si hubiese invitado a sus 700.000 miembros a enviar mensajes vía Internet colapsando el servidor de Disney? Aún cuando realmente la empresa siga una línea contraria a ellos, ¿debe ser penalizada cuando esa línea es aceptada por muchos otros? Y supongamos que Disney decide cambiar su política: ¿qué pasa si son ahora los miles de homosexuales los que lanzan la campaña? ¿Se volverá Internet un lugar inseguro, a merced de todos los grupos de presión del mundo?

Con todo lo anterior, no podemos desdeñar fácilmente este sistema y es necesario diferenciarlo del mecanismo de control democrático que un renombrado especialista en Internet define como «action alert» (Agre, 1997). Lo define como un mensaje que alguien envía a la red invitando a una acción específica en relación a un tema político actual. «Bien diseñadas las 'action alerts' son un medio poderoso para invitar a la gente a participar en los procesos de una democracia». E incluye algunas recomendaciones:

- Establecer la autenticidad. Indicar claramente quién la envía y cómo contactar.
- Poner fecha. Los mensajes a veces duermen meses en un «mailbox» antes de despertar.
- Delimitar claramente el texto de la alerta.
- Precaverse de modificaciones que exageren o deformen el mensaje.
- Pensar hasta dónde deseo propagar el aviso.
- Construirlo de modo que tenga toda la información necesaria.
- Invitar a una acción clara y definida.
- Hacerlo fácil de entender.
- Revisarlo bien antes de enviarlo.
- Iniciar un movimiento, no una desbandada («enviar donde sea apropiado»).
- Explicar la historia completa.
- No utilizar un lenguaje para convencidos.
- Evitar polémicas.
- Evitar las peticiones en cadena.
- Utilizar prácticas «buenas».

4. Control desde dentro. El propio individuo

Con esto hemos llegado a la última posición, la que defiende que sea el propio individuo el que actúe y tome decisiones. Esta idea encuentra su fundamentación en el neoliberalismo aunque también es promovida desde otras concepciones. La idea es: si hablamos de información, la situación es similar a la existencia de revistas en los quioscos: el que quiera que compre. Si hablamos de delitos como la distribución de virus o la intromisión en áreas privadas, entonces deben actuar las leyes. Pensemos que esto se aplica también a muchas facetas desconocidas hoy pero existentes como el blanqueo del dinero del narcotráfico a través de Internet, sin posible control.

Desde esta perspectiva, la tarea de padres y profesores es ayudar a los alumnos a tomar

las decisiones correctas. Sin embargo es necesario ser consecuente hasta el final con esta opción. La capacidad de tomar decisiones lleva implícita la capacidad de equivocarse así como la de tomar decisiones diferentes de las que nosotros tomaríamos. Este punto excede la polémica concreta de Internet y se extiende a decisiones sobre nuestra acción educativa.

Voy a terminar este artículo recordando que existen otros aspectos relacionados con el tema que no han sido tratados, por ejemplo, la posibilidad de utilizar sistemas de encriptación que protejan nuestros mensajes del control de otros, incluida la policía. Este tema ha gozado de una gran popularidad en EEUU debido a la legislación que prohibía utilizar sistemas cerrados a una inspección gubernamental.

Ésta ha sido una revisión rápida a una problemática compleja y que abarca situaciones muy diferentes. ¿Cómo debemos actuar los padres y los educadores en relación a Internet?

La pregunta está servida.

Referencias

AGRE , P. (1996): Mensaje enviado. Sun, 26, May, 1996 17: 23: 15-0700 (PDT), a la lista Red Rock Eater. http://communication.ucsd.edu/pagre/rre.html

AGRE , P. (1997): Designing Effective Action Alerts for the Internet. Mensaje enviado 17/9/97 a RedRockEater. Ver también en: http://communication.ucsd.edu/pagre/

BJORN, M. & YUE CHEN, Y. (1996): «The Worldwide Market: Living with the Realities of Censorship on the Internet». Webnet'96. San Francisco 15-19 octubre de 1996, http://curry.edschool.Virginia.EDU/aace/conf/webnet/html/108/108.htm

FINANCIAL TIMES (1995): «Plan by Telecom Authority to Exercise Control Over Internet Disturbs Foreign Investors and Agency». London: Financial Times, Sept. 19, 1995.

IBAÑEZ, A. (1997): Editorial. *iWorld* , suplemento de *PC-World* 135, Oct. 1997.

MCALISTER, M.J.; COMER, P. & HADLEY, K. (1996): The Internet & The WWW: Friend or Foe? Webnet'96. San Francisco, 15-19, octubre de 1996, http://curry.edschool.Virginia.EDU/aace/conf/webnet/html/388.htm

NEWSCOM (1997): Noticia de prensa, fechada el 2/10/97, http://www.usatoday.com/life/cyber/tech/ctb361.htm

SORENSEN, K. (1997): Silencing the Net. The Threat to Freedom of Expression On-line. Human Right Gopher, gopher://gopher.humanrights.org:5000/11/int/hrw/general

Antonio R. Bartolomé Pina *es profesor del Departamento de Didactica i Organització Educativa de la Universitat de Barcelona.*

Reflexiones desde el butacón