



# La red y los jóvenes, ¿donde está el peligro?.

junio 2001

Por [Javier Delgado](#)

*Para los que tenemos hijos, el dejarles el acceso a la red parece cada día más peligroso. Los medios nos dicen que existe gran cantidad de pornografía, pedófilos y criminales que están al pendiente de cómo atraparlos. Por ello intento con este artículo resumir los peligros reales de la red, y ya que la mayor preocupación es la pornografía, empesaré por ahí.*

El contenido pornográfico en la red tiene dos orígenes, uno es comercial y con fines de lucro, pero también existen una gran cantidad de **aficionados** que suben pornografía a páginas gratuitas y a los canales de IRC y News.

## La Pornografía comercial

Según las estimaciones, menos del 3% del contenido de Internet se puede considerar pornográfico, sin embargo dado que es un gran negocio, los proveedores de este tipo de contenido utilizan técnicas muy agresivas para promocionarse por lo que pareciera que el volumen es mucho mayor, por esto muchas veces nos puede llegar contenido pornográfico, incluso sin buscarlo y una vez ahí a veces utilizan técnicas que dificultan salir de esas páginas.

Es importante platicar esto con nuestros hijos pues se vuelve casi inevitable que eventualmente se topen con contenido pornográfico, y ya que algunas páginas contienen programas que parecen tomar control de nuestra computadora, esto puede crear temor en los jóvenes..

Hay varias formas en que se puede llegar al contenido pornográfico sin buscarlo.

En primer lugar están los anuncios dentro de otras paginas o **banners**. Los banners son esas pequeñas tiras que muchas paginas tienen en la parte superior y se han vuelto muy comunes pues con eso el autor del sitio o pagina percibe una pequeña cantidad de dinero o recibe promoción a cambio, según el número de veces que la gente pica en esos anuncios. Hay muchas empresas de publicidad que utilizan este método, y la mayoría de ellas no aceptan anuncios relacionados con pornografía, pero otras no oponen reparo alguno al tipo de contenido del banner, además existen sistemas de intercambio de banners organizados por pequeñas compañías o incluso por aficionados, que permiten que uno publicite de manera gratuita su pagina, lo que es muy útil para aquellos que empiezan a promocionar sus paginas personales, pero como esos banners cambian constantemente, sin saberlo uno puede estar publicitando pornografía en su pagina personal.

También como promoción, las compañías de pornografía patrocinan a muchos sitios de "**Warez**", es decir lugares donde se obtiene software pirata, como juegos "crackeados", passwords para abrir protecciones, intercambios de tips para juegos de computadora o de consolas, software para crear puertas traseras (acceso oculto a sistemas de computo) y programas para "**crackear**" esquemas de protección. Es en la búsqueda de estos materiales como muchos jóvenes llegan a las paginas pornográficas, además muchas paginas de Wares ofrecen "passwords" para acceder a paginas pornográficas, usualmente estos passwords son solo ganchos que dan acceso a material de poco valor, pero que tienen el propósito de estimular la curiosidad.

También los promotores de pornografía patrocinan algunos lugares donde se tiene espacio gratuito en Internet, a cambio de poner sus anuncios en esas paginas.

Otras técnicas a las que recurren para promocionarse, son el uso de **Spam**, es decir correo comercial no solicitado, y que por cierto técnicamente es ilegal en Estados Unidos. Para esto usan software (que se conoce como **spiders**) que recorre la red en buscando direcciones de correo dentro de las paginas de internet, también utilizan las cadenas de correo (del tipo "*firme esta petición para salvar a un niño enfermo*", o "*avise a sus amigos que hay un nuevo virus peligrosísimo...*" etc.), si reciben un correo de este tipo podrán observar puede llegar a contener cientos de direcciones de **E-mail** y cuando las envía a sus conocidos,

esta incluyendo sus direcciones en el correo, así que basta con crear y recopilar estos avisos para poder reunir una gran cantidad de direcciones de correo, para enviarles publicidad.

Además en muchos sitios de Internet, se pide la dirección de correo para poder usar algunos servicios, estas direcciones pueden recopiladas y vendidas. Una base de datos con 1 millón de correos se puede adquirir hasta por 100 dólares. *(nota: en muchos lugares existe una cláusula de confidencialidad que nadie se preocupa de leer...)* Por ello hay que tener cuidado antes de proporcionar nuestros datos, también puede ser recomendable tener una dirección de correo en un sitio gratuito y usar esta dirección exclusivamente para dar como referencia.

Con esta información se hacen envíos masivos de correos conteniendo invitaciones a visitar páginas xxx, usualmente son páginas que presentan algunas imágenes de gancho para atraer al sitio de pago. A veces tratan de atraer con el gancho de que se dan passwords etc. o pretender ser de alguna joven que busca algo emocionante.

Una vez que el usuario pica en uno de estos enlaces se tiene algunas técnicas para tratar de retenerlo. La más popular se llama "Mouse trapping". Dentro de una página de Internet se puede introducir una programación relativamente sencilla, que hace que al abrir o cerrarse la página se abra una nueva ventana a otra página o simplemente vuelve a abrir la ventana *(nota, esta técnica, también a sido declarada ilegal en EUA)*. Así, quien entra a una de estas páginas y no paga, puede terminar con una docena de ventanas que no puede cerrar, pues como la mítica hidra, al cerrar una, se abren dos ventanas más. Esto puede asustar a muchos usuarios inexpertos. Una solución es desactivar temporalmente el soporte de **Javascript** del navegador.

Otra técnica de promoción consiste en el uso de software conocido como "**robots**" en los **chats** y el **IRC** (ver más adelante en chats). Los robots consisten programas que monitorean la actividad de algunos canales de Chat. Debido a que cuando un chat se queda vacío, el primero que entra en él tiene privilegios de moderador *(puede decidir quien entra o no al chat)*, para evitar perder estos privilegios algunos usuarios expertos crearon programas para **simular** que alguien está siempre en el chat. Pero estos programas pueden tener otro uso, pueden responder cuando alguien entra al chat, o cuando menciona alguna palabra específica, e

inmediatamente le contesta y ofrece enviar links a sitios pornográficos, es como una especie de contestadora automática. Aunque estos robots no son muy sofisticados, a veces es fácil confundirlos con una persona real, tal vez un poco enajenada. Y a pesar de que muchos canales de IRC (Internet relay chat) prohíben el uso de robots a los pornógrafos les tiene sin cuidado.

Una técnica reciente, aunque afortunadamente aun no muy popular es el uso de virus como publicidad, como el reciente virus "[homepage](#)", que modifican al navegador para que por default entre en un sitio xxx. Probablemente en el futuro veamos variantes de esta técnica.

Debido a que la pornografía es un gran negocio, y que necesitan cobrar a través de tarjetas de crédito, muchos vendedores de pornografía están tratando de ser (o aparentar ser) respetables y establecer ciertas barreras entre la pornografía que ellos llaman "sana" (lo que incluye cierta dosis de sadomasoquismo y a veces bestialismo) y los "degenerados". Un ejemplo es el sitio [TheHum](#), una especie de directorio amarillo y que actualmente es uno de los sitios mas redituables de la red, siendo manejado por desde Holanda por Patrick Terwee y su esposa. De vez en cuando ellos tienen un campaña para recolectar "**osos de peluche**" entre su auditorio, para los orfanatos y en su pagina insiste que hay que luchar contra la pornografía infantil. También muchos de estos sitios han lanzado campañas a favor de la libertad de expresión, lo que no hace muy felices a los defensores de los derechos humanos, pues prefieren evitar ese tipo de apoyo.

### Los amateurs

A diferencia de los sitios de pornografía comercial que están tratando de autoregularse para hacer negocio, los aficionados no tiene ninguna limitación. Muchos simplemente escanean su colección e revistas y la suben algún servicio de paginas gratuitas. Muchos lugares donde se ofrecen paginas gratuitas como [www.geocities.com](#), [www.angelfire.com](#) y [www.freepages.com](#), tienen políticas muy estrictas contra esto, pero debido que tiene millones de sitios por vigilar no es raro encontrar pornografía incluso en sitios inesperados (como paginas familiares o de religión) es importante denunciar estos sitios al webmaster para que sean removidos.

### USENET

También existen lugares donde se intercambian fotografías entre personas o parejas. Un lugar favorito son los canales de **news groups** o [USENET](#), que es uno de los servicios mas viejos de Internet (y que para los veteranos es el verdadero Internet). Sin embargo muchos proveedores de servicio no dan facilidades para conectar a esta parte de la red, por lo que usualmente solo los usuarios mas expertos conocen estos servicios, y a pesar de que ya hay paginas de internet dedicadas a dar acceso mas sencillo, la mejor forma de accederlos es usar un programa especial de News, o configurar Outlook o Netscape Mail con las direcciones de **news** proporcionadas por el proveedor de conexión. Es importante hacer notar que los "**news groups**" tienen mucha información valiosa, pues nacieron como foros de discusión entre las universidades y uno puede encontrar interesantes foros de ciencias, humanidades, computación, antropología etc. Hay mas de 55,000 temas para escoger. Para evitar problemas muchas universidades bloquean el acceso a ciertos canales, en general los que comienzan con "alt.sex" o "alt.bin". La UNAM es un ejemplo, pues ellos bloquean los canales mas objetables. Aun así, un usuario determinado puede lograr acceso a través de muchos servicios alternativos y es justamente en estos canales donde se puede encontrar a algunos de los personajes mas extraños de la red, desde los autores de los virus, hasta a voyeurs, fetichistas y pedofilos.

### Los Chats.

Los chats son un tema muy especial, pues son de uso mas sencillo que los canales de news. Existen una red mundial de [Chats](#) que se maneja a través de programas especiales conocidos como [IRC](#) (Internet Relay Chat), el mas popular se llama [mIRC](#), sin embargo estos han cedido mucho a favor de los chats localizados en paginas comerciales de la red y que no requieren ningún software en especial.

Cuando se usa uno de los programas de acceso al IRC, se pueden enviar links, imágenes, sonido y software, por lo que también son un método muy favorecido para contactar personas e intercambiar material.

Debido al sentimiento de anonimidad que se tiene en el chat, la gente tiende a ser mas abierta o a tratar de vivir una fantasía. No es raro la mujer de 40 que dice tener 18, o el viudo que pretende ser un joven roquero... Aunque estas fantasías por si solas no son un problema, una persona hábil

puede aprender a manipularlas y ese el mayor peligro que puede enfrentar un joven inexperto. Los chats son un gran lugar de reunión entre los jóvenes, por lo que conviene enseñarles a valorar su intimidad y a razonar con el tipo de gente que llegan a conocer. Hay que hablar con ellos pues otro gran problema es que muchos padres desconocen completamente la mecánica de la red y son incapaces de dar consejo a sus hijos sobre estos temas. Debido a la gran cantidad de denuncias estos son los lugares que vigilan el FBI en EUA y la PFP en México, sin embargo existen cientos de direcciones de IRC y algunas contienen hasta 5,000 canales de charla, lo que hace muy difícil su supervisión.

Además es muy importante explicar al joven que el sentimiento de anonimidad que da el Chat, es aparente, pues una persona suficientemente determinada puede localizar la identidad real de los usuarios. Puede ser tan sencillo como enviar un "caballo de Troya", es decir un programa oculto dentro de otro programa, (*"te mando esta animación, esta padre..."*). Una vez dentro de la computadora, el [caballo de Troya](#) introduce lo que se llama una [puerta trasera](#), que

permite tener acceso a todos los archivos, programas y "passwords" en la



computadora de la víctima. En un caso reciente, una joven fue espiada por su ex-novio, que le envió un programa conocido como Back Orifice, y pudo tener acceso tanto al micrófono, como a la cámara que venía instalada en su computadora. También es posible trazar las huellas que deja la conversación y llegar hasta el proveedor de conexión del usuario, y al menos obtener su dirección real de correo electrónico.

Ejerciendo la Censura.

Para evitar el acceso de los jóvenes a contenido "indeseable" se ha desarrollado software llamado "filtrado de contenido" y también "censorware"



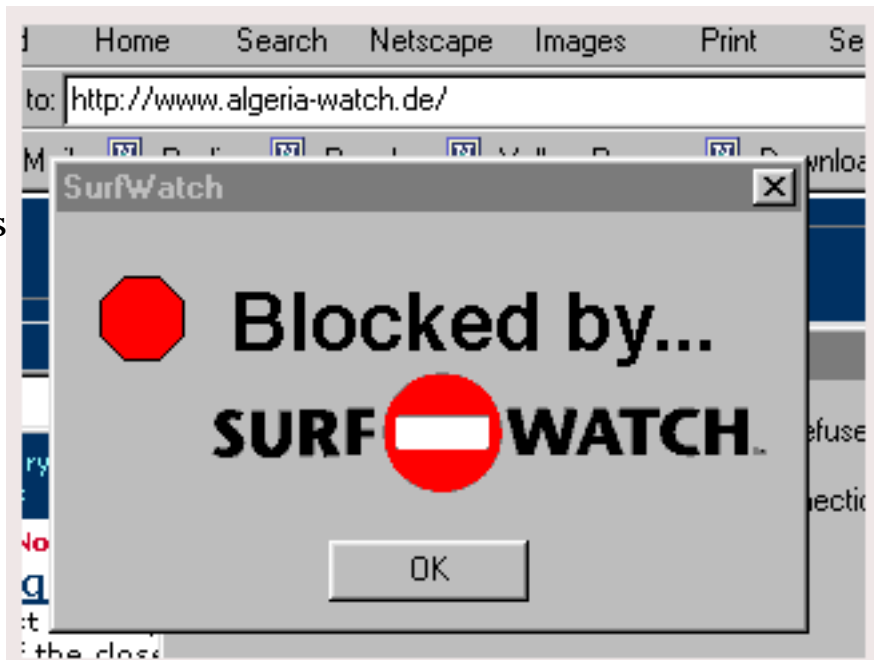
( [lea mi artículo sobre censura](#)) por sus detractores. Este software monitorea y bloquea el acceso a cierto tipo de sitios según cierto criterios. Cuando se trata de entrar a un sitio fuera de límites, generalmente aparece una pantalla indicando que no setiene autorizacion para entrar, ademas se genera una bitacora para los padres de los sitios que se ha intentado accesar.

Es importante saber que este software no es una panacea, pues existen tres problemas principales.

**Primero**, mucho jóvenes saben mas de computación que sus padres y pueden aprender a neutralizar los filtros, existen paginas en la red dedicadas a ello.

**Segundo**, los filtros no son 100% efectivos, fueron desarrollados para el habla inglesa y pueden fallar al tratar en otros idiomas o con sitios que solo contienen imágenes. Este software funciona de varias maneras:

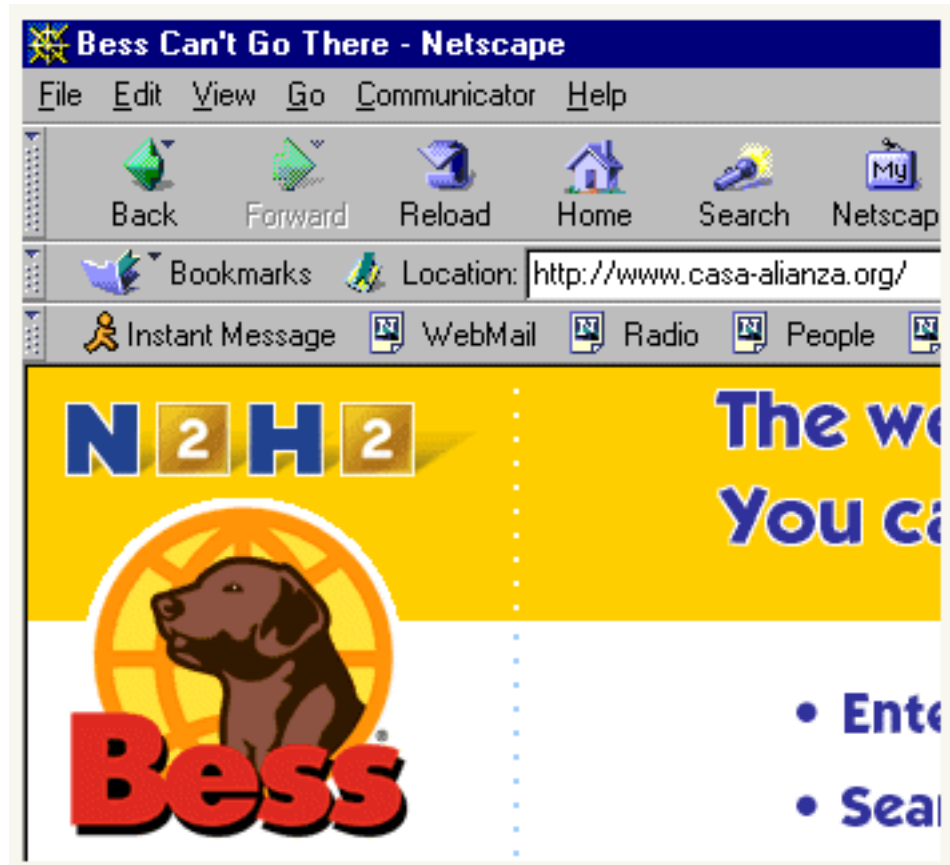
Por una parte tienen un lista de lugares prohibidos y además buscan palabras claves. Debido al gran tamaño de Internet (estimado en 5 mil



millones de documentos) no hay manera de que exista una lista real de contenido de la red (ningún buscador de Internet tiene revisado mas del 15% de la red), así que tienen que basar su criterio en buscar palabras clave como "mayores de 18", "xxx", sexo etc. El problema de esto es que puede bloquear muchos lugares inocentes. Por ejemplo si alguien hace una pagina para celebrar su **xxx** aniversario o sobre "**la reproducción asexual de las bacterias**" puede quedar clasificado automáticamente como pornografía. En un estudio del [Censorware Project](#), se reporto que los filtros de contenido bloqueaban hasta un 70% de sitios de manera errónea. Durante cierto tiempo, la pagina de la "Casa Blanca" estuvo bloqueada porque mencionaba a "**la pareja presidencial**". De igual manera, la palabra castor (**beaver**) tiene un doble sentido en ingles, y la sola mención de castores bloquea muchas paginas, incluyendo "[The Beaver University](#)", una sólida institución que tiene 120 años y que tuvo que finalmente tuvo que cambiarse de nombre a **Arcadia** debido a que muchos filtros bloquean el acceso a su sitio web.

**Tercero**, debido a que mucho de el software de contenido

esta



impulsado por asociaciones de padres de familia de EU, (que por alguna razón, tienen un sesgo político de derecha o conservador), el software tiende a bloquear sitios que no tiene que ver con el sexo o con un contenido impropio sino con su aspecto político. Hay muchos sitios de derechos civiles, asociaciones feministas, de derechos humanos y de educación sexual que también están bloqueados, el bloqueo incluye a veces lugares de anatomía, ginecología y algunas galerías de arte (El sitio del Vaticano alguna vez ha esto bloqueado...). Como ejemplo esta el sitio [www.peacefire.com](http://www.peacefire.com), que es una asociación de estudiantes que se oponen al software de filtrado. Su sitio esta bloqueado por la mayor parte del software de filtrado bajo las categorías de **"pornografía, obsceno, sadomasoquista, odio, intolerancia, ilegal, violencia, uso de drogas etc."** basta ver su sitio para encontrar que no hay nada de esto, aunque lo que si tiene es instrucciones para que los jovenes eliminen o desactiven el software de filtrado instalado por sus padres. En todo caso hubiera bastado bloquearlo solamente en la categoría de "ilegal".

Hechas estas aclaraciones, estas son las direcciones de los principales proveedores de software de filtrado

[N2H2 BESS](#)

[Net Nanny](#)

[Cyberpatrol](#). Tiene demo gratuito

[Surfwatch](#)

[Smart Filter](#) Diseñado originalmente para uso corporativo

Algunos, como CyberPatrol, ofrecen una versión de prueba por 30 días, suficiente para las vacaciones de verano.

Si los padres deciden recurrir al software de filtrado debe ser consultando con sus hijos y explicando bien las razones par evitar el contenido impropio, pues de otra manera el bloqueo puede ser contraproducente, pues puede crear un aliciente para buscar el "contenido prohibido". Tal ves la mejor solución es no instalar al computadora en la recamara de los jóvenes, sino en un área común de la casa, donde todos puedan participar y así evitar que sea un lugar donde el joven se refugie. El mejor software de filtrado se llama "criterio", pero ese debe ser instalado por los propios padres a través del ejemplo y el acercamiento al joven.

Solo así se puede aprender a disfrutar de la gran riqueza que yace en la red, pues hay que recordar que lo que ve en su navegador solo es una parte de sus servicios.

## Los Peligros

Una triste realidad de la red, es que efectivamente existe [pornografía infantil](#), lugares de reunión de [pedofilos](#). Pero tampoco hay que perder la perspectiva real de las cosas, el 70% de los [abusos a menores](#) son cometidos en el hogar por un pariente o un conocido del niño. Y en otro porcentaje apreciable, el niño cae en las manos de personas sin escrúpulos tratando de huir su realidad. Así como hay padres que usan la televisión como niñera, si saber lo que ven, también hay padres que usan la computadora como niñera, olvidando que lo mas valioso que se le puede dar a un niño es la atención de sus padres.

*Javier Delgado*

*Paralax multimedia*

*México Junio 2001*

## Recursos.

[Aprovecharse del Abuso](#)

Investigacion sobre la explotacion sexual de niños y niñas.

UNICEF 2001. Archivo en formato pdf. 900KB

**Javier Delgado, *México Junio 2001***

Calzada de las Armas#16 , Naucalpan de Juarez, Edo Mex.  
tel/fax (5) 373 3620 | (5) 363 4953

[D.R. Parallax Multimedia 1999](#)