00761

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE DERECHO

DIVISION DE ESTUDIOS DE POSTGRADO

LAS GARANTIAS CONSTITUCIONALES DE LIBERTAD DE EXPRESION Y DE INFORMACION VULNERADAS POR EL CONTENIDO NOCIVO E ILICITO DEL INTERNET

T E S I S

Q U E P R E S E N T A :

LIC. ALEJANDRA CARBAJAL VALDEZ

QUE PARA OBTENER EL GRADO DE:

M A E S T R A E N D E R E C H O

DIRECTOR DE TESIS

DR. JULIO TELLEZ VALDES

MEXICO, D. F. 2004

A mi esposo,
Quien es mi fuente constante de motivación, apoyo y amor,
Quien lucha, crece y comparte conmigo el éxito y el desacierto.

A mis padres, bollita, hermanas, cuñados (as) y sobrinos
Por su amor, cariño, comprensión y ayuda invaluables.

A la Suprema Corte de Justicia de la Nación,
Honorable institución quien a través de sus recursos materiales y humanos fortalece y exhorta a su personal a crecer laboral, profesional y humanamente para coadyuvar con ella en sus objetivos de manera eficaz.

A la Universidad Nacional Autónoma de México,
Casa sublime que albergas a todos los que buscamos el conocimiento.
Cuna de gente Ilustre.

A mis Maestros
Quienes con sus magistrales enseñanzas, experiencias y conocimientos enriquecen mi vida.

Ministra Margarita B. Luna Ramos
Por ser un ejemplo de esfuerzo y superación admirados y reconocidos para el Poder Judicial.

Dr. Julio Téllez Valdés
Mi agradecimiento especial por su apoyo y orientación incondicionales en la elaboración de esta tesis.

A mis compañeros y Amigos
Por compartir diariamente mi experiencias laborales y profesionales.

INDICE

INTRODUCCION

El desarrollo de las nuevas tecnologías ha supuesto un gran cambio en el proceso de difusión de la información que hasta ahora conocíamos. Hasta hace pocos años, si una persona deseaba que una determinada información llegase a una pluralidad de destinatarios únicamente disponía de los medios tradicionales (teléfono, fax, libros, periódicos, radio o televisión), con las consiguientes limitaciones en cuanto a los costos económicos y a las licencias que debía solicitar de las autoridades nacionales competentes.

En la actualidad, sin embargo, cualquier persona puede hacer llegar información en forma de texto, gráficos, sonidos o imagen al resto de los ciudadanos del mundo a partir de un costo relativamente bajo. Ahora bien, los bajos costos de la comunicación a través de las redes digitales contrastan con el elevado costo económico de los equipos de software y hardware que el usuario necesita para acceder a Internet, Sin embargo, el descenso de los precios de los equipos informáticos hace que, cada vez más, una familia media mexicana pueda acceder a ellos.

El navegar en Internet ha traído grandes ventajas como el poder comunicarse inmediatamente y/o intercambiar información y opinión sobre temas de mutuo interés sin límites de frontera, dadas sus características: **global** (proporciona un acceso inmediato a la información procedente de cualquier parte del mundo, sin límites geográficos), **descentralizada** (es un sistema descentralizado, que trabaja sin vigilancia y que crea múltiples puntos de acceso), **abierta** (tiene escasas barreras de acceso siendo la creación y difusión de información extremadamente bajos), **grande** (tiene una capacidad ilimitada de almacenamiento de información), **interactiva** (permite comunicaciones de uno a uno, de uno a muchos y de muchos a uno), **controlada por el usuario**

(puede controlar que información que llega a su ordenador), **independiente de la infraestructura** (no está ligada a ninguna infraestructura, aparte del sistema telefónico). Así el Internet no tiene un centro rector que dirija o apruebe el contenido que libremente circula en ella. Internet es controlada por todos los usuarios y son los usuarios que deciden pasar de un servidor a otro y elegir el contenido que desean ver. Esto lo puede realizar sin ser identificados y por tanto imposible determinar si el usuario es menor o mayor de edad[1].

La gran Red y la masiva informatización trajo consigo una gran cantidad de factores desestabilizantes dirigidos a la persona en sí: comunicación invasiva y amenazante como pornografía y publicidad engañosa, correo electrónico no solicitado (junk email o spam), sustracción y plena administración y disposición de los datos personales de los titulares del dato, o bien dirigidos a sus bienes materiales: virus autoreplicantes-mutantes-mutilantes, cookies, hacking, etc. Así pues de entre estos factores desestabilizantes.

Todo progreso genera nuevos riesgos, y por ello es comprensible que autoridades, organizaciones y usuarios observen con cierta preocupación cómo las características del nuevo medio -oferta ilimitada, descentralización, destinatario universal, internacionalización de la relación, ausencia de control, anonimato -posibilitan la multiplicación de mensajes que un ordenamiento jurídico pudiera calificar como ilícitos o que pudieran ser considerados como nocivos por una comunidad determinada. Si resulta imprescindible identificar tales contenidos y determinar quiénes son los actores que participan en su concepción y en su difusión, las cuestiones verdaderamente relevantes hacen referencia a la responsabilidad de estos intervinientes y, sobre todo, a la lucha contra la proliferación de tales contenidos en la telaraña mundial. Las próximas líneas permitirán conocer muy puntualmente todos estos problemas.

[1] Rodriguez Pereda, Katitza. TRATAMIENTO JURIDICO DE LOS CONTENIDOS NOCIVOS E ILEGALES QUE CIRCULAN EN INTERNET. Memorias del VIII Congreso Iberoamericano de Derecho e Informática por la Universalización del Derecho. México. 21 a 25 de noviembre del 2000.

La presente tesis nos motivará a reflexionar sobre los principales problemas que surgen al abordar los contenidos ilícitos y nocivos en Internet y las posibles soluciones a los mismos, ya que se ha procurado evitar un vocabulario excesivamente técnico.

El carácter transnacional de Internet obliga a realizar una aproximación internacional, presentando los casos más relevantes suscitados ante los tribunales, las leyes elaboradas por los estados involucrados así como las actividades que se llevan a cabo en los diversos foros internacionales, tanto públicos como privados.

Durante el tiempo que ha transcurrido desde el inicio del presente trabajo hasta su redacción final, las noticias no han dejado de producirse. Debido a la rapidez con la que se suceden los acontecimientos no es posible recoger todas y cada una de las iniciativas legislativas, los casos jurisprudenciales o los nuevos productos que aparecen cada día en el mercado para aumentar la utilización segura de Internet.

Por ello se incluyen al final de esta tesis las referencias que han sido utilizadas para su elaboración. En ellas, se encontrarán las direcciones de Internet de donde se ha obtenido la información y de este modo se podrá completar aquellos aspectos de la tesis que le resulten más interesantes. Las notas a pie de página han sido reducidas al mínimo y se completan con la bibliografía y con los índices de legislación y jurisprudencia citada, así como las direcciones de interés, que conducen de unas a otras, a nuevas fuentes de una información que se actualiza sin cesar.

CAPITULO I

DE LAS GARANTIAS CONSTITUCIONALES RELATIVAS A LA LIBERTAD DE EXPRESION Y DE INFORMACION

1.1. LIBERTAD DE EXPRESION

De la capacidad del hombre para pensar surge una esencial libertad entendida en sentido filosófico, que le es propia y exclusiva y que por su naturaleza no puede quedar sujeta a ninguna regulación jurídica. Como correlato a la libertad de pensar surge la de expresar el pensamiento, y esta expresión, en virtud de que se manifiesta en el mundo fáctico, sí puede ser objeto de una normatividad jurídica. Dicha normatividad se expresa, en primer término, en las Constituciones modernas como un freno a la actividad del Estado, el cual no debe establecer limitaciones a la libre expresión, salvo en los casos que la comunidad, a través del propio derecho, juzga indispensable hacerlo.

La libertad de expresión se considera entre las más preciadas por la ideología liberal, que la consagra en la Declaración de Derechos del Hombre y del Ciudadano, emitida en Francia el 26 de agosto de 1789. El artículo 10 de dicha declaración señalaba que ninguno debía ser molestado en sus opiniones, aun las religiosas, en tanto que la manifestación de ellas no perturbara el orden público establecido. Debe tenerse en cuenta que el *ancien régime* había perseguido arbitrariamente a muchos hombres sólo por expresar lo que pensaban sin que existiera ninguna regulación jurídica. Esa actitud autoritaria tuvo sus raíces en la intolerancia religiosa. En repetidas ocasiones la Iglesia persiguió en forma cruel e inhumana a los sospechosos de herejía e imaginó y aplicó refinadas torturas y cruentos castigos en contra de quienes se atrevieron a desafiarla aunque fuera sólo de palabra. De ahí que la Declaración de los Derechos del Hombre haga una referencia específica a que ni siquiera las opiniones religiosas deberían dar lugar a represiones por parte de la autoridad.

Es necesario reflexionar en que la libertad de expresión, entendida en su sentido jurídico, se caracteriza precisamente por ser un fenómeno normativo. En ocasiones se pretende sostener que esa libertad es natural, incuestionable e ilimitada, lo cual puede ser cierto desde un punto de vista estrictamente filosófico y moral, pero desde el punto de vista jurídico lo que quisieron los liberales originales y lo que siguen defendiendo las Constituciones democráticas, no es una consagración en abstracto de la libertad de expresarse, la cual indiscutiblemente es consustancial al hombre, sino una regulación jurídica que impida al Estado imponer sanciones por el solo hecho de expresar ideas, pero también hacer jurídicamente responsable a quien emite su opinión si de ello derivan consecuencias antijurídicas, como los ataques a la moral, a los derechos de tercero, la provocación de un delito o la perturbación del orden público. Así, pues, debe distinguirse entre la libertad de expresión y las consecuencias jurídicas de la misma. El hombre siempre ha sido libre de manifestar sus pensamientos, pero el expresarlos, en distintos momentos de la historia le podía llevar aparejada la imposición de un castigo o el sufrimiento de violencias injustificadas por parte de las autoridades. Lo que establecen las Constituciones modernas es una obligación por parte del Estado de abstenerse de actuar en contra de quien se expresa libremente, salvo que existan condiciones jurídicamente reguladas que justifiquen tal acción.

El liberalismo, por lo tanto, no se refería a la libertad en abstracto, sino a la serie de garantías jurídicas que permitieran que el ejercicio de la libertad de expresión no acarreara los resultados perjudiciales que hasta entonces habían sufrido los individuos, sin protección normativa alguna. Es éste uno de los aspectos básicos que con frecuencia quedan sumidos en la confusión o en la oscuridad cuando se plantea el problema de las libertades del hombre; el iusnaturalismo ha insistido en la existencia de derechos naturales que son consustanciales al individuo. El análisis del iusnaturalismo es fundamentalmente de naturaleza filosófica, pero desde el punto de vista estrictamente jurídico, basado en normas que regulan la conducta humana en

sus manifestaciones exteriores, la sola idea del derecho natural es contradictoria. Si bien al hombre le es dada, por su propia capacidad de pensar, la libertad de expresión, sólo la regulación jurídica de la misma puede determinar los efectos de dicha libertad. De este modo, la ideología liberal planteaba desde sus inicios, no la mera exaltación metafísica de la libertad, sino el marco jurídico en el que ésta podría darse, poniendo límites a la acción del poder público.

Desde la perspectiva del derecho, toda libertad es una posibilidad limitada en función del régimen que regula la vida común. Sólo puede ser materia de regulación jurídica aquella libertad cuya manifestación pueda dar lugar a consecuencias de derecho. Sería absurdo, por ejemplo, pretender regular hechos estrictamente naturales, como sería proclamar la libertad de respirar. El hecho natural, como tal, sólo puede estar sujeto a un régimen de derecho, cuando interfiere con los derechos o libertades de los demás. En ese sentido, la libertad de expresión jurídicamente regulada, se define por el marco dentro del cual puede darse. La preocupación del pensamiento liberal es que sean precisamente normas objetivas, perfectamente señalas en códigos conocidos la comunidad, las que establezcan los límites jurídicos de la mencionada libertad. Queda claro, pues, desde la propia Declaración de los Derechos del Hombre y del Ciudadano, que sólo la ley, en atención a prevenir perturbaciones del orden público, podría limitar el derecho de expresarse libremente.

En la historia constitucional mexicana la primera referencia a esta garantía la encontramos en el Decreto Constitucional para la Libertad de la América Mexicana del 22 de octubre de 1814. Se proclamaba ahí la libertad de hablar, discurrir y manifestar opiniones por medio de la imprenta, siempre que no se atacase el dogma, se turbara la tranquilidad pública o se ofendiera el honor de los ciudadanos.

La Constitución de 1917 prácticamente reprodujo el contenido del artículo 6° de la Constitución de 1857, y el único cambio que se ha introducido en este artículo fue la adición que se le incorporó al decreto publicado el 6 de diciembre de 1977 en el

Diario Oficial de la Federación, Según dicho decreto, al texto original se añadió la expresión "el derecho a la información será garantizado por el Estado".

Con esta modificación podemos encontrar tres distintas garantías en el texto. Una primera es la clásica garantía individual, entendida en el sentido ya explicado según el cual el Estado debe *abstenerse* de inquirir judicial o administrativamente a alguien por la manifestación de sus ideas, salvo que existan razones legalmente establecidas para hacerlo.

La segunda, que inspiró el contenido original de la reforma de 1977, debe entenderse como una garantía social que preserva el derecho de todos los miembros de la sociedad a recibir, información por parte de los medios de comunicación masiva que reúna ciertas cualidades.

La tercera es una interpretación paralela que se desarrolló con los años, respecto del contenido de la expresión *derecho a la información,* y consiste en un derecho de los ciudadanos a requerir del Estado, información de ciertas características respecto a las actividades del mismo, lo cual implica, a diferencia del primer sentido, una obligación de hacer por parte del Estado

La garantía individual de libre expresión. La fórmula corrientemente empleada de *libertad de expresión* aparece en nuestro artículo 6° bajo la siguiente redacción: *La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, ...*" . Esto nos plantea como primer problema el dilucidar qué debe entenderse por "manifestación de las ideas". Puede decirse que es justamente la exteriorización del pensamiento por cualquier medio, con excepción de la Impresión, que está regulada en el artículo 7, y que se conoce como libertad de imprenta.

Si bien es cierto que la expresión verbal es utilizada en medios modernos de comunicación, como la radio y la televisión, éstos deben ser considerados como

técnicas que permiten la divulgación masiva de las ideas, de la misma manera que se hizo durante muchos años por medio de la imprenta. El Constituyente de 1917, al regular la libertad de imprenta en el artículo 7° estaba refiriéndose a una forma específica de manifestación de las ideas potenciada por la tecnología empleada. Por supuesto, no podía prever fenómenos como la radio, la televisión o la transmisión de datos como por ejemplo vía INTERNET, pero es evidente que estas formas de multiplicación de las ideas manifestadas tienen una mayor similitud con la imprenta precisamente por ese carácter expansivo que permite una más amplia divulgación del pensamiento, que la simple expresión individual de las ideas.

Por otra parte, la libertad individual de expresión no se refiere exclusivamente a la manifestación de ideas por medio de la palabra, puede serlo también a través de gestos, de símbolos, o de cualquier otra forma de elaboración de imágenes o sonidos que permitan transmitir una idea.

De esta manera, la libertad de creación artística que abarca obras musicales, pictóricas, esculturales o cualesquiera otras técnicas que permitan la comunicación directa entre el creador y el espectador quedan incluidas en la protección de la garantía individual del artículo 6°, independientemente de que al multiplicarse a través de medios tecnológicos a los que ya nos hemos referido como tecnologías expansivas de la manifestación del pensamiento, puedan pasar a quedar también protegidas por la garantía relativa a la libertad de imprenta.

En cuanto a la palabra "inquisición", está empleada en su acepción gramatical de averiguación o indagación. En consecuencia, la Constitución prohíbe a las autoridades, sean judiciales o administrativas (y debe entenderse que esta prohibición se extiende al Poder Legislativo, pues se pretende proteger al individuo de la acción del Estado en general) iniciar averiguaciones con motivo de la manifestación de ideas. Pero esta manifestación no puede tampoco convertirse en el medio para vulnerar valores colectivos que también están protegidos por la ley. De tal

modo, la libertad de expresión tiene como límites los valores que la propia Constitución señala: la moral, los derechos de tercero, la seguridad de la vida comunitaria que se vería afectada con la comisión de un delito provocado como causa directa de la manifestación de ideas y el orden público.

Ahora bien, la formulación constitucional, como corresponde a las normas de esa índole, es amplia y por lo tanto debe ser desarrollada en preceptos específicos que señalen cuándo el uso de la libertad de expresión sí puede dar lugar a averiguaciones por haber transgredido alguno de los valores protegidos en el propio precepto. Así, por ejemplo, es factible tipificar en el Código Penal delitos como la difamación o la calumnia, que son cometidos por medio de la expresión, pero el legislador al configurar el delito determina las condiciones específicas en que la manifestación de las ideas se convierte en violatoria de la ley.

Si la libertad de expresión careciese absolutamente de límites podría imputarse a otra persona cualquier cosa por dañina que resultara, sin que aquélla pudiese reclamar absolutamente nada.

La Constitución garantiza la libertad de pensamiento y de la difusión del mismo, pero hace también responsable al ser humano libre para que si en uso de esa libertad, violenta la convivencia, la sociedad le pueda exigir cuentas de ello, siempre que la ley especifique las infracciones que pueda cometer.

Igualmente, en la esfera administrativa existen limitaciones que aseguran la adecuada convivencia, y por ello hay faltas de policía y buen gobierno que surgen del uso indebido de la libertad de expresión. Todos podemos convenir en la libertad que cada quien tiene de dar a conocer sus ideas, pero también estaríamos de acuerdo en que si a alguien se le ocurre hacerlo gritando en medio de la representación de una obra teatral, en vez de estar expresándose libremente, estaría alterando el orden público.

En la legislación existen algunos otros supuestos en los que se pone de manifiesto la posible interferencia de la libertad de expresión, con otros valores jurídicos. Pongamos como ejemplo el delito de corrupción de menores, si no existiera limitación jurídica al respecto, podía alegarse que se está haciendo uso de la libertad de expresión al mostrar mediante anuncios impresos o electrónicos actos de exhibicionismo corporal, lascivos o sexuales con uno o más menores de dieciocho años. En virtud de que éstas representan un ataque a los derechos de terceros, es perfectamente válido tipificar las mencionadas conductas como contrarias a la ley.

En cuanto a la provocación de algún delito, es justamente la limitación a la libertad de expresión relativa, la que permite considerar como corresponsable y autor de una conducta ilícita penal a quien incita a otro a cometerla. Pensamos que toda la autoría intelectual en materia penal se haría nugatoria si la llamada libertad de expresión se expandiera sin límites jurídicos; bastaría con alegar que se había hecho uso de dicha libertad para pedir a otro que cometiera un determinado delito y que sólo a quien lo cometió debería exigírsele responsabilidad penal.

1.2. EL DERECHO A LA INFORMACION COMO DERECHO FRENTE A OTROS PODERES SOCIALES

La reforma política realizada en 1977 incluyó la adición en el artículo 6° de la oración: "El derecho a la información será garantizado por el Estado". Esta reforma recogió distintas corrientes preocupadas por asegurar a la sociedad una obtención de información oportuna, objetiva y plural por parte de los grandes medios de comunicación masiva. Se dijo entonces que la libertad de expresión constituía un derecho público subjetivo derivado del liberalismo clásico; en cambio, el *derecho a la información* constituye un derecho público colectivo para cuya garantía el Estado debe garantizar, mediante normas jurídicas, el adecuado funcionamiento de los órganos sociales -ya no estatales- que generan y difunden información, la cual tiene una incidencia importante sobre la sociedad.

La libertad de expresión y el derecho a la información están íntimamente relacionados, pero no pueden confundirse; la libertad de expresión atiende a la necesidad personal que tiene el individuo de expresarse, en tanto que el derecho a la información se refiere a la necesidad que tiene la sociedad de contar con información adecuada. Las distorsiones o manipulaciones intencionadas por parte de quien dispone del poder social de conformar la opinión de millones de personas, según la manera como les presenten los hechos aparentemente objetivos, deben dar lugar a una exigencia de responsabilidad establecida en la ley por parte de la propia sociedad.

A través de la difusión masiva de ideas pueden también producirse ataques a importantes valores comunitarios que deben estar legalmente resguardados. En la sociedad moderna los individuos son ávidos consumidores de información y como tales tienen también el derecho a que la ley salvaguarde sus intereses, como lo hace con los consumidores de bienes o de otros servicios. La adición de 1977, a la que se

alude, derivó de un planteamiento contenido en el plan básico de gobierno aprobado por la VIII Asamblea Nacional Ordinaria del PRI, que en la parte alusiva decía:

"El derecho a la información significa superar la concepción exclusivamente mercantilista de los medios de comunicación; significa: renovar la idea tradicional, que entiende el derecho de información como equivalente a la libertad de expresión: es decir, libertad para el que produce y emite, pero que se reducirá si ignora el derecho que tienen los hombres como receptores de información"[2].

"La existencia de un verdadero derecho a la información enriquece el conocimiento que los ciudadanos requieren para una mejor participación democrática, para un ordenamiento de la conducta individual y colectiva del país conforme a sus aspiraciones" [3].

Así, del programa de un partido, pasó a formar parte del programa fundamental de la nación a partir de la iniciativa enviada por el Ejecutivo que en la parte relativa señalaba: "...el derecho a la información que mediante esta iniciativa se incorpora al artículo 6° ...será básico para el mejoramiento de una conciencia ciudadana y contribuirá a que ésta sea más enterada, vigorosa y analítica, lo cual es esencial para el progreso de nuestra sociedad"[4]. A este respecto durante el debate correspondiente en la Cámara de Diputados se sostuvo que el derecho a la información viene a completar, a continuar y modernizar el texto relativo a la libertad individual de expresión. Esta se establece y se esgrime frente al Estado, para hacer posible la disidencia, el derecho a la información se exige a través del Estado para hacer posible la democracia. Es éste el derecho "a estar informado" y no "a informar" .

La sociedad contemporánea necesita instrumentos legales que fijen los límites de la acción de medios capaces de hacer llegar instantáneamente sus mensajes a

[2] Diario de Debates de la Cámara de Diputados, del 20 octubre de 1977.
[3] Diario de Debates de la Cámara de Diputados, del 6 de octubre de 1977.
[4] *Idem*

cientos de millones de personas. Este enorme potencial es usado por un número mínimo de individuos que determina el contenido de lo que otros muchos millones van a ver u oír. Estos últimos tienen derecho, en una sociedad democrática, de hacer valer su punto de vista respecto de esos mensajes que reciben y que en el fondo son costeados por el dinero que las mismas personas pagan al comprar productos o servicios que financian a tales medios.

La sociedad exige también espacios en dichos medios de comunicación, y este fenómeno debe ser regulado.

La interpretación inicial de la expresión *derecho a la información* fue la siguiente y no otra: crear la base para que por medio de la ley se regulen las relaciones entre la sociedad y los medios de comunicación social. Sin embargo, pese a los muchos años transcurridos no ha sido posible obtener un consenso para que exista dicha normatividad. Los medios de comunicación se han resistido con éxito, alegando que no es posible limitar la libertad de expresión, lo cual es un sofisma por que precisamente, como ya vimos, la libertad de expresión es por su propia naturaleza una libertad regulada.

Por otro lado, la sociedad no ha madurado lo suficiente como para hacer conciencia de sus derechos frente a los medios colectivos de comunicación.

"Ciertamente la información tienen una real importancia económica, ha resultado ser un bien susceptible de verdadero valor patrimonial, sobre todo en la actualidad, en donde la sociedad esta dependiendo de la técnica y el saber, llegando a tener un valor inimaginable, pues independientemente del soporte material, la información es un bien en sí, constitutivo de un producto autónomo, que por su mismo contenido económico, requiere de una tutela jurídica en razón de los efectos jurídicos a que da lugar, ya sea a nivel de una relación de posisión entre autor y objeto (derecho sobre

la información) o a nivel de relación de transferencia entre aquel que la emiten y aquel que la recibe (derecho a la información).

"Desde la primera mitad del siglo XX se han acrecentado de manera geomética el desarrollo tecnológico y social de las estructuras de la información, pues es con la Declaración Universal de los Derechos del Hombre de 1948, en donde apareció el concepto de derecho a la información.

"Este concepto logra nuevos alcances que son los que vienen a sustituir a los anteriores más restringidos (de expresión e imprenta) que resultaban insuficientes, para comprender y dar respuesta a la amplia y compleja actividad informativa.

"El derecho a la información engloba a todas las libertades pero especialmente, da una respuesta integral al proceso informativo, ya que se plantea el acceso y participación de los individuos y los grupos sociales en un fenómeno de interrelación.

"El concepto de derecho a la información comprende un conjunto de tres facultades vinculadas entre sí, como lo son: difundir, investigar y recibir información; todas ellas agrupadas en dos vertientes fundamentales como lo son el deber de informar y el derecho a ser informado.

"Esta parte, que comprende las facultades de difundir e investigar, vendría a ser la fórmula moderna de la libertad de expresión, porque dicha libertad no es suficiente para referir la complejidad del proceso informativo, ni sus mecanismos de protección son suficientes para asegurar en las sociedades modernas la existencia de una comunicación libre y democrática[5]."

Este aspecto del Derecho supone en buena medida el replanteamiento de la regulación de los medios y comunicación y ya no tanto de los medios informativos, en

cuanto que el acceso a los primeros por parte de los grupos sociales más significativos sea limitado sino que inexistente. Supone también el establecimiento de fuentes de información abiertas al público, así como el acceso a los documentos administrativos y bancos de datos de carácter público.

1.3. EL DERECHO A LA INFORMACION FRENTE AL ESTADO

Este segundo aspecto más novedoso se refiere básicamente el derecho de los individuos y grupos sociales a estar informados de los sucesos públicos y, en general, de todas las informaciones que pudieran afectar su existencia; todo ello para lograr que el individuo oriente su acción y participe en la vida política de su comunidad.

Como parte de una estrategia de defensa de los propios medios se trató de desconocer el origen de la adición relativa al derecho, que ya se ha explicado; y se trató de darle un contenido distinto, argumentando que tal derecho a la información era exigible al Estado para que éste informara de sus actividades.

Esta connotación ha tenido también un largo desarrollo doctrinario, y es perfectamente justificada en una sociedad democrática. Viene a constituir una contrapartida del derecho que tiene la sociedad a recibir información suficiente, veraz, objetiva y oportuna. El Estado no puede ni debe actuar en secreto, debe explicar sus acciones tanto a los individuos en lo particular como a los representantes de los medios sociales de comunicación. Para que éstos cumplan adecuadamente con sus obligaciones frente a la sociedad, el Estado debe también proporcionar la información que se le requiera de acuerdo con una normatividad racional y objetiva.

---

[5] TELLEZ VALDES, Julio, Derecho Informático, Editorial McGraw-Hill, Segunda edición, México, 1996, pag. 66.

Dentro de esta racionalidad y objetividad está el hecho entendible de que no toda la información de que disponen los funcionarios del Estado puede ser difundida indiscriminadamente; hay informaciones que tienen que ver con la vida privada de los individuos. Pensemos, por ejemplo, que cualquier persona tuviera acceso a los registros fiscales o judiciales en donde se ventilan diferencias privadas. De tal información dispone el Estado, pero no debe disponer de ella para publicarla.

Igualmente, hay informaciones que deben permanecer reservadas por afectar a la seguridad nacional o la seguridad individual, como pueden ser en este último caso las averiguaciones de carácter penal. También debe regularse el uso que un funcionario puede dar a información a la que tiene acceso con motivo de sus tareas.

Con motivo de las discusiones sobre los acontecimientos de Tlatelolco en 1968 y la negativa del Estado a abrir sus archivos hasta que transcurriesen 30 años de los acontecimientos, sin que existiese una base legal sólida al respecto, se volvió a replantear la necesidad de regular esta versión del *derecho a la información* a fin de que el Estado asuma compromisos específicos en cuanto a la divulgación de las informaciones que posee. La sociedad requiere reglas claras en lo que toca a las responsabilidades de quienes dirigen los grandes medios de comunicación, a fin de que su actividad sea transparente y objetiva, sin privilegios, manipulaciones o deficiencias profesionales que desvirtúen el contenido de las informaciones. Como contrapartida, el propio Estado debe ceñirse a reglas en el manejo de su información. Qué es lo que se puede difundir y qué no así como las razones legalmente establecidas para ello y cuánto tiempo puede reservarse la información en archivos cuando tenga que ver con asuntos de seguridad y todos, los particulares, los responsables del manejo de medios y los funcionarios responder por las infracciones legales en que incurran.

Algunos autores consideran esta vertiente como la parte pasiva del derecho a la información; sin embargo, cabe considerar que precisamente el sentido del derecho a ser informado implica, desde el punto de vista de receptor, un abandono de esa actitud pasiva al tener la posibilidad jurídica de exigir al sujeto obligado o la cumplimentación del mencionado derecho.

En esta tesitura, es conveniente señalar que no es de nuestro interés ahondar en el estudio de esta perspectiva del derecho a la Información frente al Estado, sino que básicamente frente a los medios masivos de comunicación, ya que es ahí, donde se analizará los nuevos alcances de la libertad de expresión y de información.

CAPITULO II
LA INTERNET COMO PRINCIPAL RED DE INFORMACION

2.1. GENERALIDADES DE LA INFORMACION

Para el objetivo de esta tesis considero importante exponer lo que se entiende por información (del latín *in-formare*, poner en forma), "se trata de una noción abstracta, no obstante que posee una connotación vinculada a una de nuestra más grandes libertades, la de opinión y expresión de informaciones e ideas por cualquier medio que sea"[6]; de aquí que la información se haya considerado como "un elemento susceptible de ser transmitido por un signo o combinación de signos"[7] o como un "proceso fisico-mecánico de transmisión de datos, teniendo como dato al elemento referencial acerca de un hecho. En cibernética, es el factor cualitativo que designa la posición de un sistema, y que eventualmente es transmitido por este sistema a otro"[8]. En sentido general un conjunto de datos constituye una información.

Cualitativamente se ha concebido a la información como "el contenido de lo que es objeto de intercambio entre el sujeto y el mundo externo",[9] presentándose un conjunto de datos como elemento de las relaciones del hombre y tendientes a una ordenación.

"Son características de la Información en cualquier proceso en que intervenga[10]:

[6] Ver el articulo 19 de la Declaración Universal de los Derechos Humanos del Hombre de 1948.
[7] Diccionario Roberts, Paris, CD, 1979.
[8] Diccionario Enciclopédico Larousse. CD, México, 2003.
[9] TELLEZ VALDEZ, Julio, *Ob cit, apud* Wiener Norbert, Cibernética, p.62.
[10] TELLEZ VALDEZ, Julio, *Ob cit*, p. 61.

a) Clara e inteligible. Es decir, que su contenido y vehículo de significación debe estar dentro de las normas y lógica de comunicación que se acuerden individual o sociológicamente.

b) *Relevante.* Es decir, que debe revestir un carácter efectivo en el proceso de decisión en el que intervenga.

c) *Completa.* Esto es, que cubra el mayor rango de posibilidades existentes en el momento en que se le requiera.

d) *Oportuna.* Que intervenga y se pondere en el momento en que sea menester.

e) *Confiable.* Cuando cumpla satisfactoriamente con los elementos anteriormente enunciados.

"En general, la información circula para responder a necesidades diversas como son las de saber, conocer y elegir, la cual fluye por los mismos canales de distribución; los medios de comunicación, como lo son diarios, radio, televisión, Internet, etcétera, Ahora bien, además de la información general que responda a las necesidades de un amplio público, también encontramos aquélla que es más especializada y sectorizada, que satisface necesidades fundamentalmente documentarias, y cuyo manejo es objeto de incursión ya no tanto de los medios de comunicación sino de los medios informáticos.

"De esta forma, a través de dichos medios, se está permitiendo, mediante la integración y disponibilidad de numerosos bancos de información, la consecución de uno de los cometidos principales de la informática como lo es la adecuada toma de decisiones.

"En estos términos, informática y la información están vinculadas de manera estrecha por el empleo de las computadoras en el proceso propio de nuestra vida cotidiana, con implicaciones aún más trascendentes de las estrictamente técnicas."

2.2. LOS DIFERENTES FLUJOS DE INFORMACION

El Flujo de Datos Trasnfronterizos de acuerdo con el Consejo Económico de la Organización de las Naciones Unidas, es "la circulación de datos e información a través de las fronteras nacionales para procesamiento, almacenamiento y recuperación".[11]

"Dependiendo del tipo de datos o información que fluyan a través de los diferentes medios, tenemos a:[12]

"a) *La Información comercial,* la se manifiesta según una lógica mercantil de distribución (one-way) aun si los usos comerciales no están consolidados del todo en este aspecto. De esta forma distinguimos al flujo de prensa general y especializada; servicios documentarios y bancos de datos, sean de carácter bancario, financiero, industrial, bursátil, etcétera; comercio de audiovisuales (discos, casetes, películas, programas de televisión); comercio de programas de cómputo y tecnologías, etcétera.

"b) *La información empresarial,* como aquélla sustentada en rasgos distintivos tales como pedidos, existencias, control de producción, consolidación financiera, gestión del personal, etcétera en un cuadro puramente privado en el seno de consorcios empresariales con notorias repercusiones a nivel de dirección, decisión, administración y operación de las mismas.

"c) *La Información especial,* como aquella que aunque no necesariamente está vinculada a intereses comerciales o empresariales se convierte en intercambio de conocimientos que permiten una mejor desarrollo de las actividades educativas o de investigación a nivel técnico o científico.

---

[11] Ver recomendaciones del 23 de septiembre de 1980 en el punto relativo a las definiciones.
[12] TELLEZ VALDEZ, Julio, *Ob cit,* p. 80.

"Las redes por las que pueden circular dichas informaciones suelen ser muy variadas, y esto depende del tipo de datos que fluyan en ellas, caracterizadas en su mayoría por innegable importancia tal como es el caso, por mencionar sólo algunas[13]:

- La Red Europea de transmisiones (EURONET), que permite la conexión de bancos de información en Europa Occidental;

- La red de la sociedad internacional de telecomunicaciones Aeronáuticas (SITA), que permite el control de las telerreservaciones aéreas a nivel mundial;

- La Red Bancaria de Intercambio de Mensajes Financieros (SWIFT), que permite la comunicación a nivel mundial entre las instituciones bancarias y financieras;

- La Red de Policía Internacional (NICS), que permite el intercambio de información sobre los criminales que persiguen la INTERPOL,

- La Red Libre –INTERNET-, que caracteriza por por ser:

a) Global. Proporciona un acceso inmediato a la información procedente de cualquier parte del mundo, sin límites geográficos;
b) Descentralizada. Es un sistema descentralizado, que trabaja sin vigilancia y que crea múltiples puntos de acceso;
c) Abierta. Tiene escasas barreras de acceso siendo la creación y difusión de información extremadamente bajos);
d) Grande. Tiene una capacidad ilimitada de almacenamiento de información;
e) Interactiva. Permite comunicaciones de uno a uno, de uno a muchos y de muchos a uno;

f) Controlada por el usuario. Puede controlar que información que llega a su ordenador;

g) Independiente de la infraestructura. No está ligada a ninguna infraestructura, aparte del sistema telefónico.

Dadas las características del INTERNET, el navegar en ella, ha traído grandes ventajas como el poder comunicarse inmediatamente y/o intercambiar información y opinión sobre temas de mutuo interés sin límites de frontera. Ha resultado ser la red más utilizada en el mundo, y es por ello el motivo de nuestro interés a nuestro actual propósito, y que sobre ésta Red, es que versará el estudio de esta tesis.

2.3. ORIGEN DE LA INTERNET

A fin de tener una visión más amplia sobre el INTERNET es conveniente conocer su origen.

En los comienzos de los años 60's se desarrollaron las primeras redes de conmutación de paquetes. En este tipo de redes la información que se envía se subdivide en pequeños paquetes que son dirigidos hacia el receptor (a veces por diversos caminos) una vez allí, todas las partes se unen en el orden correcto para recuperar la información original. Con esta Tecnología se aseguraba que varios usuarios podrían mandar mensajes por las mismas líneas de comunicación; y lo que es más importante, no se establecería ninguna dependencia de un determinado anfitrión (host) central. Por este motivo, no era necesario el desembolso de grandes cantidades de dinero para formar redes de computadoras.

---

[13] *Idem*

Sin embargo, la primera experiencia a gran escala nació a paso militar, en el año 1969, varios científicos del Departamento de Defensa de Estados Unidos crearon una pequeña red de computadoras que permitía transferir informaciones secretas. Aquel invento rudimentario se llamó ARPANET (Advanced Rearch Agency Netword - Red de la Agencia para Proyectos de Investigación Avanzada). Evidentemente, esta red era absolutamente privada, y nadie podía acceder a ella libremente, su progresivo crecimiento convenció a la comunidad informática de que pronto podrían encadenarse todas las computadoras del planeta.

Este proyecto fue diseñado con la finalidad de comunicar todos los centros militares para que sobrevivieran a un posible ataque nuclear. De este modo fueron instalados diferentes nodos por multitud de centros de investigación y contratistas militares; el primero fue en la UCLA el 1o. de Septiembre de 1969, a la UCLA le siguieron universidades como la Stanford, Utah, etc.; fue hasta 1972 cuando se comenzó a considerar a INERNET como una red de redes. En octubre de ese año se realizó una demostración pública a investigadores de otros países y fue un gran éxito; entonces se formó el INWG (Internetwordking Working Group - Grupo de Trabajo en Redes) como foro de discusión para crear las bases de una gran red mundial: INTERNET en 1983.

Durante los años 70's y principios de los 80's, la tecnología utilizada en ARPANET se fue haciendo pública progresivamente, y muchos organismos de otros países comenzaron a desarrollar sus propias redes de comunicaciones.

En 1991 aparece la Commercial Internet Exchange Association, Inc., una asociación de organismos y empresas que se hizo cargo de la administración de lo que fue ARPANET. En 1992 apareció la Internet Society, que es el organismo que rige hoy en día la red de redes.

En ese mismo año, el Centro Europeo de Investigación Nuclear (CERN), una de las instituciones que más ha trabajado para que INTERNET sea como es hoy, puso en marcha la World Wide Web (WWW). Este fue el paso que dio pie al gran *boom* de INTERNET, apoyado por todo tipo de empresas e instituciones que empezaron a ver claro un nuevo horizonte. Así, la red que hasta entonces había tenido un contenido casi estrictamente didáctico y científico, comenzó a comercializarse, y a convertirse en un medio universal de divulgación de información.

A principios de los 80's, la red ARPANET se dividió en dos vertientes, la propia ARPANET y MILNET; esta última una red que se integró en la Red de Datos de Defensa de Estados Unidos. Los administradores de ARPANET procuraron desde entonces que la red continuara siendo privada, creando accesos restringidos y permitiendo algunos *gateways* o pasarelas a otras redes (como por ejemplo, CSNet) por su interés científico o tecnológico. Una de las redes que se utilizó como apoyo para ARAPANET, y que en definitiva acabaría por ser la columna vertebral de Internet, fue NSFNET, la red de la National Science Foundation, así ARPANET terminó como backbone que unía redes más pequeñas y centros de computación de la NFS, sin embargo, en 1990 ARPANET dejó de existir como tal.

Durante la década de 1983 a 1993, INTERNET pasó de un proyecto de investigación pequeño y experimental a ser la red de computación más grande del Mundo.

El sistema empleado se popularizó rápidamente, dadas las ventajas que ofrecía con respecto a otros protocolos y otras redes de computadoras del momento, y nuevas instalaciones y compañías pidieron acceder a INTERNET para explotar sus posibilidades de comunicación mientras que otros organismos constituían sus propias redes apoyándose en las bases de construcción de INTERNET. En estos años el número de redes creció considerablemente.

Los gestores de INTERNET se dieron cuenta de que su red ya no se utilizaba solo para intercambio de información sobre investigación, sino que los usuarios la estaban usando para enviar mensajes personales o de ocio, hasta para crear lazos comerciales con las compañías "semipúblicas" adscritas a la red. Esto obligó, por un lado a la mejora de protocolos y conexiones físicas, ya que al existir un alto número de usuarios personales o empresariales, se generaba una gran cantidad de tráfico de información, y por otro lado se empezó a controlar el tipo de usuarios a los que se permitía el acceso a la red, prohibiendo el uso comercial de ésta, en un intento de volver a los objetivos iniciales de utilizarla sólo para el desarrollo y la investigación.

Hace algunos años INTERNET quitó dicha restricción, debido en gran parte al apoyo y al interés del entonces presidente de Estados Unidos, Bill Clinton, que vió en la red el medio perfecto para dar un paso adelante en las Telecomunicaciones y acercarlas al ciudadano, siguiendo su política progresista.

El ritmo de crecimiento al iniciar 1990 fue realmente sorprendente. Durante 1993 tenía un crecimiento del 20% mensual, así INTENET ha dejado sus orígenes en bases militares e instituciones gubernamentales para establecerse en escuelas, universidades, centros de investigación, bibliotecas públicas e incluso los sectores comercial e industrial.

En 1996 se determinó el protocolo para una Red global, el INTERNET. El imparable auge que ha vivido y está viviendo Intenet ha superado, sin duda, cualquier expectativa prevista. Ahora el Internet es el Red más grande imaginable y no conocemos ya su importancia en el futuro cercano.[14]

A la fecha INTERNET tiene más de 30 millones de usuarios, cifra que se estima se duplicara en el próximo año. Lo que equivale a que cada segundo y fracción de un nuevo usuario, en algún país del mundo hace su primera conexión a INTERNET.

El idioma oficial de INTERNET es el inglés, por lo que la mayor parte de la documentación de la red está en este idioma. Pero en cada país se suele utilizar el idioma propio, empleando el inglés sólo para las áreas internacionales y los documentos o textos que van a ser leídos por usuarios de otros países.

La red de INTERNET está formada por sus usuarios para servir a sus propios usuarios, y estos son los que bajo su propio criterio controlan la red. Esto se puede conseguir gracias a la propia estructura de la red, la cual permite que cada empresa o asociación controle su parte de la red (Red Interna), y la gestiona de la manera más conveniente para su interior, no afectando para nada al resto de la red. De todas maneras es mucho más fácil para su entendimiento, ver a INTERNET como la entidad física que engloba a todas las redes que la componen.

Es importante distinguir que se le conoce como Intranet a aquellas redes que aprovechan el uso de la red Internet para fines privados. La gran diferencia entre Internet e intranet es simplemente la forma de utilizar la red de redes. Internet es para todo público, mientras que intranet es sólo para los usuarios autorizados.

Los usuarios de la red Internet tienen acceso a la información almacenada en múltiples servidores conectados entre sí, mientras que los usuarios de intranet sólo tienen acceso a aquella información a la cual están previamente autorizados. La clave del intranet está en que todo el que desee tener acceso a la información de un servidor determinado tiene que tener la clave de acceso a él. De lo contrario, el acceso a dicha información le será denegado.

---

[14] Ver www.infoperu.com. 21 de febrero de 2003.

INTRANET es una red de servidores que utilizan los servicios de Internet para intercomunicar empleados, pero limitando el acceso a los datos privados de la empresa sólo al personal autorizado.

En el caso de redes privadas que utilizan la tecnología internet para el intercambio de información pero que no están conectadas a la red Internet, también se dice que forman un intranet particular. Sin embargo, el auténtico intranet hace siempre uso de la red pública conocida como Internet.

En INTERNET podemos encontrar dos tipos de información: Los públicos y los privados: La información pública es la que más abunda actualmente, y es accesible por cualquier usuario. Engloba todo tipo de utilidades, juegos, programas freeware y shareware, además de una buena parte de información personal que muchas empresas proporcionan como apoyo técnico a sus productos o simplemente propaganda.

La información privada está tomando auge en los últimos años, debido a la cantidad de empresas privadas que se están incorporando a la red gracias a la comercialización que a sufrido esta últimamente. Este tipo de empresas tienen una parte de su red en forma privada, a la que sólo se le permite el acceso a sus propios usuarios, y donde se guarda la información propia de la empresa, y otra parte pública a la que permite acceder desde el exterior.

Dentro de INTERNET, como en cualquier tipo de red, las diferentes computadoras hosts como más comúnmente se les conoce, tienen asignada una dirección única que permite de esta forma designarlos al enviar correo, acceder a diferentes servicios y que los distingue de los demás, esta dirección es conocida como IP. Los Network Information Centers o NIC son los encargados de asignar los números de red o rango de direcciones apropiadas para cada organización que se integre a INTERNET.

INTERNET está experimentando un auge en el uso comercial y es esta tendencia la que ha hecho que INTERNET se expanda más. Los conceptos básicos bajo los cuales INTERNET fue fundada han sido la explicación para su habilidad de crecimiento y el manejo de más y más computadoras y usuarios.

Así pues con las mezcla de la informática y las telecomunicaciones surge el vocablo teleinformática o telemática, iniciado su robustecimiento a partir de la de década de los sesenta, como se ha venido señalando.

2.4. VENTAJAS DE LA INTERNET

Entre las bondades más generales del INTERNET se deben señalar el facilitar y fomentar el soporte técnico de la evolución de INTERNET como una infraestructura para la investigación y la educación; estimular la atención de la comunidad científica, la industria y las autoridades gubernamentales, así como educar a la comunidad científica, la industria y al público en general en lo concerniente a la tecnología, usos y aplicaciones de INTERNET; al igual que promover aplicaciones educativas dentro de INTERNET, tecnología para todo el mundo; y promover un foro para explotar las nuevas aplicaciones de INTERNET y estimular la colaboración entre organizaciones.

El Flujo de Datos Transfronterizos aporta múltiples beneficios tanto a nivel nacional como internacional, por lo que de acuerdo con lo que señala el Dr. Julio Téllez Valdés podemos mencionar[15]:

a) El favorecimiento de la paz y la democracia, en virtud de los vínculos estrechos existentes entre la libertad de circulación de información, derechos del hombre y valores fundamentales de la humanidad.[16]

La libre comunicación de mensajes y de opiniones, así como la libertad de expresión son esenciales para fomentar la democracia y la paz internacional, a través del mínimo de confianza que trae consigo el intercambio de hombres e ideas.

b) El Favorecimiento en el progreso técnico y crecimiento, en virtud a la cooperación entre científicos y la competencia de industriales y empresarios que han difundido los conocimientos y técnicas.

c) La interdependencia económica de las naciones, en virtud de la internacionalización de compañías y la especialización de actividades nacionales.

En el caso de Internet, el hecho de intercomunicar miles de computadoras a través de servidores no tendría sentido si no fuese por la posibilidad de accesar la información almacenada en cada uno de los servidores. Lo interesante consiste entonces en ubicar en los servidores todos aquellos datos de interés. Los usuarios han de poder localizar la información que en un momento dado almacenan en los servidores las personas que desean dar a conocer ciertos datos.

En los servidores de internet se almacena mucha información y se consultan muchos datos, pero puede decirse que los sistemas de mayor uso para este intercambio de información son los siguientes:

1. El WEB (la telaraña mundial) que opera esencialmente con exploradores y que permite la consulta de información en caso de que se desconozca la ubicación específica los datos deseados. La operación del WEB está basada en el uso de buscadores o localizadores de información que operan por medio de índices públicos.

---

[15] TELLEZ VALDEZ, Julio, *Ob cit*, p. 78.
[16] Ver Acta final de la Conferencia de Helsinki sobre Cooperación en los Ambitos Humanitarios. 2ª. Parte, *Problemas políticos y sociales*, núm. 324, noviembre de 1977. La Documentation Francaise.

2. La tranferencia de archivos como herramienta del Internet que permite al usuario copiar o transferir archivos de texto, gráficos, sonidos o animaciones desde el disco duro de un ordenador a otro.

3. El correo electrónico, es la ayuda dentro de Internet que permite el envío de mensajes electrónicos de un usuario a otro. Permite el envío de información (datos) a determinados servidores en los cuales otros usuarios han de encontrarlos. En este caso el almacenamiento de la información suele hacerse en un área de acceso exclusivo conocida como buzón del destinatario. Sólo dicho destinatario puede tener acceso a la información.

La ventaja principal del servicio de correo electrónico a través del Internet es el hecho de que el destinatario no necesita estar conectado a la red en el momento en el que le es enviado un mensaje.

Otra ventaja muy importante es la relativa a la confirmación de recepción, o sea, al hecho de que sea recibido automáticamente un mensaje en el momento en que el destinatario de uno de sus mensajes lo haya accesado (o sea, que haya entrado a su buzón y lo haya leído).

4. Las Listas de Distribución (*mailing lists*), son la aplicación de Internet idónea para enviar información relativa a un tema específico a una pluralidad de usuarios.

5. Los grupos de noticias o *newsgroups* son grupos de discusión en los que participan usuarios interesados en un mismo tema, sin embargo, a diferencia de lo que ocurre con las listas de distribución, los mensajes se envían a tablones de anuncios electrónicos (*Bulletin Boards*) que pueden ser consultados por cualquier usuario.

6. Las pláticas entre usuarios, las cuales se basan en el concepto de correo electrónico pero con un buzón compartido en un momento dado por un grupo de personas. La información enviada o recibida a dicho buzón es accesada en un mismo instante por todos los usuarios incorporados a la plática, y sólo es almacenada durante la duración de la plática.

7. Los exploradores de internet, los cuales permiten buscar en un gran número de servidores (desde uno hasta miles) un dato específico en base a un dominio predefinido. Por lo regular, los exploradores operan con direcciones de los archivos donde están almacenados los datos deseados.

En los próximos apartados se expondrán cada uno de estos sistemas de mayor uso para este intercambio de información que han muestrado grandes ventajas para los usuarios del Internet.

2.4.1 INTERNET Y LA TELARAÑA MUNDIAL. WORLD WIDE WEB (WWW)

En 1989 un ingeniero británico llamado Tim Berners-Lee presentó en el CERN (Laboratorio Europeo de Física de Partículas) una nueva forma de transferir la información en la redes digitales llamadas "hipertexto", que consistía en enlazar unos documentos con otros a partir de unas palabras clave o "hipervículos". A través de esta herramienta se podrían visitar los sitios web (websites) para consultar sus documentos o "páginas web". Estos documentos o páginas se encuentran alojados en millones de ordenadores repartidos por todo el planeta y suelen contener texto, aunque cada vez más ofrecen imágenes, animaciones o sonidos.[17]

Pues hasta hace poco, la comunicación entre ordenadores estaba limitada a los sistemas sólo texto, y a pantallas de terminal muy poco atractivas. Los ordenadores enviaban y recibían cadenas de texto y, como mucho, podían aderezar las letras y los números resultantes con algún que otro color de fondo.

La WWW es capaz de transmitir no sólo la información, sino también un entorno gráfico asequible a cualquier usuario que facilita la consulta de los datos ofrecidos. La WWW no es en realidad una red, sino un conjunto de programas y convenciones que facilitan el tránsito por las redes que funcionan como Internet.

A través de las palabras clave o "hipervínculos" el usuario puede ir saltando de una página web a otra para buscar datos, programas o archivos. El "hipertexto" es la herramienta más sencilla con la que los usuarios obtienen información en Internet.

Cuando se visualiza un documento WWW, el texto que aparece en la pantalla contiene palabras en otro color y subrayadas para resaltar las palabras clave. Estas palabras están asociadas a otro documento de la red a través de un URL (Uniform Resource Locator). Este URL es el nombre único e irrepetible de ese documento, y está formado por el nombre del servidor en que se encuentra, el directorio en el servidor y el nombre del documento en sí.

El usuario que recibe un documento WWW debe utilizar un programa cliente llamado navegador o explorador. Este programa es capaz de leer las etiquetas que contienen los documentos, y convertir esa información en formato gráfico.

[17] MARIN PEIDRO, Lucia, *Los Contenidos Ilícitos y Nocivos en Internet*, retavisión, Madrid, 2000, p. 45.

Esa información la podrán "bajar" o "descargar" de la Red, reproducir, imprimir o volver a enviarla a otra persona. y es que Internet, como ya se señaló, es un medio interactivo en el que cada usuario es a la vez emisor y receptor de la información. Cualquier persona puede crear su página web y ponerla a disposición del resto de los internautas. La información vertida en las páginas web es tan variada como los sujetos que la ofrecen.

En la actualidad, el número de sitios web se cuenta por millones y su crecimiento sigue siendo espectacular. Así, es posible encontrar artículos sobre medicina, música, arte, mapas y atlas de todos los países y ciudades del mundo, tiendas virtuales donde comprar desde bicicletas hasta programas de software, música o libros, información acerca de los organismos públicos regionales, nacionales o internacionales y así hasta el infinito.

Por otra parte, para mantener el orden en la red, es necesario que cada ordenador esté correctamente identificado. En general, cada país tiene un dominio principal definido (el de España es "es"), pero además hay varios dominios principales ya definidos para Internet (org - organizaciones y asociaciones; net - recursos de red; gov - gobiernos; com - empresas comerciales, etc.).

2.4.2. LA TRANSFERENCIA DE ARCHIVOS (FTP)

La transferencia de archivos es una herramienta de Internet que permite al usuario copiar o transferir archivos de texto, gráficos, sonidos o animaciones desde el disco duro de un ordenador a otro.

A diferencia de lo que ocurre con la conexión remota, el ordenador que proporciona la información (llamado servidor FTP) no le exige al usuario disponer de una cuenta - clave de acceso- en la máquina a la que desea acceder. El lenguaje con el que se comunican las máquinas recibe el nombre de Protocolo de Transferencia de Archivos (FTP).[18]

Crear un usuario FTP es la forma más cómoda de permitir a los otros usuarios que accedan a la información contenida en los archivos del servidor FTP sin necesidad de que el administrador del sistema tenga que crear una nueva cuenta para cada persona que intente acceder a la información. El usuario de FTP podrá así descargar los archivos, copiarlos, guardarlos, reenviarlos, pero no podrá modificarlos ni crear otros nuevos. La gran mayoría de los ficheros que se encuentran en la Red proporcionan información útil al navegante de Internet.

2.4.3. EL CORREO ELECTRONICO (e-mail)

A finales de los años 60, el correo electrónico era utilizado por los investigadores americanos para intercambiar entre ellos los resultados de sus trabajos. En la actualidad, el correo electrónico constituye, junto con la navegación en la *World Wide Web*, la aplicación de Internet más utilizada por los usuarios y genera un descomunal trasiego de información.[19]

En muchos aspectos, el correo electrónico es muy similar al correo postal. Tanto el remitente del mensaje como el destinatario tienen una dirección electrónica única (por ejemplo: acarbajalv@mail.scjn.gob.mx). De este modo, cualquier usuario de Internet puede enviar un mensaje a otro usuario de Internet.

[18] MARIN PEIDRO, Lucía, *Ob cit.* p. 46.
[19] MARIN PEIDRO, Lucía, *Ob cit.* p. 47.

Para ello sólo necesita conocer la dirección electrónica del destinatario y disponer de un programa de gestión de correo electrónico. Este tipo de mensajes presenta grandes ventajas respecto del correo postal tradicional, y no sólo por la rapidez con la que se reciben los mensajes (una destinataria situada en Córdoba, Argentina, tarda lo mismo en recibir el mensaje que la compañera de trabajo situada en el despacho contiguo al nuestro), sino también porque es posible adjuntar al texto archivos de sonido, imágenes o gráficos.

2.4.4. LAS LISTAS DE DISTRIBUCION (*mailing lists*)

Las listas de distribución son la aplicación de Internet idónea para enviar información relativa a un tema específico a una pluralidad de usuarios. Se trata de una herramienta que permite el envío masivo de mensajes a suscriptores de todo el mundo acerca de un tema específico. La pregunta enviada por cualquiera de los suscriptores será recibida por los otros usuarios en su buzón de correo electrónico que podrán contestarla o simplemente leerla para estar informados del tema que se debate.[20]

Las listas de distribución pueden ser abiertas, lo que supone que en ellas puede participar cualquier usuario del mundo; o pueden ser cerradas, en cuyo caso quedan restringidas a una determinada categoría de suscriptores; por ejemplo, los alumnos de un curso específico, las listas de distribución de abogados o de médicos.

En muchos casos, las listas de distribución están coordinadas por un usuario -el moderador- que se ocupa de hacer cumplir las normas de conducta de la lista recordando a los suscriptores los objetivos con los que fue creada y expulsando a aquellos suscriptores que utilicen la lista con fines distintos.

En las listas "moderadas" apenas se plantean problemas de contenidos ilícitos en la medida en que los mensajes enviados pasan primero por el moderador que decide si reenvía el mensaje al resto de los suscriptores. En los casos en los que no existe un moderador de la lista de distribución, son los propios suscriptores de la lista los que se encargan de hacer cumplir las "políticas de uso aceptable" o las normas de etiqueta la llamada *Nettiquette*- expulsando o denunciando a los suscriptores que hacen un mal uso de la lista de discusión.

2.4.5. LOS GRUPOS DE NOTICIAS (*newsgroups*)

Cuando el número de participantes en las listas de distribución es muy amplio, resulta poco práctico enviar un mensaje de correo electrónico a cada uno de los suscriptores. Los grupos de noticias o *newsgroups* son grupos de discusión en los que participan usuarios interesados en un mismo tema, sin embargo, a diferencia de lo que ocurre con las listas de distribución, los mensajes se envían a tablones de anuncios electrónicos (*Bulletin Boards*) que pueden ser consultados por cualquier usuario.[21]

Los tablones de anuncios se albergan en proveedores de servicios que se conectan entre sí formando la llamada *Usenet* que, en la actualidad, se encuentra integrada en Internet -la Red de redes-, existen miles de grupos de noticias y su cifra cambia día a día con la llegada de nuevos grupos y la desaparición de otros.

[20] MARIN PEIDRO, Lucía, *Ob cit.* p. 48.
[21] MARIN PEIDRO, Lucía, *Ob cit.* p. 49.

Los temas son tan variados como la imaginación de sus creadores y van desde los que comparten conocimientos sobre la música, el arte, astronomía o temas jurídicos, pasando por los que exponen sus fantasías sexuales, los que discuten acaloradamente acerca del color de los champiñones o los que publican poesías hasta los que comparten sus experiencias paranormales.

2.4.6. LAS CONVERSACIONES EN TIEMPO REAL (Chat)

Otra de las posibilidades que ofrece Internet para que los usuarios se comuniquen entre ellos son las conversaciones en tiempo real o *chat* mediante programas de ordenador como IRC o ICQ. El internauta necesita conectarse con un servidor de *chat* (ofrecido por el propio programa de ordenador) y, una vez conectado, puede elegir el canal en el que quiere participar (eso, si se trata del programa IRC) o bien buscar grupos que compartan los mismos intereses (con el programa ICQ). A continuación, se registra con un seudónimo y comienza la conversación.[22]

2.4.7 LAS HERRAMIENTAS DE BUSQUEDA DE LA INFORMACION (Search Engines)

De poco serviría toda la información que ofrece la Red si no fuera posible acceder a ella. Para evitar que el usuario se pierda entre millones y millones de páginas web, se han creado las herramientas de búsqueda de información.[23]

[22] MARIN PEIDRO, Lucia, *Ob cit.* p. 51.
[23] *Ídem*

Los primeros motores de búsqueda como ARCHIE, WAIS o GOPHER han ido dejando paso a los más modernos, los llamados Buscadores Web. Son directorios que permiten la búsqueda de sitios web a partir de temas genéricos (por ejemplo: Música, Programas de Ordenador, Educación, Medicina, etc.), lo que hacen buscadores tan conocidos como Olé, Yahooo Google o la búsqueda por palabras clave en una base de daros indexada (los documentos web aparecen ordenados en función del número de veces que aparece la palabra clave, como hace, por ejemplo, el buscador Hotbot).

Así pues, en internet es posible conseguir cualquier información que necesitemos. La inmensa cantidad de datos que transitan por la "superautopista de la información", se ha convertido en un motivo de satisfacción para muchos de los usuarios, ya que ven abrirse nuevas oportunidades de negocio, de empleo o el acceso ilimitado a todo saber humano.

CAPITULO III

EFECTOS DEL CONTENIDO ILICITOY NOCIVO EN EL INTERNET

3.1. GENERALIDADES DE LOS CONTENIDOS ILICITOS Y NOCIVOS

Paralelamente al sinnúmero de implicaciones positivas que han traído consigo el desarrollo acentuado de los flujos internacionales de información también han surgido riesgos de entre los que se podrían distinguir los siguientes[24]:

"1.- La vulnerabilidad social. Con una irrupción de los flujos, la alteración de archivos y programas con motivo de una técnica, catástrofe natural o intervención humana (sabotaje, terrorismo, crisis política, etc.).

"2.- Amenaza a la identidad cultural provocada por la cada vez mas frecuente apertura mundial, de lo cual resulta la transformación de las culturas nacionales respecto a aquello que ofrecen las culturas importadas. Un verdadero problema que reside en las posiciones dominantes y prácticas de los fenómenos de transcultación a través de las llamadas "industrias de la CULTURA" como lo son el cine, radio, televisión, prensa, publicaciones, etc; ahora acompañados por los bancos de datos y edición puestos a la disposición a través de las redes teleinformáticas o "autopistas de la información".

"3.- Dependencia tecnológica exagerada. La evolución de firmas multinacionales ha producido una especialización de producciones y mundialización de mercados, teniendo a la tecnología y, más específicamente, a la informática y las telecomunicaciones como sus máximas manifestaciones, creando y, sólo por momentos, satisfaciendo una serie de necesidades de los Estados en desarrollo,

[24] TELLEZ VALDEZ, Julio, *Ob cit*, p. 79.

fragmentando a sus territorios en actividades planificadas a niveles de resolución supranacionales.

"4.- Incidencias económicas notorias. El desarrollo y pérdida de nuevas tecnologías de la información traen consigo una gran cantidad de inversiones económicas, con notorias desproporciones a nivel de los verdaderamente beneficiados y aquellos que de manera ingenua consideran estar en este cuadro. Sin lugar a dudas esta industria de la información está destinada a ser la más predominante dentro de la escala económica mundial, sin que por el momento se vislumbre una corriente al respecto.

"Sin embargo, el interés de esta tesis es subrayar que a pesar de las muchas ventajas y beneficios que representa el Internet para una gran cantidad de usuarios, también es verdad, que cierta parte de la información contenida en Internet es una fuente de preocupación para algunos otros usuarios, para los gobiernos y para las propias empresas del sector"[25].

Los usuarios, haciendo hincapié de padres y educadores entre otros, están preocupados por la posibilidad de que los menores y otros colectivos merecedores de una especial protección accedan a informaciones inadecuadas en la Red. Los padres temen que sus hijos se encuentren con pornografía, violencia o racismo. Los educadores se muestran reticentes por el posible uso no académico que puedan hacer sus alumnos de ella.

Los gobiernos tropiezan con inquietantes obstáculos en la lucha contra las informaciones ilícitas y nocivas. No es fácil localizar al autor de los contenidos perniciosos puesto que se ampara en el anonimato que brinda la Red.

[25] MARIN PEIDRO, Lucía, *Ob cit.* p. 22.

Las empresas que ofrecen sus servicios a través de Internet y contribuyen a la difusión de la información también comparten estas preocupaciones, ya que como consecuencia de las dificultades mencionadas podrían ser considerados responsables y verse así perjudicada su actividad comercial y por tanto, el despegue del comercio electrónico.

Estas inquietudes tienen su origen en los contenidos que circulan en Internet como consecuencia de un uso ilegítimo o abusivo. Ciertamente, la mayor parte de los contenidos no sólo no plantean problemas, sino que resultan productivos al usuario, tanto en el ámbito personal como en el profesional. Pero en un porcentaje reducido de casos la información que el usuario encuentra es abusiva porque las especiales características de Internet han sido aprovechadas para transmitir contenidos ilícitos como pornografía infantil, informaciones racistas, xenófobas, violentas, difamatorias o perjudiciales para los derechos de ciertos usuarios. Internet facilita así nuevas formas de ataque a valores jurídicos protegidos.

Su carácter transnacional y el alcance global de las redes de transmisión digital hacen de Internet un medio privilegiado de difusión de la información. Los contenidos introducidos en la Red trascienden las fronteras de los Estados y pueden ser consultados por un usuario situado en cualquier país del mundo. En consecuencia, los abusos cometidos producen efectos en todos aquellos países que tienen acceso a la Red.

La ausencia de regulación en esta materia sobre Internet en casi todo el mundo, ha permitido que los infractores difundan todo tipo de informaciones ilícitas y nocivas, sin temor a ser inculpados o demandados. Esta característica, si bien era predicable de la Red durante los primeros años de su desarrollo, se va disipando desde el momento en el que los Estados se disponen a dictar leyes para perseguir y castigar a los infractores.

Así también, la ausencia de una autoridad "unica suprema" que controle los contenidos en la Red ha favorecido la impunidad de los infractores. Ningún Estado controla Internet porque la Red no pertenece a nadie, sino que se nutre de las aportaciones de las innumerables redes de ordenadores que existen en el mundo y se interconectan entre sí.

Esta posibilidad de transmisión de contenidos ilícitos y nocivos ha sido un motivo de preocupación para gobiernos, empresas del sector y usuarios. Para abordar esta situación, desde mediados de la pasada década, organismos internacionales, autoridades nacionales, jueces y tribunales de numerosos países se han involucrado en la búsqueda de soluciones para poner fin a estos abusos que se generan en Internet.

Por regla general, la información que el usuario encuentra en Internet es lícita, legítima y le reporta numerosos beneficios. Pero la realidad demuestra que un porcentaje, reducido si cabe, de las informaciones que se pueden encontrar en su navegación son potencialmente ilícitas o nocivas.

Pero es necesario aclarar la diferencia entre ilícito y nocivo, ya que ambos conceptos son relativos. Ni toda la información es considerada ilícita por los mismos Estados, ni toda es nociva o perjudicial para todas las personas.

Son contenidos ilícitos los merecedores de una respuesta penal: la utilización de Internet para la difusión de pornografía infantil, la difusión de contenidos racistas o xenófobos, la apología del terrorismo, las difamaciones o las violaciones de la propiedad intelectual. Son nuevas formas de ataque a valores jurídicos protegidos: la libertad e indemnidad sexual[26], la dignidad humana, el derecho al honor, a la intimidad o el derecho de la propiedad intelectual. Existe cierto consenso entre los Estados en calificar como delito este tipo de contenidos.

Por el contrario, no lo hay para los contenidos nocivos. Éstos, aunque dañinos para determinadas personas en base a sus valores éticos, religiosos o políticos, no son merecedores de respuesta penal.

Aunque los ejemplos que pueden encontrarse de contenidos ilícitos y nocivos en la Red pueden ser numerosos, hay que destacar que las acciones que han despertado más atención y reacciones más intensas han sido todas aquellas relacionadas con la pornografía, y en especial con la pornografía infantil.

Al hablar de contenidos ilícitos y nocivos hay que distinguir dos problemas que requieren respuestas diferentes. Por ejemplo, la pornografía infantil es un contenido prohibido para el conjunto de la sociedad. La pornografía, lícita para adultos, puede producir determinados efectos perjudiciales para el normal desarrollo de los menores. En el primer caso, se trata de un contenido ilícito. En el segundo, de un contenido nocivo.

Mientras que parece existir cierto acuerdo en lo que se refiere al carácter ilícito de una información -al menos en la mayoría de los Estados miembros de la Unión Europea- no puede decirse lo mismo de los contenidos nocivos. Los contenidos ilícitos son delitos merecedores de una sanción penal y entran, pues, en el ámbito de ley vigente en cada Estado. Los contenidos nocivos, si bien no constituyen delito, resultan ofensivos para sus destinatarios en base a sus opiniones raciales, religiosas, morales o políticas, y entran de este modo en el ámbito de la moral.

[26] Término empleado en el Derecho Español para referirse a la Garantía de no sufrir daños.

3.1.1. CONTENIDOS ILICITOS EN INTERNET

Son contenidos ilícitos, como ya se ha subrayado, aquellos contenidos susceptibles de entrar en el ámbito de aplicación de las normas penales de un determinado país. Cada Estado determina qué contenidos son considerados delito a la luz de su ordenamiento jurídico. Ahora bien, la calificación penal de un contenido varía mucho de un país a otro. Factor que no se corresponde con el carácter transnacional y alcance global de la Red, porque lo que es considerado delictivo en un país no lo es en otro Estado. Por ejemplo, la negación del holocausto judío es un delito en Francia, en Israel, en Austria y en Alemania, pero no está tipificado en otros Estados de la Unión Europea, ni en México y en algunos países americanos.

Los gobiernos han sido plenamente conscientes de la colisión entre la aplicación territorial de las normas penales y el carácter transnacional de la Red. De este modo, se han levantado voces desde diversos foros en demanda de una respuesta global a un problema que también es global.

Esta característica exige la cooperación internacional en la lucha contra los contenidos ilícitos en Internet. Cooperación que se pone de manifiesto en los trabajos realizados en diversas partes del mundo, por lo que se expondrá lo que se considera de mayor trascendencia en el seno de la Unión Europea. En 1996, la Comisión, en la *Comunicación sobre los contenidos ilícitos y nocivos en Internet*[27], define los contenidos ilícitos como "aquellos susceptibles de entrar bajo el ámbito de aplicación de las normas penales de los estados miembros" y destaca el consenso entre los socios comunitarios en torno al concepto de contenido ilícito.

[27] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre contenidos ilícitos y nocivos en Internet. COM (96) 487 Final, de 16 de octubre de 1996 (DO C 70, de 6 de marzo de 1997).

Algunos contenidos ilícitos generan responsabilidad penal, como sucede con los contenidos terroristas, los relacionados con la pornografía infantil, las estafas electrónicas, las falsedades documentales, la trata de seres humanos o incluso la difusión de documentos racistas o xenófobos. Otros contenidos ilícitos generan responsabilidad civil (sola o conjuntamente con la responsabilidad penal), como son la violación de la propiedad intelectual, la vulneración de la protección de datos, la difamación o la publicidad engañosa.

Internet representa de este modo una nueva forma de atacar valores jurídicos protegidos: la libertad e indemnidad sexual de los menores; el derecho al honor, a la intimidad personal y familiar y a la propia imagen; la dignidad humana; o los derechos de propiedad intelectual. Valores que eran susceptibles de ser atacados también fuera de las redes digitales, pero que se presentan especialmente vulnerables ante el uso de las nuevas tecnologías.

Sin ánimo exhaustivo, a continuación se señalan los ejemplos más relevantes de contenidos ilícitos que se pueden encontrar en la Red.

A) LA PORNOGRAFIA INFANTIL Y LAS PERVERSIONES PORNOGRAFICAS

Internet representa un mercado criminal muy lucrativo que se encuentra en pleno auge. Internet se ha convertido en el nuevo lugar de reunión de los pederastas que intercambian todo tipo de informaciones delictivas (en forma de imágenes, textos, animaciones o sonidos) a través del correo electrónico, los grupos de noticias, las listas de discusión, las páginas web o en cualquiera de los millones de salones de conversación en tiempo real *(chat)* que existen en la Red. Son delincuentes difíciles de localizar porque estos individuos, alguno de ellos integrantes de importantes redes internacionales, utilizan los ordenadores de instituciones intachables

(universidades, instituciones públicas, museos, centros religiosos, etc.) y se comunican a través de códigos que hace difícil su detección (anonimato, informaciones cifradas, etc.).

Las maniobras de atracción o seducción que, para disimular su verdadera naturaleza, denominan marketing o mercadeo, pueden desplegarse en toda su magnitud en Internet (a favor principalmente de su carácter interactivo) para atraer y condicionar a los menores, que por tales, no tienen desarrollados mecanismos de defensa ni de selección, siendo por tanto el costado débil de la ecuación, al que es necesario proteger con medidas preventivas.[28]

El ejercicio de la pedofilia por la red es un "cáncer virtual" que se extiende rápidamente por todo el mundo, el cual viaja a través de mensajes que reciben diariamente millones de equipos de cómputo.

Cualquier usuario conectado a internet está expuesto a la recepción de imágenes y videos de pornografía infantil. No es necesario visitar *webs* para recibir materiales de menores desnudos, ya que los *hackers* – expertos de la red – se encargan diariamente de hacerlos llegar a cualquier rincón del mundo.

En su tarea diaria para captar un mayor número de visitantes, los portales de internet contienen *ligas* de pornografía en sus buscadores. Con el simple hecho de escribir la palabra *sexo* (o *sex* en inglés) el usuario recibe cientos de *ligas* a *webs* de pornografía.

La comunicación en tiempo real que proporciona internet ha abierto un mercado para las mafias de explotadores de menores, quienes mediante la exclusividad de sus víctimas manejan el tráfico ilegal de imágenes de menores.

Las páginas o portales de pornografía son unas de las más visitadas por personas de todo el mundo, y por ende las más rentables.

Aun cuando muchos de estos sitios –en su mayoría estadounidenses o asiáticos- estipulan la legalidad de sus contenidos, basta ver la poca vestimenta de los menores, sus miradas y poses eróticas para darse cuenta de la perversidad de los mensajes que contienen las fotografías.

Alemania es el país con mayor número de turistas sexuales y de mayor demanda de material pornográfico, le siguen Estados Unidos, Australia, Francia y Nueva Zelanda, y desde luego México no se queda atrás.

Así, en España, la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, creada en marzo de 2000, ha perseguido 49 delitos relacionados con la pornografía infantil a través de Internet, y en Estados Unidos se calcula, por ejemplo, que cada día se añaden veinte mil páginas pornográficas a la Red. Esta es la razón por la que una gran parte de las acciones judiciales e iniciativas que comentaremos en los apartados siguientes tienen como referencia estos temas.

Durante el Congreso Mundial Contra la Explotación Sexual de Menores se concluyó que la pobreza es el factor principal por el cual los niños son obligados a prostituirse.

La pornografía puede definirse como el carácter obsceno de una obra literaria. Ello nos remite a la definición de lo obsceno: obsceno es aquello que es lascivo, ofensivo o contrario al pudor (impúdico). Tanto un concepto como el otro pueden ser catalogados como conceptos evolutivos o dinámicos ya que la definición de sus contenidos varía con el tiempo; lo obsceno, varía con los cambios que la sociedad ha tenido respecto a los valores y las virtudes. Y el concepto de obra literaria, también

[28] Véase www.delitosinformáticos.com. *Regulación del Acceso a Internet por Menores*, 18 de marzo de 2003.

ha ido evolucionando, con el surgimiento de nuevas formas de expresión del arte. Es por ello que ambos conceptos son evolutivos, por oposición a lo estático.

Siguiendo la línea de la presente definición, en cuanto a concepto evolutivo y dinámico, se podría hablar de una definición de "pornografía actual", que va más allá de la mera acepción que aparece en los diccionarios, en un artículo que ha sido extractado de publicaciones efectuadas por INTERPOL, la Unidad de Investigación de la Delincuencia en Tecnologías de Información del Cuerpo Nacional del Reino Unido de España y de la actividad desarrollada por la División Inteligencia Criminal Informática de la Policía Federal Argentina, se expresa que el concepto de "pornografía" puede resumirse en dos funciones principales: "producir excitación erótico-sexual" y, "actuar como forma de liberación ante sociedades represivas de la sexualidad", pues nadie puede negar que hace treinta años atrás, existía una cierta represión frente a todo lo referido al sexo y sus formas de manifestación; pero en la actualidad, nadie puede afirmar que se esté reprimiendo la sexualidad, ya que los quioscos de diarios, los video clubs, los sex -shops, las salas X, y las cadenas televisivas no andan con vueltas a la hora de ofrecer material sexual. Tanto es así que se hizo necesario aprobar leyes para protección de los menores[29], que recogen entre otras cuestiones preservar el desarrollo físico, mental y moral de los mismos y la emisión de programas que atenten contra las cuestiones antes nombradas, como ser que contengan escenas de pornografía o violencia gratuita. Pero diversas formas de "pornografía actual" se han alejado peligrosamente de su concepto original "erótico- sexual", para pasar a acercarse a la "criminalidad sexual", nos referimos en este caso a videos y revistas, con muchísima más fuerza en esta época de la informática todo el increíble cúmulo de material pornográfico que existe en Internet cuyos mensajes van dirigidos a estimular la consecución de conductas delictivas, y lo que es más grave aún el perjuicio que pueden ocasionar tales materiales a los menores, lo cual nos tiene que llevar indefectiblemente a la reflexión y a lanzarnos a

[29]Vgr. En México se encuentra en vigor la Ley Para la Protección de los Derechos de Niñas, Niños y Adolescentes, así como también la Ley de los Derechos de las niñas y niños en el Distrito Federal. En Estados Unidos la Ley para la Protección Online

la búsqueda de soluciones, para evitar graves daños en nuestros niños.

B) LA DIFAMACION EN INTERNET

Internet posibilita nuevas formas de ataque para lesionar valores jurídicos protegidos. Uno de esos valores lo representa el derecho al honor, a la intimidad personal y familiar, y a la propia imagen, fácilmente vulnerable en las redes digitales. Algunos usuarios de Internet aprovechan el anonimato de los mensajes de correo electrónico y la fugacidad de la información transmitida en las redes para lesionar el derecho al honor y a la propia imagen de terceros, causando daños que trascienden las fronteras de los Estados.

La jurisprudencia comparada ofrece algunos ejemplos. En 1996 se planteó en Europa el primer caso de difamación en Internet. El Sr. Geodfrey, un profesor británico, demandó a *Demon*, proveedor de servicios de Internet, por no proceder a la retirada de los mensajes difamatorios que los suscriptores del proveedor enviaban a un grupo de noticias, (soc.culture.thai) al que *Demon* daba acceso. Cuatro años más tarde las partes llegaban a un acuerdo para reparar el perjuicio causado al derecho al honor del demandante (caso *Geodfrey v Demon Internet")*. Dos años más tarde un caso similar se suscitaba ante los tribunales franceses. Estelle Halliday, conocida modelo francesa, demandó a un proveedor de servicios de Internet por albergar un sitio web desde el que se difundían fotografías íntimas de la demandante que vulneraban su derecho a la propia imagen (asunto *Estelle Halliday v. Valentin laCambre*[30]).

---

de la Infancia de 1998.

[30] Asunto *Estelle Halliday c. Valentin LaCambre*. Ordonnance de référé de 9 de junio de 1998. Tribunal de Grande Instante de

C) EL RACISMO, EL ANTISEMITISMO Y LAS CONDUCTAS VIOLENTAS

Internet también se ha convertido en un foro ideal para que personas de todo el mundo puedan comunicar sus ideas racistas, antisemitas y violentas: la incitación al odio, la discriminación o la violencia contra personas o grupos de personas por razón de su raza, nacionalidad, sexo o religión encuentran en Internet su escaparate al mundo. Cualquiera de los servicios de Internet pueden ser utilizados por individuos sin escrúpulos que, amparándose en las especiales características de la Red, hacen apología del nazismo y niegan el holocausto judío.

La jurisprudencia europea ha conocido varios casos en los últimos años. En 1996, la Asociación de Estudiantes Judíos de Francia demandó a nueve proveedores de acceso a Internet por la existencia de mensajes y documentos en los que se negaba el holocausto judío en los sitios web y foros de discusión a los que daban acceso (Asunto *UEFJ c. Cavalcom)*[31]. En junio de 1997, un tribunal alemán ordenó a varios proveedores de servicios impedir a sus abonados el acceso a sitios web calificados de neonazis. En uno de ellos, una antigua dirigente del Partido Social Demócrata Alemán daba acceso a la revista *Radikal* desde sus páginas web personales. En esta revista se contenían instrucciones acerca de cómo sabotear las líneas férreas.

París. Affaire Estelle Halliday c. Valentin LaCambre et Daniel.

[31] Asunto *UEFJ c. Cavalcom*.Ordenance de référé de 12 de junio de 1996.Tribunal de Grande Instante de París.Affaire Union des étudiants Juifs de France c. Cavalcom et autres.

D) LA VULNERACION DE LOS DERECHOS DE PROPIEDAD INTELECTUAL

La gran facilidad con la que se pueden copiar obras protegidas por los derechos de autor ha aumentado un importante volumen de comercio en el que internautas de todo el mundo intercambian obras sin la autorización de su titular: las aplicaciones de Internet se utilizan para soslayar las obligaciones económicas que imponen los derechos de autor. Numerosos sitios web se dedican a ofrecer copias no autorizadas de programas de ordenador, canciones en formato MP3 sin la autorización de su titular, etc.

La jurisprudencia, tanto europea como de los Estados Unidos, es prolífica en casos de vulneraciones de los derechos de autor. El primero de ellos lo ofrece la jurisprudencia estadounidense. En 1993, un proveedor de servicios fue demandado por albergar una página web desde la que se difundían fotografías protegidas por derechos de autor, propiedad de la revista *Playboy* (caso *Playboy c. Frena*[32]). Desde entonces, los asuntos relacionados con la vulneración de los derechos de autor se han incrementado de un modo espectacular.

[32] Sentencia *Playboy Enterprises Inc. V Frena* (1993).

3.1.2. CONTENIDOS NOCIVOS EN INTERNET

Ciertos contenidos pueden resultar ofensivos para el destinatario porque expresan opiniones políticas, creencias religiosas o juicios de valor sobre las diferencias raciales. Son los llamados contenidos nocivos, dañinos para el receptor pero que no justifican una sanción penal. Por ejemplo, páginas web que ridiculizan figuras sagradas religiosas, o imágenes pornográficas vistas por menores.

A diferencia de lo que sucede con los contenidos ilícitos, no existe acuerdo en torno al concepto de contenido nocivo, al ser éste, como ya se ha dicho, un concepto que varía de un Estado a otro en función de sus valores éticos, culturales, sociales o políticos. Hecho que se pone claramente de manifiesto en Internet: lo que es "políticamente correcto" en los Países Bajos no lo es en México o España por ejemplo, o más aún, lo que es adecuado en España o México no tiene por qué serlo en un país islámico. En suma, el concepto de contenido nocivo dependerá de las distintas tradiciones jurídicas y de las diferencias socioculturales de cada uno de los países, así como de quien sea el receptor de la información.

La regulación de los contenidos nocivos en Internet reclama una respuesta global que compatibilice dos intereses contrapuestos: de un lado, la necesidad de proteger a las personas respecto de material ofensivo; de otro, la protección del derecho fundamental a la libertad de expresión de las personas que introducen los contenidos en la Red.

3.2. LOCALIZACION DE LOS CONTENIDOS ILICITOS Y NOCIVOS

Todas los sistemas, herramientas o aplicaciones de Internet son susceptibles de constituir el soporte de contenidos ilícitos y nocivos: la navegación en la *World Wide Web* o Telaraña Mundial, la transferencia de archivos, el correo electrónico, las listas de distribución, los grupos de noticias, las conversaciones en tiempo real o los buscadores de información.

Internet es multimedia, lo que implica que las informaciones transmitidas a través de la Red -también los contenidos ilícitos y nocivos- pueden revestir la forma de texto, imágenes, animaciones o sonidos.

Para acceder a la información contenida en la Red, el usuario necesita determinadas herramientas que, por un lado, garantizan a los usuarios el acceso a la información que se encuentra en la Red, y por otro, facilitan la comunicación entre los propios navegantes.

Pues bien, cualquiera de estos sistemas, herramientas o aplicaciones puede ser utilizada como medio de difusión de información considerada ilegal o prohibida por la legislación de algún país del mundo. También los sistemas, herramientas o aplicaciones de Internet sirven como medio de comunicación entre personas que llevan a cabo actividades delictivas: si hasta no hace mucho tiempo los delincuentes se comunicaban a través del teléfono, fax o correo ordinario, ahora se comunican en tiempo real en los *chat* o se envían correos electrónicos de la misma manera que lo haría cualquier otro internauta.

Los sistemas, herramientas o aplicaciones de Internet que pueden ser utilizadas como vehículo de los contenidos ilícitos y nocivos, como ya se han explicado en el capítulo II de esta tesos.

a) *La Telaraña Mundial (World Wide Web. WWW).* En la Red ha proliferado información considerada ilícita por algunos países: sitios web en los que se detallan cómo fabricar una bomba, o páginas de asociaciones racistas y xenófobas, sitios web en los que se contienen fotografías de pornografía infantil, páginas web en las que se incluye información difamatoria, información sobre la fabricación de drogas de síntesis, páginas que incitan al suicidio o cualquier otro tipo de información considerada ilegal.

A pesar de que el número de sitios web en los que se encuentran este tipo de informaciones o contenidos ilícitos es mínimo el en relación a la ingente cantidad de información que se encuentra en Internet, lo cierto que se trata de una cuestión que es motivo de preocupación.

b) *La transferencia de archivos (FTP).* Al igual que con las páginas web, también los archivos FTP pueden contener informaciones ilícitas.

c) *El correo electrónico (e-mail).* Aunque la mayoría de los mensajes de correo electrónico persiguen fines totalmente legítimos de comunicación entre dos o más usuarios de Internet y por tanto quedan protegidos por el derecho al secreto de las comunicaciones privadas. algunos de ellos contienen información considerada ilícita por la legislación de algunos países. Por ejemplo, el envío de mensajes de correo electrónico con contenidos pornográficos a menores de edad, acoso sexual a través de *e-mail,* mensajes injuriosos o calumniosos, o el envío masivo de mensajes no solicitados con la única intención de perjudicar (es el llamado *mailbombing* que produce el colapso de los sistemas informáticos).

d) *Las listas de distribución (mailing lists).* Este también puede ser otra herramienta para mostrar contenido nocivo o ilícito en el Internet. El único control que pesa sobre los grupos de noticias son las propias normas de conducta de los foros, al igual que ocurre en las listas de distribución, y ello ha propiciado que, en no pocas ocasiones, algunos usuarios hayan hecho un uso abusivo de los *newsgroups* para incluir contenidos ilícitos.

e) *Los grupos de noticias (newsgroups).* El único control que pesa sobre los grupos de noticias son las propias normas de conducta de los foros, al igual que ocurre en las listas de distribución, y ello ha propiciado que, en no pocas ocasiones, algunos usuarios hayan hecho un uso abusivo de los *newsgroups* para incluir contenidos ilícitos. Por ejemplo, enviando mensajes con contenidos racistas -como hizo Monsieur X en agosto de 1999-, difamatorios, imágenes de pornografía infantil, instrucciones para descodificar Canal +, técnicas para inutilizar los dispositivos de protección de los programas de ordenador (software) e incluso mensajes con instrucciones para fabricar explosivos.

f) *Las conversaciones en tiempo real (chat).* Algunos canales tienen moderador que vela porque los usuarios respeten las normas de conducta del canal, si no quieren ser expulsados. Los canales de *chat* se dedican a un tema específico " (por ejemplo, "alicante", "solteros", "música", etc.), y como en la vida real, las conversaciones giran tanto en torno a temas legítimos como a temas de dudosa legalidad.

g) *Las herramientas de búsqueda de la información (search engines).* Por regla general, los motores de búsqueda permitirán al usuario acceder a los sitios web para obtener información; en ocasiones, facilitarán al usuario la localización de documentos web en los que se encuentren contenidos ilícitos y nocivos (por ejemplo,

al insertar la palabra "sexo", el buscador proporciona todo un listado de sitios web relativos al sexo, incluidos los de pornografía infantil, zoofilia, etc.).

3.3. PARTICIPANTES EN LA DIFUSION DE LOS CONTENIDOS EN INTERNET

Cualquier sujeto que participe en la difusión de los contenidos corre el riesgo de entrar en contacto con informaciones ilícitas y nocivas: los proveedores o desarrolladores de contenidos, que seleccionan y cargan información en Internet; los intermediarios técnicos que hacen posible la transmisión de la información (operadores de telecomunicaciones y proveedores o prestadores de servicios de Internet); y en fin, los propios usuarios de la Red.

Los proveedores o desarrolladores de contenidos son responsables civil y penalmente por actos propios. Es un principio general del Derecho, reconocido en todas las legislaciones. Los problemas surgen cuando el proveedor o desarrollador de contenidos ilícitos se ampara en el anonimato. En estos casos, se plantea la posible responsabilidad de los intermediarios técnicos a los que difícilmente se les puede aplicar los criterios tradicionales de la prensa escrita, que no sirven en las redes digitales dada la fugacidad de los contenidos y la dificultad de localizar el origen o el destino de la información.

También los usuarios de Internet pueden ver comprometida su responsabilidad cuando cometen actividades prohibidas por las leyes de su país.

Además de los emisores (proveedores o desarrolladores de contenidos) y los destinatarios de la información (internautas o usuarios de Internet) son necesarias nuevas figuras que posibilitan que la información llegue a los navegantes de todos los rincones del planeta: son los intermediarios técnicos, tanto los que ofrecen las instalaciones técnicas por las que se transmite la información (operadores de

telecomunicaciones) como los que ofrecen los distintos servicios de Internet (prestadores de servicios de Internet).

3.3.1. LOS PROVEEDORES O DESARROLLADORES DE CONTENIDOS

La gran cantidad de información a la que accede el usuario de Internet ha sido previamente seleccionada y cargada en las redes de transmisión digital. A la persona que selecciona los contenidos y los introduce posteriormente en la Red se la conoce como proveedor de contenidos[33]. Puede tratarse de una persona física (cualquier particular puede elaborar su página personal o enviar un mensaje a un grupo de noticias), o bien de una persona jurídica (una empresa) que pone a disposición de los usuarios de Internet un determinado contenido o una información (ya sea en un sitio web, una base de datos o una lista de distribución), los proveedores de contenidos son los que crean, producen y ponen a disposición del público contenidos.

Pero no toda persona que selecciona e introduce información en la Red para que pueda ser consultada por el resto de los internautas persigue los mismos objetivos. Unos simplemente desearán que la información tenga la más amplia difusión (esto es, utilizan las redes digitales como vía de difusión de conocimientos o de información). Son los llamados proveedores de contenidos "no profesionales", como pueden ser las entidades académicas, los investigadores, los particulares -a través de sus páginas personales-, las asociaciones de usuarios, etc. Otros, además, seleccionarán e introducirán contenidos en Internet para desplegar una actividad comercial, esto es, emplean Internet como una herramienta de marketing añadida a su actividad habitual. Son los proveedores o desarrolladores de contenidos "profesionales" (empresas, creadores de videojuegos, bancos, editores. prensa, etc.). Se trata de una distinción relevante a efectos de determinar las obligaciones de identificación que la legislación establece para cada uno de ellos, tal y como se verá

en el siguiente capítulo.

Ahora bien, para que el resto de los usuarios de Internet pueda consultar la información, el proveedor de contenidos necesita el vehículo de transmisión de la información, el medio que haga llegar la información a todos los rincones del planeta. Para ello necesita intermediarios técnicos que le faciliten esa labor.

3.3.2. LOS INTERMEDIARIOS TECNICOS

Bajo el concepto de intermediarios técnicos se agrupan dos categorías de actores: por un lado, los operadores de telecomunicaciones, y por otro, los prestadores de servicios de Internet. Ambos ofrecen al proveedor de contenidos la posibilidad de hacer accesible la información al resto de internautas. Los intermediarios técnicos, sin embargo, raramente participan en el proceso de selección o carga de la información en las redes digitales, sino que más bien limitan su tarea a hacer posible la transmisión en línea.

Los operadores de telecomunicaciones. Los operadores de telecomunicaciones[34] son empresas intermediarias en la comunicación en línea que aseguran la interconexión entre las redes, proporcionando la infraestructura que permite la transmisión de información (los cables, los encaminadores[35], los interruptores, etc.).

No es de sorprenderse que ahora seamos destinatarios de la publicidad de diferentes compañías que ofrecen el servicio de Internet, de modo que, como usuarios o abonados a un servicio telefónico, podemos elegir las condiciones de

---

[33] Ejemplos en México: UNAM, IPN, UNITEC, UVM.

[34] Ejemplos en México: Cisco, Marconi, 3com, ATT, Enterasys, Extreme.

[35] Un encaminador o *router* es un mecanismo de hardware o software empleado para direccional mensajes entre nodos y subredes que, atendiendo a su estado, pretende hacerlo de la manera más eficiente posible.

prestación del servicio que nos sean más favorables.

Los proveedores o prestadores de servicios de Internet (ISP). Los proveedores o prestadores de servicios de Internet[36] facilitan la transmisión de la información a través de las líneas digitales, pero ni la seleccionan ni la modifican. Estas empresas intermediarias ofrecen distintos servicios al usuario, que van desde el acceso a Internet hasta los servicios de valor añadido (por ejemplo, el alojamiento de sitios web, cuentas de correo electrónico y la asistencia técnica al cliente).

Este tipo de intermediarios técnicos desarrollan funciones distintas, de manera exclusiva o compartida. Esto significa que una misma empresa puede ofrecer un único servicio (por ejemplo, alojamiento de sitios web) o varios al mismo tiempo: un Portal puede disponer de servicio de conversación en tiempo real, listas de distribución o herramientas de búsqueda.

Es importante distinguir los diferentes servicios que ofrecen estas empresas y el papel específico que desempeñan en la transmisión de los contenidos en las redes digitales, en la medida en que de ellas dependerá el grado de responsabilidad que se les, pueda imponer por los contenidos ilícitos introducidos por sus clientes.

El proveedor de acceso a Internet (PAI). El proveedor de acceso o a Internet (PAI) es un intermediario técnico que pone su servidor[37] -conectado permanentemente a la Red- a disposición de sus abonados para permitirles navegar, consultar los sitios web e intercambiar correo electrónico. Esto significa que el usuario puede conectarse a Internet a través del sistema informático del PAI. Para ello necesita un ordenador y un módem[38] conectado a la línea telefónica o a través

[36] Ejemplos en México: Avantel, TELMEX (Prodigy o Infinitum), ATT, e-go.
[37] Ejemplos en México: Avantel, TELMEX (Prodigy o Infinitum), ATT.
[38] Un módem es un dispositivo que permite la comunicación entre ordenadores a través de la línea telefónica normal o una línea de cable.

de la Red Digital de Servicios Integrados (RDSI). El servicio de acceso permite la conexión a través de nodos de los que son propietarias las compañías telefónicas[39].

El funcionamiento es el siguiente: cuando el usuario escribe la dirección URL[40] de un sitio web en la pantalla de su ordenador está haciendo una llamada telefónica a un nodo, que normalmente será el nodo local, pues es el más cercano y, por tanto, el de menor costo económico. A su vez, el nodo conecta con el PAI del usuario (que previamente le ha dado un número de usuario y una contraseña). Comprobados los datos y autorizado por el proveedor, el usuario accede a la Red.

Si son varias máquinas de una red privada (Intranet) las que acceden a la Red, el PAI recibe el nombre de *proxy,* una de cuyas funciones consiste en centralizar el tráfico entre Internet y la red privada con el fin de evitar que cada una de las máquinas de la intranet tenga que disponer necesariamente de una conexión directa a Internet. Es el sistema utilizado por las Universidades, o un buen número de empresas.

Proveedor de alojamiento de sitios web (PAW). Los proveedores de alojamiento de sitios web[41] son intermediarios técnicos que alquilan espacio en el disco duro de su sistema informático a sus clientes para que puedan albergar en él sus páginas web. Su función consiste en almacenar contenidos seleccionados e "introducidos" por sus clientes.

También desempeñan una función de alojamiento de sitios web los llamados *Mirror,* servidores de Internet que albergan copias exactas de otros sitios web o partes de él. Suelen contar con la autorización del proveedor de alojamiento original

[39] En el 99% de los casos los proveedores de acceso no controlan la línea que le conecta a Internet ya que ésta pertenece a los operadores de telecomunicaciones. Los proveedores de acceso se limitan a arrendar las líneas de gran capacidad a las compañías telefónicas para subarrendarlar a su vez a sus clientes, los usuarios.

[40] El *Uniform Resource Locator (URL)* es un sistema unificado que permite la identificación de los recursos disponibles en Internet. Las direcciones URL se componen de un protocolo, un nombre de dominio y la dirección local del documento dentro del servidor. Un ejemplo de URL es http://www.ua.es/bibliotreca

[41] IBM, UNISYS, GEOCITIES, YAHOO, TERRA, ANANTEL.

y sirven para aumentar la rapidez de acceso del usuario a servidores que están localizados en países más lejanos.

Operadores de listas de distribución o foros de discusión (OLD). Los intermediarios técnicos que facilitan el acceso a listas de distribución reciben el nombre de operadores de listas de distribución[42] (OLD) y su tarea consiste en alquilar o ceder espacio en el disco duro de su sistema Informático para que sus abogados puedan enviar y recibir mensajes en su buzón de correo. Además, los operadores pueden moderar, o no, las listas de distribución. Por ejemplo, una universidad puede ofrecer una lista de distribución -moderada por un profesor- a los alumnos matriculados en un curso de especialización para que puedan debatir las cuestiones propias de la materia que están estudiando.

Operadores de grupos de noticias (OGN). Si la empresa intermediaria alquila o cede espacio en su sistema informático para que los usuarios puedan consultar la gran variedad de grupos de noticias que existen en la Red, recibirá entonces la denominación de operador de grupos de noticias[43], o, más comúnmente, servidor de noticias. Existen servidores situados en muchos países del mundo, si bien la red a través de la cual se conectaban originariamente formaba la llamada *Usenet*, que en la actualidad se encuentra integrada en Internet.

La enorme variedad de grupos de noticias que existen los convierte en un foro ideal para transmitir todo tipo de información, que suele quedar grabada en el sistema informático del servidor durante un tiempo variable. Los grupos de noticias pueden ser consultados por los suscriptores sin que los mensajes que en ellos se contienen tengan que ser enviados al buzón de correo de cada uno de los usuarios.

---

[42] Ejemplos en México: UNAM, UAM, ITESM, ITAM.
[43] Ejemplos en México: UNAM, UAM, UVM, ITESM, ITAM

Operadores de conversaciones en tiempo real (OC). Los operadores de charla en tiempo real *(chat)* son los intermediarios técnicos en la comunicación en línea[44] que permiten a los usuarios de Internet comunicarse en tiempo real con otros usuarios mediante los programas citados anteriormente. El IRC *(Inter Relay Chat)*, por ejemplo, permite que distintos usuarios de Internet; se comuniquen a través de mensajes escritos en la pantalla de su ordenador que son leídos en tiempo real por otro u otros usuarios. El usuario se conecta a Internet y contacta con el operador de *chat* que le oferta los distintos canales clasificados por temas, entre los que puede elegir el usuario. El ICQ *(I seek you)*. por su parte, es un programa de *software* de conversación en tiempo real que permite que sus usuarios puedan saber si otros usuarios se encuentran conectados a la Red.

Buscador o herramientas de búsqueda (B). Con el fin de facilitar la tarea de búsqueda de información en las redes digitales han surgido distintas empresas especializadas en proporcionar las herramientas necesarias a los usuarios[45]. Como se señalaba en el apartado 2.4.7, la búsqueda se puede llevar a cabo por temas o por palabras clave. Incluso, es posible localizar personas a través de sistemas como WAIS, Astra, WHOIS o X500.

Portal de acceso a Internet (P). Más recientemente han aparecido intermediarios en la comunicación en línea que funcionan como "puertas de acceso a Internet". Son los llamados Portales[46], que clasifican la información de Internet con el fin de reducir los tiempos de búsqueda y guían al usuario en su navegación por la Red, además de ofrecerles toda una gama de servicios de valor añadido (cuentas de correo, servicios de chat, comercio electrónico, etc.).

---

[44] Ejemplos en México: www.elchat.com, www.avantel.net, www.latinchat.com.

[45] Ejemplos en México: www.yahoo.com, www.altavista.com, www.google.com, www.vivisimo.com, www.pandia.com, www.webcrawler.com

[46] Ejemplos en México: www.todito.com, www.esmas.com, www.prodigy.com

Los Portales pueden ser de carácter general u horizontales (por ejemplo, EresMas.com, Ya.com) o pueden estar dedicados a temas específicos, o verticales *(Portalatino.com,* dedicado a los derechos de los autores; *All Law -alllaw.com-*, específico para el mundo jurídico; el Portal del *Magister Lucentinus -auipit.com-* de la Universidad de Alicante, que contiene textos legales y jurisprudenciales, resúmenes en hipertexto sobre propiedad industrial, propiedad intelectual y Derecho de las Nuevas tecnologías, etc.).

3.3.3. LOS USUARIOS DE INTERNET

La información cobra sentido cuando es recibida por el destinatario, que en mundo de Internet recibe el nombre de usuario, navegante o internauta. Es la persona que consulta o intercambia informaciones a partir de su ordenador, que está conectado al sistema informático de su PAI.

Si el receptor de la información es único -por ejemplo, cuando se envía un correo electrónico o se participa en una conversación en tiempo real- el contenido de la misma quedará amparado en el derecho a la libertad de expresión que, junto con el derecho al secreto de las comunicaciones, hace que sólo pueda ser interceptada previa resolución judicial.

Si por el contrario el receptor es plural -por ejemplo, cuando la información se contiene en los documentos de un sitio web- no se considerará comunicación privada, y los contenidos que se viertan o la información que se difunda serán considerados comunicación pública no protegida por el derecho al secreto de las comunicaciones y, por tanto, susceptible de tener cabida dentro del ámbito de aplicación de las normas penales.

El usuario debe, al igual que los restantes actores de Internet, hacer un uso responsable de las redes digitales y respetar los derechos de terceros (derechos de propiedad intelectual, respeto de la vida privada, protección de menores, al respeto mutuo, a la convivencia pacífica, etc.). A pesar de ello, son frecuentes los casos en los que esto no ocurre, y así son condenados usuarios por "descargar" contenidos ilícitos de la Red. Fue el caso de *Philippe* H., quien fue condenado, a principios de 1998, por adquirir pornografía infantil a través de Internet en Francia.

3.3.4. MODO DE TRANSMITIR LA INFORMACION EN LA RED

Con el fin de clarificar la posición que ocupa cada uno de los actores de Internet en el proceso de transmisión en línea, veamos las siguientes situaciones.

Primera. El usuario quiere consultar una página web. Para ello, contrata con un proveedor de acceso a Internet (PAI) que le proporciona el acceso a la Red a través de las líneas telefónicas que ha subarrendado a un operador de telecomunicaciones (OT). Para llegar al sistema informático en el que está alojado el sitio web (PAW) al que el usuario quiere acceder dispone de varias posibilidades: uno, que conozca la dirección del sitio web; en este caso, basta tan sólo con escribir la dirección URL en el navegador de su ordenador. Dos, que no conozca la dirección del sitio web; en este supuesto, puede hacer uso de los Portales de Acceso a Internet (P) -que le guiarán hasta encontrar el lugar que busca- o de las Herramientas de Búsqueda (B), ya sea a través de índices temáticos o a través de palabras clave.

Segunda. El usuario quiere enviar un mensaje de correo electrónico. El emisor, conectado a la Red a través de su PAI, envía; un mensaje que es recibido por el proveedor que le ha ofrecido una cuenta de correo (normalmente, el propio PAI, otros intermediarios pueden ofrecer este servicio: los portales, los buscadores o los

proveedores de alojamiento). El mensaje es enviado a través de la Red hasta llegar al destinatario también conectado a la Red mediante un PAI.

Tercera. El usuario quiere hacer uso de las listas de distribución y de los grupos de noticias. Al igual que en los supuestos anteriores, el usuario de Internet debe acceder a la Red a través de un PAI conectado a la línea telefónica que le conecta con el operador de grupos de noticias (OGN) u operador de listas de distribución (OLD).

3.4. FACTORES QUE DIFICULTAN REGULAR LOS CONTENIDOS DEL INTERNET

Muchos expertos reconocen la dificultad de legislar sobre Internet ¿Se puede condenar a alguien a que no toque el ordenador?

"El mundo en el que nos vemos inmersos con las nuevas tecnologías de la información, de mensajes cifrados, puertas que se abren y cierran, y kafkiana la pretensión de regular esto". Con tales palabras cerraba Josep M. Tamarit, catedrático de la Universidad de Lleida, el seminario sobre *Internet y derecho penal*, realizado en Barcelona realizado en marzo del 2003. Un seminario dominado por las paradojas entre el viejo mundo de la *dura lex* y la frontera electrónica. Amadeu Abril, miembro de la ICANN, se quejaba de que "criminalizamos todo lo que ocurre en la red y estamos empezando a exagerar. La mayoría de problemas vienen de los *parásitos simpáticos*, que hacen un uso marginal y permisible seguramente"[47].

"Otro equipo, personas como el capitán de la Guardia Civil Anselmo del Moral, quien se quejó de la dificultad de identificación en la red, la transnacionalidad y lo

[47] Consúltese pub80.ezboard.com

que se ha disparado el fraude electrónico. Del Moral pidió la regulación del uso del cifrado, la creación de una fiscalía de delitos informáticos y que "no se pongan las pegas que se nos han puesto cuando el único rastro es el número de teléfono.

"Susan F. Wilson, fiscal de la Oficina de Delitos Informáticos y Propiedad Intelectual estadounidense, se expresó de forma semejante: al grito de "nadie está a salvo" y "amenazan nuestras vidas", llamó a "vigilar a los piratas en el mundo real", interceptando *carriers* y teléfonos. La apoyó el catedrático Ulrich Sieber, recién llegado de una convención de Múnich. Su lema: "Paremos la confrontación, hagamos una nueva alianza entre la industria de Internet y las fuerzas de la ley". Otro: "Lo que es ilegal *off line*, lo es *on line*". Y otro: "Si no podemos controlar a todos los proveedores, controlemos sólo a los de contenido". En el seminario se admitió la dificultad de regular con leyes nacionales un fenómeno supranacional y que resulta difícil pensar en una legislación homogénea en todos los países.

"No solo la Ley sobre la Sociedad de la Información pone trabas al desarrollo de la internet y la industria del software. El panorama internacional no es mucho mejor, hay muchísimos países que tienen muy restringido el acceso a internet. Y en los países en los que no está restringido, está o regulado o esplado. En definitiva, yo voy a ir aprendiendo a usar el silbo por si algún día no me queda otro medio de expresión[48].

"Es difícil hablar de regular el contenido o la conducta en internet, porque se trata de algo que no es tangible, a lo cual no se le puede aplicar una regulación directa, ni se le puede clausurar tan fácilmente; Pero si esta de parte de la sociedad el querer fomentar el uso de contenido apropiado y no discriminatorio, ni ofensivo para ninguno de los usuarios del internet, considerado por muchos como el mayor avance tecnológico de las ultimas décadas. El internet se puede considerar como un arma de

[48] Consúltese pub80.ezboard.com

dos filos, puede seguir creciendo y ayudando a la sociedad, convertirse en el futuro de los negocios internacionales, universidades, etc., y/o se puede convertir en algo que destruya la sociedad como la conocemos hoy día. Para regular el contenido de internet, debe ser una organización a nivel mundial tan grande tal vez como la ONU, donde todas la naciones entren en un consenso sobre como quieren que sus países y habitantes utilicen la herramienta del internet. El internet es la Biblioteca mas grande del mundo, donde se puede conseguir absolutamente todo, hoy día en el mas del 50% de los habitantes del mundo utilizan el internet, por lo tanto tenemos que crear conciencia de que este exceso de libertad a cualquier tipo de información, puede desencadenar que nuestros niños vean cosas que en nada aporten a su enseñanza o que algunos sectores de la sociedad se sientan ofendido por algún contenido discriminatorio, lo cual puede causar que nuestra sociedad se siga dividiendo, y nuestros niños maduren con unas ideas negativas o erróneas de cómo ser mejores seres humanos"[49].

Existen diversos factores que hacen difícil establecer una legislación única para regular el contenido del internet, entre ellos:

a) La utilización anónima de Internet
b) La dificultad para identificar a los proveedores o desarroladores de contenidos de Internet y la privacidad.
c) Los problemas de territorialidad
d) Las limitantes de jurisdicción
e) El no ser internet propiamente un "medio de comunicación social".

Así en los siguiente apartados se explicarán los incisos señalados.

[49] MIRANDA, Emilio, Conferencia sobre la *Regulación del Internet*, España, 18 de Octubre del 2002.

3.4.1. LA UTILIZACION ANONIMA DE INTERNET

Ya se ha señalado que la localización de los proveedores de contenidos es uno de los principales problemas que plantea la atribución de responsabilidad. El anonimato es posible tanto en la creación de las páginas web como en el envío de mensajes de correo electrónico. Cualquiera de estas aplicaciones de Internet puede contener informaciones ilícitas o nocivas.

Normalmente, el creador de una página web puede localizarse a través de su dirección URL en La Red. En los contratos de alojamiento de páginas web se exige la identificación del cliente. Sin embargo, han proliferado en Internet proveedores de alojamiento gratuitos que no exigen la identificación de sus usuarios; basta con aportar una dirección electrónica que muy bien podría no ser real puesto que no suele contrastarse.

La posibilidad de crear páginas web de forma anónima ha traído a determinados individuos que han visto en Internet el medio idóneo para transmitir impunemente cualquier tipo de material ilícito. A finales de 1999 un juez francés señaló, en el *Asunto Lacostt*[50], que el anonimato de los clientes favorece su irresponsabilidad por los contenidos que seleccionan en introducen posteriormente en la Red.

Existen en el mercado programas de software que permiten enviar correos electrónicos de forma anónima. Son los llamados *Anonymous Remailers* que eliminan los datos del mensaje que revelan la identidad del remitente y lo reenvían al destinatario, que no tiene medios para averiguar quién lo ha enviado.

[50] Asunto *lacoste*. Sentencia de 8 de diciembre de 1999. Tribunal de Grande Instante de Nanterre, Affaire Madame L. C. Les sociétés Multimania Production, Fance Cybermedia, SPPI, Esterel.

Hay diferentes tipos de *remailers:* los de tipo *cipherpunk* y los de tipo *mixmaster.* Los *Cipherpunk* permiten al usuario enviar al servidor de correo un mensaje cifrado en el que se contienen las instrucciones para su gestión. Estas instrucciones pueden consistir en guardar el mensaje y enviarlo en la fecha y hora solicitada por el remitente o en enviar los mensajes en un orden determinado. Automáticamente, el servidor de correo sustituye el encabezado y la firma del mensaje con otras nuevas.

Más recientemente han aparecido los *Mixmaster;* que permiten un mayor grado de anonimato. El remitente sustituye su dirección real por un pseudónimo, de forma que las personas con las que se comunica sólo tienen como referencia el alias del remitente. Los servidores de este tipo también aceptan instrucciones codificadas del usuario.

El envío de mensajes anónimos ofrece sin duda muchas ventajas. Permite que los usuarios de Internet hagan comunicaciones confidenciales delicadas, por ejemplo, consultas en línea acerca del SIDA, la homosexualidad, datos médicos, grupos de ayuda mutua, etc. También personas que son objeto de persecución política se pueden beneficiar del anonimato. En estos casos, el envío anónimo de mensajes cumple una función personal y social, por lo que parece muy conveniente mantener este tipo de programas de ordenador. Son las mismas razones por las que resulta imprescindible preservar el anonimato de las personas que llaman, por ejemplo, al Teléfono de la Esperanza, o que se hacen análisis de SIDA en Sanidad, protegiendo su identidad con un código numérico.

No obstante, el anonimato presenta algunos inconvenientes. Los *remailers* han amparado el envío de todo tipo de informaciones ilícitas a otros usuarios, a grupos de noticias y a listas de distribución. Sin embargo, los *remailers* presentan fisuras por las que se puede penetrar en el sistema y rastrear la identidad del remitente. No es fácil, pero es posible. En este sentido, resultan convenientes las alternativas al anonimato

absoluto en la Red, como propone el Reino Unido en "R3 Safety Net", que aboga por el uso de pseudónimos identificables. En este sistema, los datos que correlacionen el pseudónimo con la identidad de la persona quedarían protegidos por la legislación de protección de datos correspondiente.

3.4.2. LA IDENTIFICACION DE LOS PROVEEDORES O DESARROLLADORES DE CONTENIDOS DE INTERNET Y LA PRIVACIDAD

La dificultad de localizar al autor de un contenido ilícito preocupa seriamente a todas las autoridades públicas. Por este motivo, han surgido numerosas iniciativas y legislación de diversos países que pretenden paliar los problemas derivados del anonimato en la Red imponiendo a los prestadores de servicios de Internet la obligación de identificar a sus clientes.

La tensión se manifiesta entre dos polos. De un lado, la necesidad de proteger a los menores y la dignidad humana y la idemnidad sexual en las redes digitales mediante el castigo y la sanción del responsable (para lo cual es necesario proceder a su identificación). De otro, la salvaguardia del derecho al secreto de las comunicaciones, el derecho a la intimidad y el anonimato.

3.4.3. PROBLEMAS DE TERRITORIALIDAD

"Antes de analizar temas como el de la regulación legal de los contenidos ilícitos de Internet, hay que entender que para abordar la problemática de la red, imaginaria -y geográficamente- debemos situarnos en el lugar físico o en el país donde esté instalado un servidor computacional que provea dichos contenidos (cosa que tecnológicamente puede no ser tan fácil de determinar). No hay que

atender al Estado o país en que estén ubicados los usuarios-navegantes de la red, porque éstos, telemáticamente y a través del ciberespacio, lo que hacen es llegar hasta o acceder a ese determinado servidor y a las páginas con diversos contenidos que en él se mantienen, porque ellos lo desean así y porque libremente han optado por acceder a dichos sitios, acción virtual que tecnológicamente se materializa porque varios ISP o proveedores de conectividad lo posibilitan mundialmente.

"Una idea es esencial, Internet -una red telemática pública y abierta- descansa en su "no regulación" o "desregulación local", lo que implica que no se puede censurar desde un Estado determinado una realidad virtual que -normativamente y en teoría- sólo podría llegar a regularse mediante un instrumento internacional, por cierto, siempre y cuando existan criterios uniformes respecto a la forma de hacerlo, vgr. respecto a la improcedencia de difundir contenidos pornográficos. Pero ocurre -es la realidad- que en países más liberales como Holanda la pornografía no es considerada ilegal, al menos no al nivel de países más conservadores como Chile.[51]

3.4.4. LIMITANTES DE JURISDICCION

"Internet no respeta límites geográficos y no reconoce fronteras o jurisdicciones estatales. Los canales de la red traspasan todas las fronteras geográficas y políticas, en consecuencia, por ahora existe incertidumbre respecto a la ley aplicable a actos que carecen de localización física precisa, y son "aterritoriales". Leyes como las chilenas -vgr. de delitos contra la moral, de abusos de publicidad, de derechos del consumidor, de propiedad intelectual e industrial, etc.- sólo pueden pretender tener vigencia dentro del territorio de cada país y sus tribunales

[51] JIJERA LEIVA, Renato Javier, *Criterios Jurisprudenciales en materia de responsabilidad de los ISP*, Ponencia en el VIII Congreso Iberoamericano de Derecho e Informática. Del 21 al 25 de noviembre del 2000. Mexico.

no pueden aplicarlas en el extranjero porque carecen de Jurisdicción para hacerlo. En consecuencia, siempre existirá incertidumbre respecto de la ley aplicable a actos que carecen de localización física precisa.

"Frente al tema de la difusión o distribución de información de contenidos ilícitos, cada uno de los Estados en que estén instalados los servidores respectivos puede aplicar su legislación interna de delitos contra la moral, el orden público, la seguridad económica, la propiedad intelectual, la violación de secretos, etc. Pero ese Estado no puede pretender aplicar sus normas jurídicas más allá de los límites territoriales de su jurisdicción; existen excepciones, por ejemplo en materia de genocidio y delitos contra los derechos humanos, ...pero estas situaciones han sido calificadas previamente por la vía de acuerdos o tratados internacionales. Pues bien: la sanción legal de la difusión en Internet de información ilícita (datos, documentos e imágenes) también -teóricamente- debe acordarse por la vía de un tratado internacional; sólo así se evitarán prácticas de censura o atentados locales contra la libertad de expresión." [52]

3.4.5. INTERNET NO ES UN "MEDIO DE COMUNICACION SOCIAL"

"En Chile, por ejemplo dos parlamentarios pretendieron alguna vez regular localmente Internet con ocasión del debate del Proyecto de Ley Sobre Libertad de Opinión e Información y Ejercicio del Periodismo, también conocido como "Ley de Prensa", opción que afortunadamente no prosperó.

"Nunca entendieron que Internet no es un "Medio de Comunicación Social" de aquellos a que aluden la Constitución y las leyes, como la prensa escrita, la radio y la televisión. Nunca comprendieron que en Internet no existe un editor o un director responsable contra quien dirigirse, por ejemplo si empiezan a circular mensajes

antiracistas, neofazistas, avisos de servicios sexuales, etc. A mayor abundamiento: para la prensa escrita Internet constituye solamente una nueva forma -digital y virtual- de difundirse, pero las responsabilidades de lo que en sus páginas WEB se diga o informe siempre serán imputable al periodista, editor o director de un específico medio de prensa, de la misma manera que lo sería en base a la publicación del diario en soporte papel".[53]

3.5. CONSIDERACIONES SOBRE LA VULNERACION A CIERTOS DERECHOS EN EL USO DE LA LIBERTAD DE EXPRESION Y DE INFORMACION A TRAVES DEL INTERNET

Es comprensible el deseo de muchas personas de proteger a los usuarios (tanto adultos como niños) que navegan por Internet (que cada vez son más y más jóvenes) del contenido de los numerosos nodos violentos o pornográficos, de proteger su indemnidad sexual, así como el respeto a la vida privada y a la intimidad tanto personal como familiar, es decir, el derecho a la privacidad, a la intimidad, como un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona que sólo a ésta le incuben. Es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas o injerencias externas en ciertas áreas reservadas del ser humano como son: el derecho a la inviolabilidad de la comunicaciones privadas, el derecho a la propia imagen, el derecho al honor, el derecho a la privacidad informática, el derecho a no ser molestado entre otros.

Así pues el derecho al respeto a la vida privada o intimidad, al honor e incluso a la propia imagen, son considerados ya como derechos humanos fundamentales,

---

[52] JIJERA LEIVA, *Op cit.*
[53] *Idem*

establecidos por diversos instrumentos internacionales como son la Declaración Universal de los Derechos Humanos aprobada por la Asamblea general de las Naciones Unidas en 1948, el Pacto Internacional de Derechos Civiles y Políticos de 1966, la Convención Americana sobre Derechos Humanos de 1969, y en la Convención sobre los Derechos del Niño de 1989, instrumentos todos estos firmados y ratificados por nuestro país (cabe señalar que también existen otros instrumentos que establecen este derecho como son: la Convención de Roma para la protección de los Derechos Humanos y las Libertades Fundamentales de 1959, la Declaración de los Derechos y libertades fundamentales aprobadas por el parlamento europeo y la Carta Africana de los Derechos del Hombre y de los Pueblos de 1981 y de los que México no es parte.) a saber:

DECLARACION UNIVERSAL DE LOS DERECHOS HUMANOS (1948)

En su artículo 12 establece que nadie será objeto de injerencias arbitrarias en su vida ; privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques.

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLITICOS (1966)

En su artículo 17 establece las mismas disposiciones que el artículo 12 de la Declaración Universal de los Derechos Humanos y en su artículo 19 al hablar de la libertad de expresión señala que el ejercicio de ese derecho entraña deberes y responsabilidades especiales por lo que podrá estar sujeto a ciertas restricciones fijadas por la ley y que sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás, así como para proteger la seguridad nacional, el orden público, la salud o moral públicas.

CONVENCION AMERICANA SOBRE DERECHOS HUMANOS (1969) -PACTO DE SAN JOSÉ-

El artículo 11 se refiere a que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación. Y establece también el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques. El artículo 13 establece la libertad de pensamiento y expresión determinando que no deberá existir previa censura, pero que el ejercicio de esos derechos estará sujeto a responsabilidades ulteriores, mismas que deberán estar expresamente fijadas por la ley y, que deberán tender a asegurar entre otras cuestiones, el respeto a los derechos o a la reputación de los demás.

CONVENCION SOBRE LOS DERECHOS DEL NIÑO (1989)

En su artículo 16 menciona que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación; y que el niño tiene derecho también a la protección de la ley contra esas injerencias y ataques.

En lo que respecta a nuestra legislación constitucional podemos decir que la tutela de la vida privada se desprende del contenido de los artículos 6°, 7° y 16 de la Constitución que establecen:

Artículo 6. Que la libertad de expresión tiene como límite el respetar los derechos de tercero.

Artículo 7. Que la libertad de imprenta tiene como límite el respetar la vida privada.

Artículo 16. Que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones sino en virtud de mandamiento escrito de autoridad competente que funde y motive la causa legal del procedimiento. Dicho artículo

también establece la inviolabilidad del domicilio, así como la inviolabilidad de las comunicaciones privadas y de la correspondencia

Es evidente que la protección de la vida privada frente a actos de las autoridades se encuentra debidamente instituida en el primer párrafo del artículo 16 constitucional al señalar que para que una injerencia de la autoridad en nuestra intimidad sea válida ésta deberá provenir de una orden de una autoridad facultada por la propia ley para realizar dicha intervención plasmada por escrito, la cual deberá estar debidamente razonada y justificada además de estar prevista en una ley el acto de molestia en cuestión.

Lo mismo ocurre con la intervención de comunicaciones privadas por los diversos medios ya que nuestra constitución establece condiciones, casos y requisitos en los que el Estado puede realizar dicha intervención (aunque debemos decir que estos todavía son insuficientes y faltan precisarse ciertas situaciones y reglamentar mejor dichas intervenciones).

El problema fundamental se encuentra cuando la intimidad o privacidad del ser humano, su honor, su imagen o su indemnidad sexual se ven vulnerados por particulares y concretamente por el exceso en el ejercicio de la libertad de expresión o del derecho a la información. Es decir, cuando con motivo del ejercicio de la libre expresión de las ideas o de la actividad informativa se vulnera la esfera privada del individuo.

Esto ocurre debido a la ambigüedad de los términos que manejan tanto el artículo 6° como el 7°, ya que ninguno de los dos establece cuándo la libertad de expresión afecta los derechos de tercero o cuándo la libertad de imprenta puede llegar a vulnerar la vida privada. El único criterio objetivo que de ellos podría desprenderse es la limitante relativa a que con la libertad de expresión no se cometa algún delito. Con lo cual nos veríamos remitidos a los códigos penales para saber en qué casos el

abuso de la libertad de expresión encuadra en algún tipo penal específico (difamación, calumnia, injurias, etc.).

En la legislación mexicana existen algunos otros supuestos en los que se pone de manifiesto la posible interferencia de la libertad de expresión, con otros valores jurídicos. Por ejemplo el delito de corrupción de menores, si no existiera limitación jurídica al respecto, podía alegarse que se está haciendo uso de la libertad de expresión al mostrar mediante anuncios impresos o electrónicos actos de exhibicionismo corporal, lascivos o sexuales con uno o más menores de dieciocho años. En virtud de que éstas representan un ataque a los derechos de terceros, es perfectamente válido tipificar las mencionadas conductas como contrarias a la ley.

En cuanto a la provocación de algún delito, es justamente la limitación a la libertad de expresión relativa, la que permite considerar como corresponsable y autor de una conducta ilícita penal a quien incita a otro a cometerla. Pensamos que toda la autoría intelectual en materia penal se haría nugatoria si la llamada libertad de expresión se expandiera sin límites jurídicos; bastaría con alegar que se había hecho uso de dicha libertad para pedir a otro que cometiera un determinado delito y que sólo a quien lo cometió debería exigírsele responsabilidad penal.

Y áunque es cierto que es cierto que determinados límites a las libertades de expresión y de información ya han sido reconocidos legal y legítimamente por una gran cantidad de Estados en diversos instrumentos internacionales, de los cuales México es parte tales como:

A) LA DECLARACION UNIVERSAL DE DERECHOS HUMANOS

Artículo 19

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Artículo 29

2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.

3. Estos derechos y libertades no podrán en ningún caso ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas.

B) EL PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS

Artículo 19

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Artículo 20

1. Toda propaganda en favor de la guerra estará prohibida por la ley.

2. Toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley.

C) LA CONVENCION SOBRE LOS DERECHOS DEL NIÑO

Artículo 13

1. El niño tendrá derecho a la libertad de expresión; ese derecho incluirá la libertad de buscar, recibir y difundir informaciones e ideas de todo tipo, sin consideración de fronteras, ya sea oralmente, por escrito o impresas, en forma artística o por cualquier otro medio elegido por el niño.

2. El ejercicio de tal derecho podrá estar sujeto a ciertas restricciones, que serán únicamente las que la ley previa y sean necesarias.

a) Para el respeto de los derechos o la reputación de los demás; o

b) Para la protección de la seguridad nacional o el orden público o para proteger la salud o la moral públicas.

D) LA CONVENCION INTERNACIONAL SOBRE LA ELIMINACION DE TODAS LAS FORMAS DE DISCRIMINACION RACIAL

Artículo 4

Los Estados partes condenan toda la propaganda y todas las organizaciones que se inspiren en ideas o teorías basadas en la superioridad de una raza o de un grupo de personas de un determinado color u origen étnico, o que pretendan justificar o promover el odio racial y la discriminación racial, cualquiera que sea su forma, y se comprometen a tomar medidas inmediatas y positivas destinadas a eliminar toda incitación a tal discriminación o actos de tal discriminación, y, con ese fin, teniendo

debidamente en cuenta los principios incorporados en la Declaración Universal de Derechos Humanos, así como los derechos expresamente enunciados en el artículo 5 de la presente Convención, tomarán, entre otras, las siguientes medidas:

a) Declararán como acto punible conforme a la ley toda difusión de ideas basadas en la superioridad o en el odio racial, toda incitación a la discriminación racial, así como todo acto de violencia o toda incitación a cometer tales actos contra cualquier raza o grupo de personas de otro color u origen étnico, y toda asistencia a las actividades racistas, incluida su financiación;

b) Declararán ilegales y prohibirán las organizaciones, así como las actividades organizadas de propaganda y toda otra actividad de propaganda, que promuevan la discriminación racial e inciten a ella, y reconocerán que la participación en tales organizaciones o en tales actividades constituye un delito penado por la ley;

E) LA CONVENCION AMERICANA SOBRE DERECHOS HUMANOS

Artículo 13

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a. el respeto a los derechos o a la reputación de los demás, o

b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de

información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

Sin lugar a dudas, también es cierto lo importante que sería contar con una legislación reglamentaria específica y apropiada que estableciera de manera clara y con un criterio objetivo lo que comprende la vida privada o ámbito íntimo del individuo para así poder establecer con precisión los límites de estos dos derechos que en ocasiones parecen confrontarse estableciéndose una lucha entre la libertad de expresión y el derecho a la intimidad.

El tema del respeto a las comunicaciones privadas es también un asunto importante pues, a últimas fechas y debido a los avances de la tecnología se han dado bastantes casos en los que comunicaciones de carácter privado entre dos personas han sido interceptadas y lo que es peor hechas publicas y dadas a conocer a través de medios de comunicación, afectando severamente la reputación e imagen de quienes en ellas participaron, sin que se hayan fincado, hasta ahora, responsabilidades por esos actos[54].

[54] Actualmente en México sólo existe unainciativa de refrmas y adiciones sobre diversas disposiciones del Código Penal para el Distrito Federal en Materia de Fuero Común, y para toda la República en Materia de Fuero Federal en donde se sancionan

Considero que la conducta del Estado en lo que respecta a la protección de la vida privada en sus múltiples aspectos no debe concretarse únicamente a una conducta pasiva, es decir, a un no hacer, y a respetar esas áreas destinadas de manera exclusiva al particular como ocurre tradicionalmente en las garantías de libertad, sino que la conducta del Estado debe ser activa como ocurre en las garantías de legalidad, realizando actos y tomando providencias tendientes a evitar la violación de esos derechos, no sólo con respecto a sus autoridades sino también con respecto a otros particulares.

Asimismo es importante mencionar que actualmente existe una definición o mejor dicho un catálogo de actos que se consideran como ataques a la vida privada, contenido en el artículo 1 de la Ley de Imprenta, reglamentaria de los artículos 6 y 7 de la Constitución. Pero es importante decir que la validez de esta ley ha sido cuestionada severamente por múltiples razones entre las que destacan:

El haber sido expedida por Venustiano Carranza, en cuanto Jefe del Ejército Constitucionalista y encargado del Poder Ejecutivo, con dudosas facultades para ello. No es una auténtica "ley" expedida por el Poder Legislativo (Congreso de la Unión). El haber sido emitida el 9 de abril, publicada el 12 de abril y entrado en vigor el día 15 del mismo abril de 1917, fecha en que la Constitución ya había sido promulgada pero aún no entraba en vigor, con lo que no podría de -algún modo regular los artículos de una Constitución que todavía no entraba en vigor, tomando en cuenta que nuestra Constitución comenzó a regir hasta el día 10 de mayo de 1917. Además resulta extraño que Carranza emitiera esa ley como la misma dice: "entretanto el Congreso de la Unión reglamenta los artículos 6 y 7", suena ilógico querer hacer una ley de una "- vigencia tan efímera.

Por otra parte, también es de notarse que Carranza violó la propia Constitución que en sus -artículos transitorios (SEXTO y DECIMOSEXTO) estableció que

---

dichos actos (art. 167 frac. VI, 173, 174).

correspondería al Congreso Constitucional expedir las leyes relativas a Garantías Individuales en el periodo ordinario de sesiones que iniciaría el 1°. de septiembre de 1917.

Por otro lado, y respecto al catálogo que dicha ley establece como ataques a la vida privada y a todo el contenido de dicha ley, el mismo ha sido catalogado generalmente como obsoleto y que debe ser revisado y actualizado adecuándolo a nuestra época.

Aunque ha sido muy cuestionada esta ley, como ya se ha mencionado, debemos apuntar que la Suprema Corte la ha declarado válida hasta en tanto el Congreso de la Unión no expida una nueva que venga a sustituirla, Sin embargo, en la práctica dicha norma es letra muerta, pues realmente no se aplica prácticamente en ninguna parte.

Por lo anterior, considero que sería importante contar con una legislación emitida por el Congreso de la Unión[55], que precisara de mejor manera estas cuestiones, aclarando que no deberá tratarse de una ley mordaza que impida a la prensa y a los medios desempeñar su función informativa, pero sí de sujetar estas actividades al orden jurídico y al respeto a los derechos fundamentales de todos los ciudadanos. No se trata de coartar la libertad de expresión sino de evitar el abuso que pueda hacerse de este derecho, fincando de manera clara las responsabilidades conducentes una vez ejercida en exceso esa libertad de expresión y de información pues recordemos que libertad sin responsabilidad es libertinaje.

Así pues, es importante reglamentar el derecho a la información[56] y el derecho al honor, a la intimidad, y a la imagen propia delimitando bien las fronteras entre unos y

---

[55] Vgr. La Ley Española, La Ley Orgánica 1/1982 de 5 de Mayo de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

[56] Actualmente se encuentra en vigor la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en la primera sección del Diario Oficial de la Federación el martes 11 de junio de 2002.

otros y estableciendo los medios para salvaguardarlos y para restituir a los afectados cuando estos hubieren sido vulnerados.

Otro aspecto digno de comentarse es el relativo a la responsabilidad civil consistente en la obligación de la reparación del daño moral cuando se infringe el honor, la imagen o la dignidad de una persona. Al respecto el artículo 1916 del Código Civil Federal establece que "por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad psíquica o física de las personas.

Cuando un hecho u omisión ilícitos produzcan un daño moral el responsable del mismo tendrá la obligación de repararlo mediante una indemnización en dinero con independencia de que se haya causado daño material..., etc.

... El monto o de la indemnización lo determinará el juez tomando en cuenta los derechos lesionados, el grado de responsabilidad, la situación económica del responsable y la de la víctima, así como las demás circunstancias del caso.

Cuando el daño moral haya afectado a la víctima en su decoro, honor, reputación o consideración el juez ordenará a petición de ésta y con cargo al responsable la publicación de un extracto de la sentencia que refleje adecuadamente la naturaleza y alcance de la misma, a través de los medios informativos que considere convenientes. En los casos en que el daño derive de un acto que hay tenido difusión en los medios informativos el juez ordenará que los mismos den publicidad al extracto de la sentencia con la misma relevancia que hubiere tenido la difusión original."

Esta hipótesis normativa del artículo 1916 se debió a una reforma llevada a cabo en 1982[57], y lo que parecía ser un avance en esta materia se vino abajo debido a cuestiones políticas y a que la comunidad periodística sintió que dicha redacción podía lesionar o limitar las garantías de expresión e información previstas en los artículos 6 y 7 constitucionales por lo que al darse esta reforma en el texto del artículo 1916 se introdujo también un artículo 1916 bis. Que delimitó los alcances del daño moral en relación con la prensa y que dice textualmente: "No estará obligado a la reparación del daño moral quien ejerza sus derechos de opinión, crítica, expresión e información en los términos y con las limitaciones de los artículos 6 y 7 de la Constitución General de la República..."

Como podemos apreciar este último artículo que se agregó tiene nada más un sentido político y demagógico, pues como ya mencionamos, los artículos 6 y 7 tienen como límites el respeto a la vida privada y el no atacar derechos de terceros y lo que pretendió hacer la reforma de 1982 al modificar el artículo 1916 era establecer con claridad la reparación del daño moral cuando se ataca precisamente la vida privada y los derechos de terceros(???).

En esta tesitura, considero que sería oportuno tomar en cuenta lo que otros países ya han hecho en lo que respecta a esta materia y que consagran en sus Constituciones como derechos fundamentales de manera expresa el derecho a la intimidad, al honor y a la propia imagen. Entre ellos podemos encontrar a Alemania, Austria, Finlandia, Portugal, Suecia, España y Estados Unidos.

Atento a todo lo anterior, también considero que sería muy importante incluir en nuestro texto constitucional de manera expresa como garantía individual el derecho a la intimidad personal y familiar y el respeto al honor y a la propia, imagen contra actos no sólo de las propias autoridades sino también de otros particulares que en el ejercicio indebido y excesivo de sus derechos y libertad de expresión e información

[57] Reforma al Código Civil, publicada en el Diario Oficial de la Federación el 31 de diciembre de 1982.

pudieran transgredir esos derechos fundamentales relativos a la vida privada.

De igual forma considero que es necesaria la creación de una ley o conjunto de éstas que regulen de manera clara y objetiva los límites de estos derechos estableciendo de manera puntual lo que se considera vida pública y vida privada, que regulen de forma completa todo lo relativo a la recopilación, manejo, uso e información de datos sensibles (entendiendo por estos todos aquellos que revelen cuestiones de origen racial, étnico, opiniones y preferencias políticas, convicciones religiosas, filosóficas o morales, afiliaciones partidistas o sindicales, cuestiones de salud, vida sexual, etc.), inviolabilidad de comunicaciones de todo tipo (por vía verbal directa, escrita, telefónica, telegráfica, postal, electrónica, etc.), estableciendo las sanciones correspondientes por vulnerar dichos derechos y fijando de manera precisa el procedimiento para la reparación del daño causado y las medidas necesarias para restituir al afectado en su imagen y reputación.

Deberán establecerse, a su vez, en legislación secundaria los procedimientos para que mediante la acción de "protección de datos personales" se le dé a conocer a la persona la información que sobre ella se encuentre en archivos, registros o bancos de datos públicos o privados y la finalidad de estos, así como también para que la persona pueda exigir su rectificación, actualización, inclusión, complementación, reserva, suspensión o cancelación (cabe señalar que al respecto existe ya una minuta con proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos[58]: Personales que actualmente se encuentra en análisis y que sería oportuna su aprobación).

Es cierto que los derechos señalados se han visto afectados en el uso de Internet, sin embargo, también es comprensible la preocupación de aquellos que defienden la libertad en la Red y que temen que se institucionalicen determinados instrumentos

[58] Legislatura LVIII, Año 2, Periodo 2, Núm. Gaceta 55, Fecha 30 de Abril de 2002. Se aprobó en votación nominal por 92 y ninguno en contra. Pasó a la Cámara de Diputados para sus efectos constitucionales.

potencialmente útiles para la censura señalando la violación a estos derechos como excusa. Los filtros de contenidos están en el punto de mira[59].

Internet a fin de cuentas es una herramienta tecnológica o telemática en la que se pueden transmitir datos, documentos, imágenes y sonidos de diversa naturaleza o contenido, sean lícitos o ilícitos, morales o inmorales, permitidos o prohibidos, benignos o nocivos. Esta es una característica de la esencia de la red, sin embargo, la interrogante sería: ¿debe dejarse una total libertad de expresión en Internet o es necesario establecer mecanismos de control y censura para determinados tipos de servicios y contenidos?. Dicho de otra forma, lo que debe buscarse es un adecuado equilibrio entre esta garantía de la necesaria libre circulación de la información -en definitiva un derecho tan fundamental como la libertad de expresión- y la protección del interés público, sin que existan a priori prácticas de censura arbitraria y abusiva pero trazar una línea divisoria puede no ser tan fácil atendida la naturaleza y las características de Internet.

La cuestión se traduce en determinar para la difusión virtual de contenidos ilícitos, limitantes de alguna naturaleza (tanto jurídicos como técnológicos) a la libertad de expresión y de información, lo cual ayudará a disminuir dichos contenidos, y poque que no? hasta los nocivos, a fin de lograr que el internet cada vez más sea un espacio seguro de navegación.

[59] TUYA, Melisa, *Control de Contenidos en Internet, ¿niñeras o censores?*, 5 de abril de 2002. www.baquia.com

CAPITULO IV
ESFUERZOS JURIDICOS CONTRA LOS CONTENIDOS ILICITOS Y NOCIVOS DEL INTERNET

4.1. PANORAMA INTERNACIONAL

A principios de los años 90's primero las empresas y luego los particulares se incorporan paulatinamente a las redes digitales. Pronto llegaría al gran público[60].

A partir de este momento, los usuarios -profesionales o no- podían crear sus páginas web y hacer uso de los servicios de Internet.

Pero con ello, la Red se convierte también en el vehículo ideal para todo tipo de abusos. Los valores jurídicos protegidos son objeto de nuevas formas de ataque en las redes digitales y las consecuencias trascienden las fronteras de los Estados.

El desarrollo increíblemente acelerado que los medios de comunicación, y en especial la Internet y la World Wide Web (WWW), han sufrido en los últimos años supone nuevos retos en la disciplina del Derecho. Las estructuras jurídicas, que de por sí pueden considerarse como cada vez más discordantes con la realidad, han quedado severamente cuestionadas frente a la evolución de dichos medios de comunicación. Ello se debe, entre otros motivos, a que nuestras normas no fueron diseñadas para regular un mundo virtual, sino una realidad "con los pies puestos en la tierra"; y, por otro lado, debido a la dificultad de ajustar las normas operantes a una nueva realidad que se encuentra en constante evolución, con lo que pudiera esperarse que la incertidumbre jurídica no sólo permanezca sino que vaya en aumento de una forma sorprendente.

[60] MARIN PEIDRO, Lucia, *Ob cit.* p. 24.

El manejo y transferencia de la información a cualquier nivel representa un importante porcentaje en el funcionamiento adecuado de la economía mundial en donde la especialización y la interdependencia de los Estados se define cada vez más.

A nivel mundial se hace manifiesta la preocupación respecto al Flujo de Datos Fronterizos, en virtud a su trascendencia en estratos escenciales. El problema radica en la posibilidad de limitar, o en su caso favorecer la circulación de datos a través de las fronteras nacionales dependiendo de los beneficios o afectaciones que esto pueda traer consigo, a los demás Estados de la comunidad internacional.

La preocupación comienza a manifestarse a mediados de los años 90's. Entidades e instituciones públicas y privadas se reúnen en foros internacionales para debatir el problema, alarmados por el incremento de nuevas vulneraciones de los derechos de los usuarios en Internet. Las Red se expande y los contenidos ilícitos y nocivos aumentan en cantidad y en intensidad.

Las primeras demandas por contenidos ilícitos se plantean en 1993 en los Estados Unidos[61]; dos años más tarde, también en Europa[62].

Algunos Estados intentan resolver la cuestión cuando se plantea el caso ante los tribunales[63]. Otros dictan leyes específicas para combatir los efectos perjudiciales de los contenidos ilícitos y nocivos -en ocasiones, sin éxito[64]-, adaptan sus legislaciones para atajar el problema[65] o simplemente aplican la legislación existente[66]. El objetivo es perseguir y castigar a los responsables de los ataques a valores jurídicos

[61] Sentencia *playboy v Frena* (1993).
[62] Caso *Compuserve* (1995).
[63] Francia, Alemania, Reino Unido.
[64] Francia, Estados Unidos.
[65] Reino Unidos, España, Irlanda.
[66] Austria.

protegidos. Se hace necesario definir qué conductas no se pueden tolerar, instrumentar nuevos medios para perseguir a los infractores y delimitar la responsabilidad de los actores. Para ello no sirven los criterios tradicionales. Urge elaborar nuevas respuestas que salvaguarden al mismo tiempo las libertades fundamentales: libertad de expresión y derecho a la información, derecho al secreto de las comunicaciones y a la intimidad de los usuarios.

Los Estados pronto se dieron cuenta de que el carácter transnacional y descentralizado de Internet y la ausencia de control la convertían en un medio de comunicación privilegiado para todo tipo de actividades delictivas.

Una regulación nacional no es suficiente para dar respuesta a un problema que es, por naturaleza, global. Por esta razón, los foros internacionales han reaccionado en la búsqueda de soluciones que propicien el equilibrio entre los usos lícitos de Internet y la protección de la sociedad frente a la utilización abusiva de las redes digitales.

Gobiernos se muestran dispuestos a luchar más eficazmente contra los contenidos ilícitos y la sanción de los culpables fomentando al mismo tiempo el desarrollo del comercio electrónico. Las asociaciones de proveedoreso prestadores de servicios rechazan cualquier tipo de responsabilidad por los actos ilícitos y nocivos de sus clientes para no perjudicar su actividad comercial. Las asociaciones a favor de la libertad de expresión reivindican el derecho de los internautas a la libre circulación de la información, el derecho al secreto de las comunicaciones privadas, el derecho a la intimidad y al anonimato. Las asociaciones de padres, educadores, y las ONGs de protección de la infancia y de la dignidad humana reclaman el castigo y la persecución de los responsables y el derecho a hacer de la Red un medio seguro para los menores. Finalmente, las asociaciones de protección de los derechos de autor solicitan vías eficaces para hacer valer sus derechos frente a las vulneraciones que se están produciendo en la Red.

Este debate ha desembocado en propuestas legislativas en el seno de la Unión Europea que serán implementadas en los Estados miembros.

Para controlar a quienes así actuan en Internet, algunos Estados, como ya se señalaba, han elaborado ya normas específicas, otros han modificado sus leyes para adaptarlas al entorno digital, y otros han aplicado la legislación existente. Sin embargo, las actividades delictivas que se cometen en las redes digitales tienen una clara dimensión internacional. Los contenidos ilícitos, desde el momento en el que se introducen en la Red, son accesibles desde cualquier ordenador del mundo conectado a Internet. Por eso resulta necesario abordar la regulación de los contenidos ilícitos desde instancias internacionales para luchar eficazmente contra las consecuencias transnacionales de los contenidos ilícitos y nocivos. Las soluciones se centran en aumentar la cooperación con la justicia y la policía para perseguir y castigar a los responsables de los contenidos perniciosos en la Red.

La cumbre de ministros de Interior y Justicia de la Unión Europea celebrada en Estocolmo logró el compromiso de los "Quince" de adaptar sus legislaciones penales a la idea común de prohibición de la pornografía infantil. Hasta ahora, en buena parte de los sistemas judiciales europeos, el tratamiento penal de las imágenes obscenas que tienen a los menores como forzados protagonistas, limita su castigo a la difusión, exhibición o comercialización, entendiendo que la simple tenencia de ese material había de quedar fuera de toda sanción penal. Tal planteamiento obedecía a un trasnochado enfoque que veía en el consumo de pornografía infantil una lícita opción fruto del ejercicio de la libertad personal.

La decisión ahora adoptada por la Unión Europea no es ajena a la multiplicación de usuarios de Internet, un fenómeno expansivo que ha desbordado todas las previsiones y que cuenta a su favor con el anonimato que permite la utilización de fórmulas de encriptación ofrecidas por las nuevas tecnologías. Está fuera de dudas

que la dignidad de la infancia, la naturaleza de los valores en juego y, en fin, el impacto que en el proceso de formación de un niño puede provocar su sometimiento a sevicias sexuales, imponen y justifican el cambio de orientación legislativa[67].

En Europa se han dado una serie de propuestas con el fin de solucionar el problema del contenido nocivo para menores o el contenido ilícito que atenta contra la dignidad del hombre.

La Unión Europea ha sido consciente, desde el año 1994, de la necesidad de proporcionar una respuesta supranacional a la hora de combatir los contenidos ilícitos en Internet. De este modo, todas las instituciones (Consejo, Comisión y Parlamento) han asumido un papel activo para desarrollar esta tarea. [68]

En abril de 1996[69], el Consejo de Telecomunicaciones se reúne en Bolonia para determinar si los contenidos en Internet deben ser regulados. El Consejo de Ministros le pide a la Comisión que examine los problemas éticos que se suscitan en las redes digitales[70] y, meses más tarde, que decida si la regulación de los contenidos debe ser internacional o comunitaria.

La Comisión recoge el testigo y publica en octubre de ese mismo año dos textos clave: la *Comunicación sobre contenidos ilícitos y nocivos en Internet*[71] y el *Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*[72]. Son documentos complementarios que plantean las estrategias jurídicas y políticas que debe tomar la Unión Europea, La Comunicación es una reflexión sobre las soluciones que se pueden adoptar para

[67] Consultar web La Rioja.
[68] Pregunta escrita B4-0224/94, del Sr. Van der Waal sobre pornografía informática de 16 de diciembre de 1994.
[69] Reunión del Consejo de Telecomunicaciones en Bolonia (Italia) los días 24 y 25 de abril de 1996.
[70] Reunión del Consejo de Telecomunicaciones el día 27 de septiembre de 1996.
[71] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre contenidos ilícitos y nocivos en Internet. COM (96) 487 Final, de 16 de octubre de 1996. La Comunicación es aprobado por Resolución del Consejo y de los representantes de los gobiernos de los estados miembros reunidos en el seno del Consejo de 17 de febrero de 1997 sobre los contenidos ilícitos y nocivos en Internet. 97/C 70/01 (DO C 70, de 6 de marzo de 1997).
[72] Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de

resolver los nuevos problemas que plantea Internet, mientras que el Libro Verde estimula un debate público para definir los problemas de fondo y el camino que deben seguir las partes implicadas.

Resultado de estos documentos fue el Informe elaborado a finales de ese año por el Grupo de Trabajo sobre los contenidos ilícitos y nocivos en Internet que fue presentado al Consejo de Telecomunicaciones[73]. El Informe propone la elaboración de códigos de conducta, líneas directas, un organismo independiente de autoregulación, campañas de información y el desarrollo de mecanismos de filtrado, propuestas que fueron aprobadas por Resolución del Consejo de las Telecomunicaciones el 28 de noviembre de 1996 e incorporadas en 1997 al *Plan de Acción para fomentar la utilización segura de Internet*[74].

Otros documentos siguieron reclamando soluciones en la lucha contra los contenidos ilícitos y nocivos como las ideas recogidas en la *Recomendación relativa a la competitividad de la industria europea*[75] *de 24 de septiembre de 1998 dirigida a los Estados miembros, a la industria y a otros sectores interesados.*

A diferencia de lo que sucede en otras instancias supranacionales, las instituciones comunitarias son conscientes de que la lucha contra los contenidos perniciosos no queda resuelta únicamente con una declaración de intenciones, sino que se necesita de un soporte económico para materializarlas. Así, el *Plan Plurianual para promover e uso seguro de Internet*[76] de enero de 1999 concede un presupuesto de 25 millones de euros para hacer efectivas las propuestas.

---

información. COM (96) 483 Final, de 16 de octubre de 1996.

[73] Informe del Grupo de Trabajo sobre los contenidos ilícitos y nocivos en Internet presentado al Consejo de Telecomunicaciones el 28 de noviembre de 1996.

[74] Comunicación de la Comisión al Parlamento, al Consejo, al Comité Económico y Social y al Comité de las Regiones sobre el Plan de Acción para promover el uso seguro de Internet, COM (97) 582 Final/97/0337, de 26 de noviembre de 1997.

[75] Recomendación del Consejo de 24 de septiembre de 1998 relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana (DO C L270, de 7 de octubre de 1998).

[76] Decisión núm. 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba el Plan Plurianual de Acción Comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales (DO L 033, de 6 de febrero de 1999).

El texto más reciente es de diciembre de 1999, *las Conclusiones del Consejo sobre la protección de los menores ante el desarrollo de los servicios audiovisuales digitales*[77] que pide a los Estados miembros que supervisen la eficacia de sus sistemas de protección de menores e intensifiquen sus esfuerzos en el establecimiento de medidas educativas y de concienciación; que reúnan a la industria y a las partes afectadas a fin de estudiar cómo se puede dar más transparencia a los métodos de calificación moral de los contenidos; y que prosigan sus trabajos con vistas a promover la puesta en marcha de la Recomendación relativa a la competitividad de la industria europea de 24 de septiembre de 1998.

Los trabajos del Consejo y de la Comisión se completan con las resoluciones del Parlamento Europeo contra el racismo y la xenofobia, el antisemitismo, la trata de mujeres, la pornografía, la pederastia y el terrorismo en las redes digitales.

Los principios subyacentes en los trabajos de las instituciones comunitarias reflejan la tensión entre los principios comunitarios (mercado interior, normas de competencia y libre prestación de servicios) y los principios generales (protección de menores, libertad de expresión y derecho a la intimidad). Los Estados miembros sólo pueden limitar la libre prestación de servicios en base a la protección de los menores si la medida es proporcionada.

Veamos sin ánimo exhaustivo los siguientes esfuerzos legislativos de carácter internacional más destacados:

[77] Conclusiones del Consejo, de 17 de diciembre de 1999, sobre la protección de menores ante el desarrollo de los servicios audiovisuales digitales. COM 2000/C/06 (DO C 8, de 12 de enero de 2000).

4.1.1. EL LIBRO VERDE SOBRE LA PROTECCION DE MENORES Y LA DIGNIDAD HUMANA EN SERVICIOS AUDIOVISUALES E INFORMATIVOS

Mediante carta de 23 de octubre de 1996, la Comisión transmitió al Parlamento Europeo una comunicación sobre los contenidos ilícitos y nocivos en Internet (COM (96) 0487), el Libro Verde trata acerca de la protección de menores y la dignidad humana en servicios audiovisuales e informativos (C4-0592/96), el informe del grupo de trabajo de la DG XIII acerca de contenidos ilegales y ofensivos en Internet y la Resolución sobre las comunicaciones (COM 96-0487) y (C4 0592/96) adoptadas el 24 de abril de 1997 por el Parlamento Europeo. Los textos reflejan el espíritu con el que está inspirándose el Parlamento Europeo en relación con estos temas.

Entre algunos de los principios que se desprenden de estos textos:

A. El no molestar a nadie por sus opiniones y apoyar la libre comunicación de pensamiento y opiniones como derecho fundamental en todas las sociedades democráticas.

B. Establecer que el derecho a la libertad de expresión es imprescriptible y que la libertad de cada persona comienza ahí donde termina la de los demás.

C. Señalar que el respeto a la integridad de la persona, en particular la protección de los niños, reviste importancia fundamental.

D. Considerar que la pornografía infantil es un grave delito contra los niños porque constituye un documento visual o escrito de abusos reales contra éstos.

E. Establecer que toda persona tiene derecho a la confidencialidad de su correspondencia y que el correo electrónico está sujeto a este mismo derecho.

F. Reconocer que en los medios de comunicación siempre han existido contenidos ilícitos y nocivos, pero que la informática en red se caracteriza por ser un medio de comunicación sin comunicadores y sin fronteras, por lo que su control por parte de los Estados y de los gobiernos es difícil o imposible.

G. Considerar que aunque la prevención, y en su caso la represión, de la difusión de mensajes de contenido condenable (perversiones pornográficas) sea competencia de los Estados miembros en virtud del ejercicio de sus poderes de policía, la Unión Europea no puede desinteresarse de estos problemas tan estrechamente vinculados a las libertades públicas.

H. Señalar que la telemática puede fácilmente transportar a domicilio atentados contra la dignidad humana y alentar comportamientos susceptibles de sanción penal, por lo que son indispensables, ante todo, la responsabilidad y la capacidad crítica individual y familiar en el uso de la telemática.

I. Considerando que un planteamiento exclusivamente represivo de las redes informáticas, de las cuales Internet sólo es la prefiguración, perjudicaría gravemente la contribución de estas últimas al desarrollo de nuestra sociedad; si bien son necesarias, al mismo tiempo, hay factibles formas de autorregulación.

En virtud de los textos señalados se acuerda, que todos los Estados miembros deben disponer en sus legislaciones nacionales toda la normativa que tipifique delitos como la pornografía infantil, pero deja claro, que las normas nacionales no ofrecen por sí solas una respuesta satisfactoria a los problemas jurídicos planteados por la universalización y el carácter transfronterizo de Internet.

Con relación a la protección de menores del contenido nocivo, el Libro Verde promueve el uso de los sistemas de control familiar del contenido. Igualmente deja claro que dichos sistemas no son del todo suficientes e inclusive promueven la autorregulación.

Con relación a la protección de la dignidad humana (pornografía infantil), señala que los Estados aún no se han puesto de acuerdo; unos creen en la autorregulación, otros promueven campañas agresivas de prevención contra la pornografía infantil.

Posteriormente, se emitió la resolución sobre el Libro Verde relativo a la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información (COM(96)0483 - C4-0621/96). En esta norma se acuerda, que todos los Estados miembros deben disponer en sus legislaciones nacionales toda la normativa que tipifique delitos como la pornografía infantil, pero deja claro, que las normas nacionales no ofrecen por sí solas una respuesta satisfactoria a los problemas jurídicos planteados por la universalización y el carácter transfronterizo de Internet.

Asimismo, insta a la cooperación de los Estados miembros en el marco de la cooperación en los asuntos de justicia e interior y el intercambio de datos que favorezcan las investigaciones, pesquisas para facilitar así la persecución de las infracciones.

Igualmente, pretenden que la Unión Europea establezca un marco coherente y adecuado que defina, concretamente, los principios y objetivos que se deban aplicar y alcanzar, a efectos de la protección de los menores y de la dignidad humana para cada tipo de proveedor de servicios; señala que, en este ámbito, se debe aplicar el principio de que el objetivo de la protección de los menores y la dignidad humana ha de lograrse tanto mediante la imposición de obligaciones

jurídicas mínimas para los proveedores de contenidos como mediante medidas de autocontrol y ayudas para que los consumidores tomen decisiones responsables; asimismo, que las medidas de protección de los menores y de la dignidad humana en los nuevos servicios sólo pueden ser efectivas si se coordinan a nivel mundial.

Con relación a la protección de la dignidad humana (pornografía infantil), señala que los estados aún no se han puesto de acuerdo; unos creen en la autorregulación, otros promueven campañas agresivas de prevención contra la pornografía infantil.

Pide que se impongan a los proveedores o prestadores de acceso y desarrolladores de contenidos las siguientes obligaciones jurídicas mínimas:

- Responsabilidad ilimitada y, en su caso, penal respecto de los contenidos puestos a disposición por ellos mismos;

- Responsabilidad respecto de los contenidos ajenos, sancionables penalmente, que hagan accesibles, si conocen positivamente su contenido concreto y tienen la posibilidad técnica de impedir su utilización.

- Establecimiento de órganos de libre autocontrol y códigos de conducta públicos que permitan tomar decisiones en los casos de contenidos, que sin ser sancionables penalmente, puedan afectar a la protección de los menores y la dignidad humana;

Por ello la seguridad en la Red ha sido desde los comienzos de su utilización, uno de los principales puntos de preocupación de los usuarios, así como de las empresas y de los Gobiernos.

En ese sentido, y dada la facilidad con la que se puede acceder a cualquier página web o intercambiar archivos pornográficos que afecten el desarrollo del menor o la libre circulación de contenidos totalmente ilícitos, es que existen algunos intentos por parte de algunos gobiernos de controlar el contenido que circula en ella, así como la intención de las empresas de autorregularlo.

Vint Cerf, uno de los padres fundadores de la Internet, está preocupado por los planes de la Unión Europea de establecer nuevas reglas para combatir el delito informático, que podrían chocar contra las actuales normas sobre defensa de la intimidad.

Cerf, quien a comienzos de la década de los 70's colaboró en el desarrollo de la Internet, dice que una red de sistemas más seguros es una prioridad inmediata para el desarrollo exitoso de la Red.

4.1.2. RESOLUCION DEL CONSEJO DE TELECOMUNICACIONES SOBRE CONTENIDOS ILICITOS Y NOCIVOS EN INTERNET

Posteriormente, la comisión transmitió al Parlamento Europeo "La comunicación sobre contenidos ilícitos y nocivos en Internet" (COM (96) 0487 y C4 0592/96), adoptada por el Parlamento Europeo con fecha 24 de abril de 1997, y con fecha 17 de Febrero de 1997 fue adoptada formalmente "La Resolución del Consejo de Telecomunicaciones sobre contenidos ilícitos y nocivos en Internet". En ambos documentos se insta a los Estados miembros a que pongan en marcha las siguientes medidas:

A. Fomentar y facilitar sistemas de autorregulación, que incluyan instancias representativas de los suministradores y usuarios de los servicios de Internet,

códigos de conducta eficaces y, eventualmente, mecanismos de información de emergencia accesibles al público;

B. Fomentar el suministro a los usuarios de mecanismos de filtro y alentar la creación de sistemas de evaluación; por ejemplo, debería fomentarse la norma PICS[78].

C. Debe primar el equilibrio entre la garantía de la libre circulación de la información y la protección del interés público.

Los proveedoreso desarrolladores de contenidos son responsables de sus acciones. Esto, además de ser un principio generalmente admitido en una gran cantidad de ordenamientos jurídicos, lo recuerda la Comisión Europea en su *Comunicación sobre contenidos ilícitos y nocivos en Internet* de 1996. De este modo, un proveedor o desarrollador de contenidos ilícitos es responsable de los contenidos que genera o difunde en Internet a través de cualquiera de las aplicaciones de la Red, ya sea correo electrónico, sitios web o mensajes en los grupos de noticias o listas de distribución.

4.1.3. CONVENIO SOBRE LA DELINCUENCIA EN EL CIBERESPACIO

La actividad más relevante que se ha llevado a cabo bajo los auspicios del Consejo de Europa tiene su origen en abril de 1997, con la creación de un Comité de Expertos de los Delitos en el Ciberespacio (PC-CY) al que se le encarga la elaboración de un *Convenio sobre la Delincuencia en el Ciberespacio* que ha visto a lo largo del año 2000. Este proyecto recoge los trabajos previos que sirvieron de base a la *Recomendación núm. R* (89)9 *sobre la criminalidad en relación con la*

[78] *Platform for Internet Content Selection*, que es un servicio para seleccionar contenidos en Internet que lanzó oficialmente el World Wide Consortim

informática[79] y la *Recomendación núm. R* (95) 13 *relativa a los problemas de procedimiento penal relacionados con la tecnología de la información*[80]. Entre otros aspectos, el Convenio elabora un listado de conductas que deberán ser tipificadas como delitos por los Estados partes del Convenio, genéricamente agrupados en los llamados "delitos informáticos": las conductas delictivas contra la propia Red, esto es, ataques contra los sistemas informáticos y contra la confidencialidad, integridad y disponibilidad de los documentos electrónicos (por ejemplo, los accesos no autorizados -*hacking*-, los daños informáticos -producidos por los virus informáticos-, etc.); delitos ya conocidos en el mundo real, aunque cometidos mediante la utilización de medios informáticos (estafas electrónicas, falsedades documentales, etc.); y finalmente, los delitos relacionados con los contenidos en Internet: la violación de los derechos de propiedad intelectual y la distribución de material ilícito u ofensivo para la dignidad humana. Éstos últimos son llamados "ciber-infracciones" *(Cyber-offences* o *Distribution-of-fences)* y preocupan especialmente a los gobiernos por las dimensiones transnacionales que adquieren en la Red.

No obstante, el proyecto de *Convención sobre Delincuencia en Ciberespacio* se enfrenta con un problema de difícil solución, y éste es la reticencia de los Estados a ceder parte de su soberanía, puesto que quieren conservar la capacidad decisoria sobre qué es ilícito o nocivo. En cualquier caso, el proyecto de Convención es un ejemplo de consenso internacional acerca de la necesidad de abordar la regulación de los contenidos ilícitos en Internet que conjugue el principio de la libre circulación de la información en las redes digitales y la persecución y el castigo de la difusión de información ilegal. Además, la Convención no se limitará a los estados miembros del Consejo de Europa sino que estará abierta a la firma también para estados no miembros.

[79] Recomendación del Consejo de Ministros del Consejo de Europa núm. R (89) 9 sobre la criminalidad en relación con la informática de 13 de septiembre de 1989.
[80] Recomendación del Comité de Ministros del Consejo de Europa núm. R (95) 13 sobre los problemas de procedimiento penal relacionado con la tecnología de la información, de 11 de septiembre de 1995.

4.1.4. DECLARACION MINISTERIAL DE BONN SOBRE LAS "REDES MUNDIALES DE LA INFORMACION"

Entre 1997 y 1998, la Organización para la Cooperación y el Desarrollo (OCDE) ha emprendido iniciativas específicas en materia de lucha contra la pornografía infantil en las redes digitales. Los ministros, en la *Declaración Ministerial de Bonn sobre las "Redes mundiales de la información*[81]*"*, de julio de 1997, coinciden en señalar que es fundamental la cooperación internacional en la lucha contra el uso indebido de la Red.

4.1.5. CONFERENCIA DE ESTOCOLMO CONTRA LA EXPLOTACION COMERCIAL SEXUAL DE LOS MENORES

Quizás el organismo más activo en la lucha contra la pornografía infantil en Internet haya sido la UNESCO, bajo cuyo patrocinio se han celebrado numerosas conferencias internacionales. La primera fue en 1996. La *Conferencia de Estocolmo contra la explotación comercial sexual de los menores* elabora un Plan de Acción en el que se reclama la necesidad de acrecentar la cooperación entre las partes implicadas -autoridades nacionales e internacionales, operadores y usuarios- para que la lucha contra la explotación sexual de los menores sea eficaz, mediante la sanción de la prostitución, tráfico y pornografía infantil, incluyendo la posesión de material pornográfico infantil y otras actividades sexuales ilegales.

[81] Declaración Ministerial de Bonn sobre "Las redes mundiales de la información", Reunión de la OCDE, celebrada en Bonn, los días 6-8 de julio de 1997.

4.1.6. REUNION DE EXPERTOS EN PARIS SOBRE "ABUSO SEXUAL DE MENORES, PORNOGRAFIA INFANTIL Y PEDERASTIA EN INTERNET"

En 1999, la Declaración de la *Reunión de Expertos en París sobre "Abuso sexual de menores, pornografía infantil y pederastia en Internet*[82]" acentúa la necesidad de proteger a los menores frente a los contenidos ilícitos y nocivos que pueden encontrar en la Red, salvaguardando al mismo tiempo las libertades fundamentales (derecho a la libertad de expresión, de información y de protección de la intimidad). Es necesaria la coordinación entre gobiernos, industria, padres y educadores que garantice que los responsables serán perseguidos y castigados. Estas medidas son desarrolladas meses más tarde en la *Conferencia de Viena contra la pornografía infantil en Internet*[83] que insta a los Estados a armonizar sus legislaciones para castigar la distribución, exportación, transmisión, importación, posesión y publicidad de la pornografía infantil así como a suscribir la futura Convención sobre Delincuencia en el Ciberespacio. Se celebró la *Conferencia de Bruselas sobre la lucha contra la pederastia en Internet de* 2000[84]en la que representantes de las partes implicadas han expuesto los logros alcanzados y los métodos que le han resultado eficaces.

[82] Reunión de Expertos sobre "Asunto sexual de menores, pornografía infantil y pederastia en Internet", celebrada en París en enero de 1999.
[83] Conferencia internacional contra la pornografía infantil en internet, celebrada los días 29 de septiembre-1 de octubre de 1999 en Viena, Austria.
[84] Foro internacional sobre la lucha contra la pornografía infantil en Internet. Celebrada el 17 de marzo de 2000 en Bruselas,

4.1.7. PLAN PLURIANUAL DE ACCION COMUNITARIA, PARA PROPICIAR UNA MAYOR SEGURIDAD EN LA UTILIZACION DE INTERNET

La Decisión N ° 276/1999/CE del Parlamento Europeo y del Consejo del 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria, para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales, y que abarcó un periodo de 1 de enero de 1999 al 31 de diciembre del 2002, impulsa las siguientes acciones:

A. Alentar al sector a que impulse el uso de medios de filtros y sistemas de clasificación, que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo y a los adultos decidir que contenidos lícitos desean tener acceso y que tengan en cuenta la diversidad cultural y lingüística.

B. Mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet.

C. Fomentar la autorregulación del sector y los mecanismos de supervisión de los contenidos cuando se refieran a contenidos como la pornografía infantil.

"El Plan Plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet" "tiene como líneas de actuación junto con la recomendación relativa a la protección de los menores y de la dignidad humana, un instrumento para la aplicación de un planteamiento europeo sobre la seguridad en la utilización de Internet, que se basa en la autorregulación del sector, el filtrado y la

---

Bélgica.

clasificación de contenidos así como la sensibilización. Dicho planteamiento ha recibido un claro apoyo del Parlamento Europeo, del Consejo y de los Estados miembros, así como del ámbito europeo más amplio de la Declaración de Bonn, que firmaron los Ministros de veintinueve Estados europeos" .

El texto señala que ésta línea de actuación tiene por objetivo incitar a los interesados (empresas, usuarios) a crear e implantar mecanismos de autorregulación adecuados, plantear la creación de una red europea de "líneas directas" "*hot line*" que permitan a los usuarios notificar los contenidos que hayan encontrado al utilizar Internet y que a su juicio sean ilícitos.

El texto es claro y aparentemente, al destacar que la competencia de perseguir y castigar a los responsables de los contenidos ilícitos siga correspondiendo a las autoridades nacionales policiales y judiciales. Sin embargo, con algunas de las facultades otorgadas a las líneas directas, no sólo pondrán al descubierto la existencia de contenidos ilícitos sino que también podrán restringir su circulación. Considero que ésta circunstancia realizarse a petición de autoridad competente y no a propio criterio del proveedor o prestador de servicios.

En el plan fomento de la autorregulación establece, que el sector debe contribuir con eficacia a la limitación del flujo de contenidos ilícitos y nocivos. Cabe recalcar, que dicha limitación de flujo sólo debe realizarse a petición de autoridad competente, no pudiendo censurarse, por ningún motivo, el contenido nocivo para los menores, pues éste contenido es perfectamente legal .

La autorregulación, tal como se presenta, pareciese una opción viable para solucionar los problemas en Internet, sin embargo, éstos mecanismos de autorregulación se toman la atribución de ser la autoridad oficial procediendo a retirar arbitrariamente el contenido ilícito, sin que se cumpla con un debido proceso

ni se respete el derecho de defensa de la persona que alojó o transmitió el contenido ilícito.

Es que esta "autorregulación" no han tomado en cuenta al usuario o consumidor sino que las empresas toman decisiones en función a sus intereses, censurando el contenido y evitando que el nombre de su empresa se vea perjudicado al estar envuelto en algún proceso de esas índole.

Las organizaciones deberían limitarse a detectar contenidos de pornografía infantil y denunciarlo a la policía con el fin que se realice la investigación correspondiente y sea la autoridad oficial competente quien proceda a dictar sentencia censurando legalmente dicho contenido ilícito y no realizando una censura ilegal y arbitraria.

4.1.8. MEDIDAS DIRIGIDAS A LOS PROVEEDORES DE SERVICIOS DE INTERNET

Con fecha 29 de mayo del 2000 se promulgó la Decisión del Consejo de la Unión Europea que establece una serie de medidas dirigidas a los Proveedores o prestadores de Servicios de Internet para el conocimiento y posterior control por las autoridades competentes, sobre los contenidos con la finalidad de combatir los que son ilícitos en Internet.

La respectiva decisión establece que los Proveedores de Servicios de Internet, deberán informar a las autoridades competentes acerca del material de pornografía infantil del que tengan conocimiento y que se difunda a través de los servicios que prestan; Igualmente, lo facultan para retirarlo, salvo que las autoridades competentes dispongan otra cosa; así mismo le otorgan facultades para la creación

de sistemas propios de control destinados a combatir la producción, el tratamiento, la posesión y la difusión de material pornográfico infantil en la Red.

4.1.9. DIRECTIVA 2000/31/CE DE LA COMUNIDAD EUROPEA SOBRE COMERCIO ELECTRONICO

Durante los años que siguieron las profundas divergencias jurisprudenciales y legislativas que se apreciaron en los Estados miembros entorpecían gravemente el mercado interior constituyendo un obstáculo a la libre prestación de servicios y distorsionando la libre competencia. En respuesta a estas disparidades, y con el fin de proteger el correcto funcionamiento del mercado interior, la Comisión publicó en 1998 una propuesta de Directiva, llamada *"Directiva de Comercio Electrónico"*[85].

La propuesta establece un régimen horizontal de responsabilidad civil y penal de los prestadores de servicios de la sociedad de la información. Este régimen de responsabilidad es único para cualquier tipo de infracción que se pueda cometer en las redes digitales: contenidos pornográficos, difamación, racismo y xenofobia, publicidad engañosa, vulneración de los derechos de autor, competencia desleal, etc. Las exoneraciones de la Directiva de Comercio Electrónico denotan una gran influencia de la ley estadounidense *Digital Milenium Copyright Act* (DMCA), la cual se verá más adelante -relativa a la responsabilidad por violación de la propiedad intelectual- que había entrado en vigor apenas unos meses antes.

Se señala que la eventual responsabilidad jurídica a priori de los ISP depende de tres circunstancias: que sus servidores almacenen datos o contenidos ilícitos; que pueda "suponerse razonablemente" que tienen conciencia de la aparente ilicitud de la naturaleza de la información; y, que no hayan tomado "medidas razonables" para

[85]Propuesta modificada de directiva del Parlamento Europeo y del Consejo, relativa a determinados aspectos jurídicos del comercio electrónico relacionados con el mercado interior. COM (99) 427 Final.

retirar o eliminar esa información. Por cierto, todas son circunstancias a ser calificadas con posterioridad a la eventual comisión de un delito por uno de los usuarios o abonados de un ISP.

Se les han imputado a los proveedores de conectividad responsabilidades por facilitar la distribución de información ilícita, tema también delicado porque aspectos como mejorías en la prestación de servicios o mayores coberturas en el funcionamiento de una empresa ISP podrían interpretarse judicial -y erróneamente- como intentos de facilitación. Analógicamente, tal opción sería equivalente al absurdo de sancionar a las compañías de teléfono por permitir a sus usuarios que se conecten con líneas de conversaciones eróticas o pornográficas.

La propuesta contiene tres supuestos de exoneración de responsabilidad para los proveedores o prestadores de servicios de Internet por los actos ilícitos cometidos por sus clientes.

El primero de ellos se refiere a la exención por la actividad de mero transporte: los proveedores o prestadores de servicios de Internet no se consideran responsables si la actividad que desarrollan consiste en facilitar un acceso a Internet en el que se den las siguientes circunstancias: a) que no haya originado él mismo la transmisión; b) que no seleccione al destinatario de la transmisión; y c) que no seleccione ni modifique los datos transmitidos. Si se cumplen estas condiciones, los proveedores de acceso a Internet no serán responsables civil o penalmente por los contenidos ilícitos y nocivos introducidos en Internet por sus usuarios.

La realización de copias temporales de los contenidos ilícitos también queda exenta, siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones -Internet- y que su duración no supere el tiempo razonablemente necesario para dicha transmisión.

El hecho de que el proveedor de acceso a Internet quede exento de responsabilidad no le libera de las medidas cautelares que le puedan imponer las autoridades judiciales nacionales, obligándole, por ejemplo, a cortar el acceso a la Red del cliente que lleva a cabo la actividad ilícita.

El segundo de estos supuestos alude a la actividad de *caching* llevada a cabo por el proveedor de servicios, que queda exenta de responsabilidad siempre que éste no modifique la información, respete sus condiciones de acceso, respete las normas relativas a su actualización y no interfiera en la tecnología utilizada para obtener datos sobre el uso de la información. Ahora bien, en cuanto el proveedor de servicios tenga conocimiento efectivo de que la información ha sido retirada del lugar de Internet en el que se encontraba inicialmente, o que se ha imposibilitado acceder a ella, o que la autoridad competente ha ordenado su retirada o ha prohibido el acceso, deberá actuar con prontitud para retirar la información o hacer que el acceso a ella sea imposible.

Pero, ¿qué significa que el proveedor o prestador de servicios tenga "conocimiento efectivo de la infracción"? La propuesta de Directiva pretende exigir cierta diligencia al intermediario por las actuaciones llevadas a cabo por los usuarios del servicio, de modo que si el proveedor o prestador de servicios de Internet sabe de las infracciones o puede saberlo y no hace nada para evitarlo, no puede beneficiarse de la limitación de la responsabilidad. En consecuencia, para exigir la responsabilidad a un prestador de servicios, se deberá probar que el proveedor de servicios tuvo conocimiento de la actividad ilícita en el curso de sus actividades normales y no hizo nada para impedirlo, lo cual plantea claramente problemas de prueba.

La tercera se refiere a la exención por la actividad de alojamiento de datos puestos a disposición del proveedor de servicios por el usuario de Internet (por ejemplo, la actividad consistente en albergar páginas web, los grupos de noticias o los foros de discusión). En este caso, los proveedores de alojamiento podrán beneficiarse de la

exoneración de responsabilidad si cumplen dos condiciones: que no tengan realmente conocimiento de que la actividad es ilícita, o que, en cuanto tengan conocimiento del carácter ilícito del contenido que albergan, actúen con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible. Por ejemplo, un proveedor de servicios de Internet tiene conocimiento de que en un sitio web albergado en su sistema se están cometiendo infracciones de; derechos de autor a través de la difusión no autorizada de canciones en formato MP3; para no ser considerado responsable de la violación de los derechos de autor por su cliente, la propuesta de Directiva le exige que actúe con "prontitud" para retirar o bloquear las páginas web infractoras.

Esta circunstacia no afectará el que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miemboros, exija al prestador de servicios poner fin a una infracción o impedirla, ni la posibilidad que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos.

La forma en que está redactada esta última exoneración plantea la temida pregunta:

¿Tienen los proveedores de servicios de Internet la obligación de controlar los contenidos? Los prestadores de servicios de Internet sólo pueden ser responsables si se les impone un deber o se le solicite la vigilancia sobre los contenidos que transitan por sus sistemas informáticos por parte de la autoridad judicial del país, a tenor de los dispuesto en la legislación nacional, cuando resulte necesario para garantizar la seguridad del Estado, la defensa, la seguridad pública para prevenir, investigar, detectar y perseguir infracciones penales.

En esta directiva queda claramente establecida la posición de la Comunidad Europea con relación a la irresponsabilidad del proveedor que brinda el servicio de

servicio y acceso cuando el contenido es de un tercero y la empresa no tenga conocimiento de la ilicitud del contenido. Igualmente faculta a la empresa a retirar el contenido apenas tenga conocimiento.

Considero que debió señalarse que el retiro del contenido debe realizarse a solicitud de la autoridad competente para evitar cualquier tipo de censura privatizada.

4.1.10. INFORME FINAL -INCORE- SOBRE PROPICIAR EL USO SEGURO EN INTERNET: AUTO - ETIQUETADO Y FILTROS

Con fecha 15 de junio del 2000, la Comisión Europea publicó el Informe final INCORE[86] sobre propiciar el uso seguro en Internet: Auto - Etiquetado y Filtros. Este informe tiene como finalidad evaluar la posibilidad de un auto etiquetado y filtro desde una perspectiva europea.

El informe concluye señalando que el auto etiquetado y el sistema de filtros cuentan en Europa con la potencia teórica y técnica de conocer las necesidades de los consumidores de la Comunidad Europea. Agrega, que el sistema será eficiente en la medida que la mayor cantidad de páginas sean etiquetadas. Igualmente, señalan que es mejor que las páginas etiquetadas sean aquellas que afecten el desarrollo del menor y sobretodo aquellas con un elevado tráfico.

4.1.11. CUMBRE CELEBRADA A INSTANCIAS DEL CONSEJO SUPERIOR DEL AUDIOVISUAL FRANCES –CSA- EN COLABORACION CON LA UNESCO

En la cumbre celebrada a instancias del Consejo Superior del Audiovisual francés CSA en colaboración con la UNESCO se planteó en sus propuestas de trabajo previas a la cumbre una serie de posibles líneas de actuación, que tomaban como referencia las distintas experiencias y puntos de vista de Estados, organismos reguladores tanto del audiovisual como de las telecomunicaciones, productores o desarrolladores de contenidos, proveedores de servicios de Internet, usuarios y consumidores, entre otros.

En esta cumbre el CSA recogió la opinión de organismos reguladores de los cinco continentes así como elaboró un informe que sirvió de base para el debate que tuvo lugar en París. En esta cumbre se llegaron a varias conclusiones, entre ellas:

I. En lo que respecta al marco jurídico aplicable a los contenidos audiovisuales difundidos por Internet es que no es urgente adoptar una regulación en esta materia, entre otros porque el Internet no es una zona con regulación, resulta aplicable en este ámbito el common law, y los jueces y las autoridades policiales pueden intervenir; en los Estados Unidos existe jurisprudencia en algunos Estados de casos fijos por la Corte sin el marco legal existente en materia penal. (El Interpol's cyber-patrols ha probado su eficiencia en la Red).

II.Una actuación legislativa precipitada e inadecuada podría dificultar la expansión de estos servicios, y frenar al desarrollo tecnológico y a la creación de nuevos contenidos para Internet.

---

[86] *Incoreintegrated Concept por Groundwater* Remediation, fundado en 1993.

III. Es necesario encontrar un equilibrio entre regulación y la autorregulación. En este punto señala, que la co-rregulación parece ser la opción jurídica más viable:

La (concertación entre las autoridades públicas y el sector privado) parece la solución más apropiada. El Estado no puede llegar a controlar todo; y la autorregulación por sí sola no garantiza el cumplimiento efectivo de los objetivos perseguidos en esta materia, por lo que la co-regulación parece la fórmula más adecuada.

El equilibrio entre regulación y autorregulación en cada país debe establecerse atendiendo a la tradición existente en el mismo en esta materia.

En este sentido, la DLM[87] en Alemania señala que la autorregulación en Internet parece ser la principal opción sin la intervención de la autoridad competente, pero por varias razones, el *Landesmedienanstalten* ha observado que la autoregulación sólo trabaja eficazmente, si está acompañada por un órgano de autocontrol. Francia también apoya la co-rregulación. Se resalto, que las leyes generales canadienses combinadas con las medidas de autorregulación, son los métodos más efectivos.

La co-regulación puede traducirse en la creación de organismos en los que estén representados los poderes públicos y los distintos grupos sociales afectados.

III. La reflexión sobre la regulación de Internet debe realizarse tanto a escala internacional como nacional.

El debate sobre la regulación de Internet debe proyectarse en todos los foros internacionales relevantes, tales como G8, UIT, OMPI, OMC, ONU, UNESCO.

Los Noruegos señalan que deben inventarse nuevas formas de regulación. Los portugueses, indican una regulación global, descentralizada y flexible. Malta sugiere por un instante, la adopción de un proyecto de convención sobre la regulación de servicios distribuidos públicamente en Internet, para que luego sea enviada a la UNESCO con mira de un conferencia internacional a la que asistan miembros o no de la UNESCO.

IV. Medidas adoptadas con relación a la circulación del contenido en Internet: Campañas de sensibilización a los usuarios: Por ejemplo la prevención adoptada por Australia, Malasia, Singapur, Reino Unido para evitar cualquier riesgo al menor y/o promover el uso de sistema de filtros dirigido a los padres. Muchos países también han implementado en los colegios programas de entrenamiento en el uso de Internet, durante los cuales se educa precisamente a los menores en los riesgos que puede acarrear Internet y como se puede llegar a evitarse; elaboración de códigos de buena conducta; creación de líneas directas (*hot lines*); clasificación de contenidos; desarrollo de sistemas de filtrado; establecimiento de reglas sobre atribución de responsabilidad por la difusión de contenidos.

4.1.12.CONVENCION SOBRE EL CIBERCRIMEN

Con fecha 2 de Octubre del 2000, se publicó la Convención sobre el Ciber Crimen[88], Proyecto N° 22 REV 2. Este proyecto, en el artículo 9 relativo al tema sobre pornografía infantil en concordancia con el artículo 11, establece que cada Estado parte debe normar y adoptar otras medidas como puedan ser necesarias para establecer como ofensas criminales en cada país, al que intencionalmente ayude o sea cómplice en la comisión del delito de pornografía infantil.

---

[87] Foro Multidisciplinario sobre *Documento Legible por Máquina*, intgrado por un grupo de expertos.

[88] Budapest, Hungría, Firmada por un total de 30 paises (Estados Unidos, Japón, Canadá, Sudáfrica y 26 de los 43 paises

Si bien es cierto que la comunidad europea ha dejado claro la irresponsabilidad de los proveedores o prestadores de servicios de Internet –ISP_ frente a los contenidos ilícitos alojados por terceros, éstos artículos pueden conducir a que cada país con el fin de "no ayudar" o "o no ser cómplice" en la comisión del delito de pornografía infantil, llegue a regular y/o adoptar medidas autorreguladoras, que pongan un freno al libre flujo de información censurando arbitrariamente el contenido ilícito y responsabilizando al proveedor de Internet por los contenidos que una tercera persona aloje en sus servidores, lo cual impulsaría el monitoreo de las comunicaciones privadas.

A nuestro entender, los ISP son empresas privadas que pueden elegir qué es lo que transportan, casi todos actúan simplemente como un sistema encaminado que proporciona a sus clientes acceso al contenido de Internet en tal sentido, los ISP no son editores y por ende no tienen porque responsabilizarse por el contenido que alojam, posición que es adoptada por las directivas generales de la Comisión Europea.

4.1.13. MANUAL DE LA INTRERPOL

La Interpol ha elaborado un manual que describe los controles de acceso, los archivo de registro, las copias de seguridad, los cortafuegos[89], los sistemas de detección de intrusos[90] y como manejar los incidentes. Además recoge, de forma esquemática, los principales riesgos existente en materia de seguridad y ofrece consejos para prevenirlos.

---

miembros del Consejo de Europa.

[89] Se pueden encontrar en software o hardware, permiten bloquear páginas de Internet a las que no se desea tener acceso. Ejemplos CheckPoint, Symantec Client Security.

[90] Existen en presentaciones de Hardware o Software, permiten detectar personas o equipos que intentan ingresar a nuestra información de forma local o remota. Ejemplos Symantec Gateways Security, ISS Blackice.

El documento también integra las preguntas a realizar y los datos de interés que deben recoger los investigadores tras un incidente, información muy útil para que las empresas optimicen los reportes y faciliten las investigaciones que se lleven a cabo.

El Manual tiene, como principales destinatarios, a los investigadores y también es distribuido en CD-ROM.

El presidente de la Interpol abogó por el "trabajo conjunto" entre los cuerpos de seguridad y las entidades civiles dedicadas a la protección del menor.

La distribución de pornografía infantil por Internet es el delito contra los menores que más prolifera en el mundo, aseguró el Presidente de Interpol, Jesús Espigares. El policía inauguró en Palma de Mallorca, España, el 24 de abril del 2003 la XVII reunión del grupo policial internacional especializado en crímenes contra niños y adolescentes. El comisario abogó por el "trabajo conjunto" entre los cuerpos de seguridad y las entidades civiles dedicadas a la protección del menor.

El presidente de Interpol hizo hincapié en la importancia de reuniones de trabajo como las que se celebran en Palma para coordinar actuaciones y compartir experiencias sobre la persecución de la explotación de todo tipo que sufren cientos de miles de menores en el mundo.

Espigares abogó por el "trabajo conjunto" entre los cuerpos de seguridad y "las entidades civiles dedicadas a la protección del menor" y resaltó que las conclusiones de la reunión, en la que toman parte 130 expertos de 34 delegaciones, serán una guía de trabajo para todas las policías del mundo.

En este sentido, indicó que "la situación social y económica" de países subdesarrollados que "tratan de salir adelante ofreciendo mano de obra barata" fomenta el abuso laboral sobre menores, pero se mostró convencido de que las

grandes multinacionales implantadas en estos Estados no participan directamente de esta explotación.

La reunión de Palma se continuará con la celebración de grupos de trabajo específicos sobre prostitución infantil y turismo sexual, delincuentes sexuales, formación de policías, desaparición de menores y pornografía infantil[91].

4.2. ESFUERZOS JURIDICOS NACIONALES

4.2.1. ESTADOS UNIDOS DE AMERICA

Así algunos países han venido elaborando normas específicamente destinadas a combatir los contenidos ilícitos en Internet. Un ejemplo lo encontramos en los Estados Unidos. El 1 de febrero de 1996 el Congreso aprobó la *Communications Decency Act* 1996 (CDA) que prevela multas de 2 500 dólares así como penas de hasta dos años de privación de libertad para quienes iniciaran la transmisión de material obsceno e indecente a menores. La ley imponía un exceso de responsabilidad a los proveedores o prestadores de servicios de Internet que no tenían medios para determinar la edad de los destinatarios de las transmisiones electrónicas y obligaba a controlar los mensajes de contenido sexual que se difundían en Internet. Además, la formulación tan amplia con la que se había redactado la ley levantó las protestas de diversas asociaciones a favor de la libertad de expresión que alegaron que la CDA era contraria al derecho recogido en la Primera Enmienda de la Constitución de los Estados Unidos. El 11 de junio de 1996 fue declarada inconstitucional por un Tribunal de Filadelfia, sentencia que fue confirmada por el Tribunal Supremo el 26 de junio de 1996[92]

[91] Documento de la Interpol sobre cibercrimen de 25 de mayo de 2001.
[92] Supreme Coourt, *Reno Attorney General of the United Status et al. V American Civil Liberties Union et al.* 26 de junio de 1.

Una norma como la CDA vulnera el derecho a la libertad de información y expresión de personas de otras partes del mundo que consideran que esos mismos contenidos no son obscenos, derechos que se encuentran plenamente garantizados en las Constituciones de los diferentes países y consagrado en el artículo 19 de la Declaración Universal de Derecho Humanos que dispone:

"Todo el mundo tiene derecho a la libertad de opinión y expresión; este derecho incluye el derecho a defender las propias opiniones sin interferencias y a buscar, recibir e impartir información e ideas a través de cualquier medio sin importar las fronteras"

Igualmente, las personas mayores pueden buscar y encontrar contenidos legales pero obscenos. En ese sentido, cabe reiterar la no procedencia de ningún tipo de censura sobre este contenido, que fuera de Internet, es también una publicación plenamente garantizada por la libertad de expresión. En tal sentido, coincidimos con la opinión de David Casacubertas, que al respecto señala:

"...no podemos hacer que determinadas publicaciones estén garantizadas por la libertad de expresión fuera de Internet y en cambio dentro no se pueda..."

Sin embargo, una gran cantidad de usuarios de Internet que consideran que el fundamento de protección a los menores para justificar la censura de contenidos nocivos, no puede llegar al punto de vulnerar los derechos de libertad de expresión e información de personas de todas partes del mundo que, perfecta y legalmente pueden ver contenidos obscenos o ver contenidos que para su costumbre no son obscenos[93].

Las leyes en Estados Unidos son muy severas contra la pornografía infantil, la que se produce con menores de edad y los representa en posturas obscenas o en

actos sexuales, y aún aquella en la cual los participantes sean adultos "que actúan y se ven como niños".

El advenimiento de internet ha dado una nueva vía para quienes producen, venden, compran, distribuyen y disfrutan de la pornografía infantil. Así entre 1996 y 1999 la Oficina Federal de Investigaciones registró un aumento del 1225 por ciento en sus operaciones contra este crimen. También las leyes restringen las formas de pornografía que pueden producirse y distribuirse en Estados Unidos, pero en el caso de las escenas eróticas u obscenas con menores, ni siquiera es necesaria la distribución para que sea un delito, basta con que una persona tenga en su casa esos materiales para que sea posible su procesamiento.

El argumento principal que sustentó la aprobación en 1996 de la Ley de Protección contra la Pornografía Infantil fue que, a diferencia de otros materiales gráficos en los que se representan actos repudiables, repugnantes o criminales en la producción de pornografía infantil, los mismos actores -los niños y niñas- son víctimas de un abuso. "Hay, esencialmente, dos observaciones a esta ley", dijo Stephen Block, un abogado de la Unión de Libertades Civiles. "Una es que es demasiado amplia, es decir que va demasiado lejos y prohíbe, de hecho, la expresión que de otra forma sería legal", indicó. "La otra es que es demasiado vaga y puede usarse de maneras diferentes".

... Las reservas son pertinentes en el caso de la novedosa tecnología digital que permite las maravillas de ficción que millones de espectadores en todo el mundo han disfrutado en películas como "Parque Jurásico", o "El Día de la Independencia". Esa misma tecnología, que además mejora día a día, permite la creación de imágenes casi realistas de niños que "virtualmente, no pueden distinguirse de las reales", según Roger Parloff, de la revista de internet "Inside".

---

[93] Consultar web Cibernauta.

Un agente policial, citado en el informe del Senado durante los debates de la ley de 1996, afirmó que "pronto ya no será necesario molestar sexualmente a un menor para producir la pornografía infantil que explota y degrada a los niños y puede usarse para el abuso real".[94]

Bruce Taylor, del Centro Nacional de Ley para los Niños y las Familias, indicó que "si el pederasta no puede distinguir qué es y qué no es real, entonces ese material es igualmente incitante para él, y puede ser igualmente seductor para el niño". Pero, al mismo tiempo, en un país donde tanto se disputa desde hace más de 200 años sobre la libertad de expresión, el hecho es que la ley contra la pornografía infantil, aplicada a las "producciones virtuales", criminaliza la expresión puramente ficticia de las fantasías de su autor.

La libertad de expresión en Estados Unidos comprende la tolerancia a la manifestación de las ideas y las propuestas más extremas, y aún más abominadas por la sociedad, en tanto no se pase del dicho al hecho. Así, por ejemplo, no es un delito la expresión pública, en la prensa, en las calles, en internet o en películas de propuestas racistas o ideas políticas revolucionarias, pero es un crimen el ataque personal o la acción para el derrocamiento del gobierno.

A pesar del claro fracaso que supuso la CDA, el Congreso de los Estados Unidos aprobó en octubre de 1998 una nueva ley en relación con los contenidos ilícitos en Internet, la *Children's On-line Protection Act* 1998 (llamada COPA o CDA II) en la que se intenta una vez más regular los contenidos ilícitos en Internet. La Ley considera delito el hecho de que los operadores ofrezcan material sexualmente explícito a los menores de 17 años. Afecta por tanto, a los proveedores de contenidos y también a los proveedores de servicios que alojan páginas web, a los servidores de noticias o a los servidores de listas de distribución.

La medida se aplicaba a cualquier tipo de comunicación (texto, imágenes, sonidos) que contuviera desnudos, sexo (real o virtual) o en la que se detectase "una falta de valores morales, científicos, literarios, artísticos y políticos". Las sanciones consistían en seis meses de prisión y multas de hasta 150 000 dólares por cada día de incumplimiento. En febrero de 1999 la Ley fue objeto de recurso de inconstitucionalidad ante un Tribunal de Filadelfia. A la hora de escribir estas líneas la Ley sigue en suspenso y no parece que vaya a ser aplicada, por los mismos motivos por los que fue declarada inconstitucional la CDA de 1996, esto es, por constituir una vulneración del derecho a la libertad de expresión y por la imposibilidad de imponer unos estándares morales en Internet, caracterizada por la multiculturalidad, transnacionalidad y su carácter abierto.

La Ley para la Protección Online de la Infancia (Child Online Protection Act), aprobada por el Congreso y firmada por Bill Clinton en 1998, exige la implantación de unos sistemas de control previos en la Web para impedir el acceso de los menores a material potencialmente dañino.

En diciembre de 1999 el Tribunal de Apelaciones del noveno Distrito Federal en California, en una demanda contra el gobierno, calificó como violación de la Constitución la ley de 1996 contra la pornografía infantil. Los gremios de productores cinematográficos ahora esperan que el Tribunal Supremo emita su fallo.

El Tribunal Supremo de Estados Unidos dijo que escucharía la apelación del Departamento de Justicia para que se permita al gobierno federal endurecer la ley de 1998 que pretende proteger a los menores de la pornografía infantil[95].

---

[94] Más información Mercury Center.
[95] REUTERS BRUCE, Harris. CIBERNAUTA. Washigton.

Los magistrados acordaron revisar la sentencia de un tribunal de apelaciones que prohibió el reforzamiento de la ley basándose en la libertad de expresión, consagrada en la Constitución, porque confiaba en la madurez de los ciudadanos para identificar el material online dañino para los menores.

El alto tribunal ha decidido ahora escuchar los argumentos del gobierno y emitirá una resolución al respecto.

El Tribunal de California que conoció el caso llegó a las siguientes conclusiones, que desgranaban los distintos supuestos de responsabilidad en los que podía incurrir un proveedor de servicios de Internet por los contenidos ilícitos introducidos por sus clientes: a) el proveedor de servicios no podía ser responsable directo de la infracción, por cuanto que los contenidos ilícitos (las obras protegidas por derechos de autor) habían sido cargados en la Red por un cliente; b) tampoco era responsable subsidiario de la infracción porque no existía vinculación entre las actividades ilícitas llevadas a cabo por el usuario y los beneficios económicos obtenidos por el proveedor de servicios de Internet; y c) no tiene responsabilidad concurrente porque *Netcom* no había incitado la conducta ilícita del usuario.

Por fin, quedaban clarificadas en la jurisprudencia las parcelas de responsabilidad de los proveedores de servicios de Internet. Los distintos casos que se suscitaban ante los tribunales ponían de manifiesto la necesidad de elaborar una ley específica. A partir de este momento, la solución se abordaría desde una perspectiva vertical, lo que significa que se iban a dictar leyes distintas según se tratase de responsabilidad por contenidos pornográficos, responsabilidad por infracción de los derechos de autor o por vulneración del derecho al honor.

En octubre de 1998, el Gobierno de los Estados Unidos dictó una ley destinada a proteger los derechos de autor en las redes digitales. La *Digital Millenium Copyright Act*[96] (en adelante, DMCA), que entró en vigor en octubre de 1998, contiene una sección específicamente dedicada a la responsabilidad de los intermediarios.

La DMCA es régimen optativo y voluntario para los proveedores de servicios. Significa que pueden elegir entre acogerse al régimen general de la legislación sobre *copyright* o bien acogerse al régimen más favorable de la DMCA. Si optan por el primer régimen, su actuación deberá respetar las normas vigentes relativas al *copyright* en las que se establecen elevadas indemnizaciones por la infracción de los derechos de autor. Por el contrario, si el proveedor decide acogerse al régimen que incorpora la DMCA, gozará de la protección que le conceden los cuatro supuestos de exención de responsabilidad.

Para que un proveedor de servicios de Internet pueda acogerse al régimen de la DMCA es necesario que cumpla tres requisitos previos. El primero consiste en que el prestador del servicio está obligado a informar a sus clientes acerca de las condiciones de rescisión del contrato así como los supuestos que darían lugar a ello. Esta condición tiene por objeto evitar los casos frecuentes en los que infractores de los derechos de autor, que han visto bloqueada su página web, puedan volver a contratar con el mismo proveedor de servicios bajo una identidad distinta (por ejemplo, un pseudónimo o incluso amparándose en el anonimato). El segundo requisito exige al prestador de servicios de Internet que no interfiera y permita las medidas tecnológicas que los autores utilizan para proteger sus obras (por ejemplo,

[96] Además de la DMCA, dos proyectos de ley contiene disposiciones relativas a la responsabilidad de los proveedores ce servicios de Internet por violación de los derechos de propiedad intelectual. (1) La propuesta de *Digital Copyright Clarification and Technology Education Act* de 1997 contiene la exoneración de responsabilidad por infracción de los derechos de autor a los centros educativos; (2) La propuesta de *On line Copyright Infringement Liability Limitation Act* de 1998, contiene la exoneración de responsabilidad del proveedor de acceso siempre que no hubiera iniciado la transmisión, no seleccionara el material y no hiciera copias del material infractor durante más tiempo del necesario. Esta última ley también establece que los proveedores de servicios no están obligados a controlar los contenidos que transitan por sus sistemas.

las llamadas *digital watermarks)*. Finalmente, los intermediarios están obligados a proteger la intimidad y privacidad de los usuarios del servicio, lo que les libera de la obligación de controlar los contenidos que transitan por sus sistemas.

Cumplidos los tres requerimientos, el proveedor de servicios de Internet podrá beneficiarse de los cuatro supuestos de exoneración de responsabilidad que recoge la DMCA. Los PSI no podrán ser demandados por infracción de los derechos de autor si su actividad se encuadra en alguna de las descritas y además cumplen los requerimientos establecidos en la Ley. Son cuatro exoneraciones:

Primera, la actividad de mero transporte. El prestador de servicios de Internet no se considera responsable si la actividad que desarrolla consiste en transmitir, encaminar o en proporcionar la conexión al material infractor (es decir, que actúa como un mero transportista) y reúne las condiciones que exige la DMCA (que el prestador se servicios no seleccione el material, no lo modifique, etc.).

Segunda, la actividad de *caching* que consiste en mantener en la memoria *caché* del ordenador una copia oculta de las últimas páginas web visitadas, de forma que si el usuario vuelve a solicitarlas, las páginas se leen desde el propio ordenador sin tener que acceder de nuevo a la Red, aumentando considerablemente la rapidez en la navegación en la Red. Los sitios web almacenados en la memoria oculta del ordenador pueden contener informaciones ilícitas y nocivas. De éstas, el proveedor de servicios del Internet no será responsable si la actividad de almacenamiento temporal tiene por objetivo hacer más eficiente la transmisión.

Tercera, el alojamiento de datos. El prestador de servicios de Internet no será considerado responsable por almacenar material, por ejemplo, un salón de *chat* o un sitio web, siempre que cumpla con las siguientes condiciones: a) que no tenga conocimiento real del carácter infractor del material; b) que no tenga conocimiento de la información de la que se deriva el carácter aparente de la actividad infractora; c) que actúe con prontitud para retirar o impedir el acceso al material tan pronto como sea consciente; d) que no reciba un beneficio económico directamente relacionado con la actividad infractora; y, finalmente, e) que retire con celeridad el material infractor tras haberle sido notificada la presunta infracción.

Cuarta, los motores de búsqueda y localización de información. Los buscadores de Internet no serán responsables por la infracción de los derechos de autor cuando su actividad consista en vincular a los usuarios con un sitio web que contenga material ilícito y además, se cumplan las condiciones apuntadas en el apartado anterior.

El procedimiento de notificación y descarga del material infractor es el siguiente: todas las personas que ofrezcan sus servicios a través de Internet deben inscribirse en la Oficina de Propiedad Intelectual (se incluyen tanto los proveedores de contenidos profesionales, no profesionales y todas las categorías de proveedores de servicios: universidades, empresas, etc.). Cuando un usuario detecta contenidos que vulneran los derechos de autor, debe notificárselo al PSI mediante un documento firmado. Si la notificación es falsa, incurre en responsabilidad por haber actuado con mala fe. Recibida la notificación, el PSI tiene que actuar con prontitud para retirar el material y posteriormente debe notificar a la persona que introdujo el contenido ilícito en la Red. Éste puede responder alegando que el material no es ilícito. En estos casos, el PSI deberá volver a cargar el contenido en la Red salvo que se haya presentado una demanda ante los tribunales.

El procedimiento de notificación y descarga del material infractor está pensado para los contenidos ilícitos en los sitios web, y no para las infracciones de los derechos de autor en los grupos de noticias o en las listas de distribución. De este modo, por ejemplo, sí una persona ve cómo su obra protegida por derechos de autor es a enviada a un grupo de noticias, no tiene medios para impedir la violación de sus derechos, quedando de este modo indefenso.

A medida que el debate se intensificaba en los Estados Unidos, en Europa los jueces se enfrentaban con los primeros casos de responsabilidad de los proveedores de servicios por contenidos ilícitos introducidos por sus usuarios. En 1995, *Compuserve*[97] (filial alemana de un proveedor de servicios de Ohio, Estados Unidos) fue denunciado por un usuario alemán por dar acceso a más de doscientos grupos de noticias en los que se difundían mensajes de pornografía infantil y otras perversiones pornográficas. El director de *Compuserve* bloqueó el acceso de sus abonados de todo el mundo, lo cual levantó las protestas de aquellos que veían cómo se imponían los valores de la sociedad alemana al resto de los internautas. Poco después, el acceso a los grupos de noticias se restableció salvo para los ciudadanos alemanes. A pesar de ello, el Director del PSI *Compuserve* fue condenado en 1998 a dos años de libertad vigilada por complicidad en la difusión de material pornográfico, sentencia que fue anulada en 1999, en consonancia con las disposiciones introducidas por la llamada *Ley Mutimedia* de 1997 que establece que los proveedores de acceso no son responsables de los contenidos ilicitos a los que sólo proporcionen acceso, mientras que; los proveedores de alojamiento sólo son responsables si tienen conocimiento del carácter ilícito del contenido y además, les es posible eliminarlo de su oferta de servicios.

[97] Caso *Compusuerve*

El Acta de Protección de la Intimidad en Internet para los Niños, que entró en vigor el mes abril del 2002, prohíbe a todas las empresas de la Red destinadas a los niños, recopilar datos personales a menos que dispongan del permiso de los padres. Además, a las páginas se les pide que anuncien sus políticas sobre intimidad, para explicar cómo usan o comparten esa información.

En su lucha por erradicar el mal uso de la red mundial, las autoridades estadounidenses buscan, a través de su servicio de inteligencia, atrapar a las mafias de prostitución, aunque ello signifique en muchas ocasiones violar el derecho de privacidad de los usuarios.

La compañía McAfee ha dispuesto de un software "Internet Guard Dog", que ayuda a los padres a supervisar y controlar las actividades "online" de sus hijos y los mantiene a salvo de los peligros de Internet, según informa la compañía, el martes 19 de junio del 2001 en una nota de prensa.

"McAfee Internet Guard Dog" proporciona un conjunto integral de funciones personalizables de privacidad y seguridad para la Red, que incluyen el bloqueo de cookies, el filtrado de sitios web y la protección completa de antivirus[98].

Uno de los métodos más comunes en la actualidad, para salvaguardar la privacidad de los usuarios de *e-mail*, es a través de la encriptación –poner candados-. El *pret Good Privacy* (PGP) es un software que protegé la privacidad del servicio de correo electrónico. El PGP es tan sólido que ni siquiera las computadoras más poderosas del mundo pueden violarlo, incluyendo los servicios de inteligencia de las potencias mundiales. Por ello, en su momento los agentes del FBI consideraron el programa como una arma de alta tecnología.

[98] Consultar web iBrujula.com.

Su creador, Phil Ziimmermann, es consultor independiente de ingeniería de *software*, experto en sistemas de seguridad para datos y comunicaciones. Es un luchador social que busca el respeto a la privacidad de los usuarios de la red.

El Gobierno de Estados Unidos anunció haber aprobado un fondo de 8.6 millones de dólares para becar a 200 estudiantes de seguridad informática que acepten trabajar como policías cibernéticos después de graduarse.

La Fundación Nacional de Ciencia dijo que había seleccionado a seis universidades para participar en el programa, cuyo objetivo es enfrentarse a la escasez de expertos en seguridad informática en el gobierno federal.

El gobierno pagará dos años de estudio de los participantes, quienes se enrolarán primero como trabajadores de verano en oficinas federales y, después de graduarse, serán empleados regulares.

Los participantes deberán trabajar para el gobierno al menos un año por cada año de beca recibida y luego quedarán en libertad para seguir siendo empleados públicos o irse al sector privado.

Rita Colwell, Directora de la Fundación Nacional de Ciencia, anunció el programa, conocido como Becas por Servicio, en una reunión sobre educación en seguridad cibernética en la Universidad George Mason de Fairfax, Virginia.

"Estas becas animarán a los jóvenes a ingresar en el terreno de la seguridad de información y les dará la oportunidad de poner sus talentos en primera línea de los esfuerzos gubernamentales de ciberseguridad", añadió Calwell[99].

[99] REUTERS BRUCE, Harris. ESTADOS UNIDOS APRUEBA BECAS PARA POLICIAS CIBERNETICOS. Washington, 3 de mayo de 2001.

4.2.2. ESPAÑA

Actualmente España cuenta una ley denominada: Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, la cual señala en su exposición de motivos que sólo se permitirá restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países en los supuestos previstos en la Directiva 2000/31/CE, que son: la producción de un daño o peligro graves contra ciertos valores fundamentales, como el orden público, la salud pública o la *protección de los menores,* y el incumplimiento de la ley nacional que resulte aplicable en las materias excluidas del principio de país de origen.

Dicha ley, como indica su nombre, pretende dar respuesta normativa a dos aspectos: en primer lugar regular la denominada sociedad de la información, como "realidad" que interconecta a los proveedores de servicios y a los usuarios, y en segundo lugar, regular el quid de Internet cual es la contratación electrónica.

Entre otros aspectos, regula el régimen de responsabilidad civil y penal de los intermediarios técnicos. Esta Ley implementará la llamada Directiva de Comercio Electrónico que establece exenciones de responsabilidad en la línea de las recogidas en la DMCA, muy favorables al desarrollo del comercio electrónico. La obligación de identificar al usuario que recae sobre los intermediarios debe ser reforzada con sanciones para el caso de incumplimiento.

Resulta positiva la creación de organismos especializados como los departamentos creados en la Guardia Civil y la Policía Nacional. España se encuentra a la par con los países que encabezan la lucha contra los contenidos ilícitos en la Red.

Así la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico establece en el Capítulo III artículo 18 los Códigos de Conducta.

Artículo 18. Códigos de conducta:

"... 2. En la elaboración de dichos códigos, habrá de procurarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones que representen a los discapacitados, cuando afecten a sus respectivos intereses.

Además, cuando su contenido pueda afectarles, tales códigos habrán de tener especialmente en cuenta la protección de los *menores* y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias."

Como puede apreciarse a pesar de que España es uno de los países que tiene un alto índice de casos de pedófilos su legislación sigue siendo muy escasas al respecto.

Sin embargo, como ya se señalaba, esta ley pretende trasladar la normativa comunitaria 2000/31 CE con todas sus limitaciones y controles exigidos para los proveedores de servicios y los intermediarios. Así, y para ilustrar esto, sirvan a modo ejemplo las siguientes medidas que se atribuirán a la Administración: la potestad de cerrar o interrumpir los servicios de los Proveedores, de suspender temporalmente su actividad, de cerrar provisionalmente sus establecimientos, o de incautar sus equipos.

A este respecto la AEPSI (Asociación Española de Proveedores de Servicios de Internet) se ha manifestado muy críticamente alegando que el regulado normativo adelantado en el Proyecto les deja en una situación de indefensión jurídica al tiempo que les dificulta su actividad, como por ejemplo, al introducir la novedosa prohibición

de enviar comunicaciones comerciales por vía electrónica, ya sea a través de e-mail o de cualquier medio análogo, por ejemplo, cuando éstas no hayan sido solicitadas por el interesado o no haya consentido previamente (que por otro lado parece una prohibición socialmente demandada).

Como resumen podemos decir que, independientemente de las potestades que se va a arrogar la administración, el proyecto normativo es necesario, conveniente y positivo. Necesario porque la confianza en el medio electrónico es escasa; conveniente porque en la misma medida en que la red se va desarrollando y ampliando su campo de acción e interacción con los usuarios en esa misma medida se deben regular los controles y actividades de estos proveedores e intermediarios; y positiva porque quien va a salir beneficiado con esta regulación es el consumidor y el usuario.

La preocupación acerca de los contenidos ilícitos y nocivos en la Red ha generado un debate internacional que ha permitido vislumbrar algunas soluciones que garanticen la protección de los valores jurídicos en las redes digitales (derecho al honor, protección de los menores y de la dignidad humana o propiedad intelectual).

La Unión de Consumidores de Andalucía UCE ha alertado del "libre" acceso de menores a páginas pornográficas de Internet en los ciber-cafés, por lo que ha solicitado que estos locales tengan una sala para los más jóvenes donde estén restringidos los juegos "online" y las web con contenido pornográfico.

Para UCE, la solución pasaría por disponer de dos salas independientes, siendo una de ellas de acceso prohibido a menores e instalando códigos de seguridad para determinadas páginas web con contenido sexual o violento.

La unidad de delitos tecnológicos de la policía española ha prestado especial atención a la cuestión de la pornografía infantil, habilitando incluso una oficina virtual de denuncias, www.policia.es, con un servicio de alertas 24 horas, http://www.mir.es/policia/uiti/alerta24.htm, para prevención urgente de delitos tecnológicos[100].

Durante la legislatura el Gobierno del PP impulsó la modificación del Código Penal a fin de crear una nueva figura que castigara la simple posesión de material pornográfico que contuviera imágenes explícitas de explotación sexual de niños, pero siempre que aquella posesión estuviera orientada a la comercialización o exhibición. El acuerdo de los Quince busca sancionar la simple tenencia de material pornográfico y unificar la descripción de los nuevos delitos incrementando las penas.

En España la adquisición o posesión de pornografía no es un delito. Sorprendentemente, tampoco se castiga la adquisición de pornografía infantil. La reforma del Código Penal español, realizada por Ley Orgánica 11/1999, sobre los "delitos relativos a la libertad e indemnidad sexual de los menores" castiga la comercialización de pornografía infantil (Art. 189) con penas de uno a tres años de prisión, independientemente del origen -extranjero o desconocido- del material pornográfico, dejando fuera -al haber sido rechazada la enmienda en el Senado que preveía su castigo- conductas que perseveran en el ataque a la libertad y dignidad de los menores que han sido objeto de abusos sexuales, y que contribuyen a la expansión del lucrativo mercado generado en torno a los menores.

El resto de los Estados miembros, entre los que se encuentra España, aplica el régimen general en materia de responsabilidad civil y penal. Por ejemplo, si un proveedor de contenidos difunde pornografía infantil en Internet, está cometiendo el tipo sancionado en el artículo 189.1 del Código Penal[101] que castiga con la pena de

[100] Consultar webs iBrujula.com, El Periódico, El País, El Mundo, y ABC.
[101] El artículo 189 de Código Penal es un precepto incorporado por la Ley Orgánica 11/1999, de 30 de abril, de los "delitos

prisión de uno a tres años al que comercialice pornografía infantil, con independencia de que su origen sea extranjero o desconocido. De este modo, se hace posible el castigo de aquellas personas que produzcan, vendan, exhiban o faciliten la producción, venta, difusión o exhibición de material pederasta por cualquier medio, incluido los electrónicos. La posesión de dicho material para la realización de estas conductas se sanciona, en España, con la pena de 12 a 18 meses de prisión.

En España, el Anteproyecto de Ley de Comercio Electrónico de 2000 contiene un precepto específico relativo a la responsabilidad por actos propios de los proveedores de contenidos[102], sometiéndoles al régimen general de responsabilidad civil y penal.

Igualmente, la legislación propuesta en España -el Anteproyecto de Ley de Comercio Electrónico de 2000-, contiene severas obligaciones para que los proveedores de servicios de Internet identifiquen a los proveedores de contenidos cuando así lo requieran las autoridades competentes, posibilitando la localización tanto de los creadores de las páginas web no profesionales como de los remitentes de mensajes anónimos. Desde el momento en que sea posible identificar al proveedor de contenidos, éste responderá por actos propios.

Si éstas son las obligaciones legales que recaen sobre los intermediarios, podemos preguntamos ahora si los propios proveedores de contenidos tienen la obligación de identificarse cuando crean su página web o envían un correo electrónico.

---

contra la libertad e indemnidad sexuales" que rellena la laguna existente en relación con la protección de la infancia. Se tipifica así, por primera vez en España, la comercialización de pornografía infantil.

[102] El artículo artículo 8 del anteproyecto de Ley de Comercio Electrónico española establece que:" 1. Los prestadores de servicios de la sociedad de la información responderán de los daños y perjuicios que causen en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta Ley o no actúen con la debida diligencia. 2. La responsabilidad será exigible conforme a las normas generales sobre culpa contractual o extracontractual, según proceda. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia. 3. Lo dispuesto en este artículo, se

Ciertamente, los proveedores de contenidos profesionales (aquellos que persiguen un beneficio económico con su actividad) deben identificarse, tal y como establece la *Directiva 97/7/CE. relativa a la protección de los consumidores en materia de contratos de Venta a distancia*[103]. En estos casos, toda persona que venda un producto o un servicio, también por vía electrónica, debe identificarse. Esta obligación se extiende en la *propuesta de Directiva de Comercio Electrónico* de 1999[104] (la llamada Directiva de Comercio Electrónico) a todos los proveedores de contenidos, ya sean profesionales o no. No obstante, cabe señalar que el Anteproyecto de Ley español sobre Comercio Electrónico de 2000, parecía dar un paso atrás y libera de la obligación de identificarse a los proveedores de contenidos no profesionales.

Responsabilidad de los intermediarios. En los casos en los que no ha sido posible responsabilizar al proveedor de contenidos por los actos ilícitos cometidos en Internet, bien porque han surgido problemas de localización, bien porque el proveedor de contenidos carecía de recursos económicos suficientes, las víctimas del acto ilícito se han dirigido a los sujetos que han posibilitado la difusión de los contenidos en la Red: los operadores de telecomunicaciones y los prestadores de servicios de Internet. De este modo, se ha suscitado el debate acerca de cuál era el alcance de la responsabilidad de los intermediarios en la comunicación en línea por los actos ilícitos o nocivos cometidos por sus clientes.

Responsabilidad de los operadores de telecomunicaciones. Los operadores de telecomunicaciones ofrecen las infraestructuras necesarias para transmitir la información, pero no participan en el proceso de selección y puesta a disposición al público de determinados contenidos. Se trata de empresas que no presentan los inconvenientes de los proveedores de contenidos, y en la medida en que contribuyen

---

entiende sin perjuicio de lo establecido en la Legislación de protección a los consumidores y usuarios en lo penal".

[103] Directiva 97/7/CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia (DO CL 144, de 14 de junio de 1997).

[104] Propuesta modificada de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior. COM (1999) 427 Final de 17 de agosto de 1999.

a la transmisión de la información se les ha querido ver como potenciales responsables de los contenidos ilícitos y nocivos que han transitado por sus instalaciones.

Ahora bien, los operadores de telecomunicaciones han alegado que son meros transportistas de la información y por tanto, no pueden ser responsables de los contenidos que sus suscriptores introducen en la Red, al igual que sucede en los medios de comunicación tradicionales. Por ejemplo, una compañía telefónica no es responsable del contenido de las conversaciones telefónicas de sus abonados.

El consenso ha sido total en los foros internacionales en los que se ha debatido el alcance de la responsabilidad de los operadores de telecomunicaciones, y se ha llegado a la conclusión de que no serán responsables penal o civilmente de los contenidos ilícitos introducidos en Internet por sus clientes.

Esta solución se recoge en las normas elaboradas en el seno de la Unión Europea. La *Propuesta de Directiva sobre Comercio Electrónico* de 1999[105] contempla la exoneración de responsabilidad, tanto civil como penal, de los operadores de telecomunicaciones cuando su actividad consista en transmitir datos facilitados por el abonado, y además, se cumplan las siguientes circunstancias: primero, que el operador de telecomunicaciones no haya originado él mismo la transmisión; segundo, que tampoco haya seleccionado el destinatario de la transmisión; y tercero, que no haya modificado; ni seleccionado los datos transmitidos. La exoneración de responsabilidad de los operadores de telecomunicaciones no les libera de la posibilidad de que las autoridades judiciales nacionales les puedan imponer determinadas medidas cautelares respecto a sus clientes cuando éstos utilicen las redes para difundir contenidos ilícitos.

[105] *Idem*

Igualmente, los operadores de telecomunicaciones quedan exentos de responsabilidad en el Anteproyecto de Ley sobre Comercio Electrónico de 2000 en los casos en los que no hayan originado o modificado ellos mismos los datos o seleccionado éstos o a sus destinatarios.

Si, por el contrario, se trata de un acto ilícito cometido por el propio operador de telecomunicaciones (por ejemplo, que vulnere su obligación de proteger datos de carácter personal), deberá responder por actos propios conforme a la legislación vigente.

Responsabilidad de los proveedores de servicios de Internet. Los proveedores de servicios de Internet han sido el objetivo predilecto de las personas perjudicadas por los contenidos ilícitos y nocivos introducidos en la Red en los casos en los que no era posible identificar al autor del material ilícito o nocivo. Hasta tal punto que la cuestión de su responsabilidad ha sido el caballo de batalla en los foros internacionales en los que se ha tratado esta cuestión.

La clarificación de la responsabilidad de los proveedores de los servicios de Internet era esencial para lograr el despegue del comercio electrónico. Las autoridades públicas fueron conscientes de que la disparidad de legislaciones y las distintas respuestas que ofrecía la jurisprudencia constituía un claro obstáculo al desarrollo del comercio electrónico porque propiciaba la emigración de las empresas hacia países de legislación más permisiva.

Mientras se debatía la propuesta de Directiva en el seno de la Unión Europea, España carecía de legislación específica materia de responsabilidad de los proveedores de servicios de Internet, y sus jueces no se habían enfrentado a la

cuestión. Resultaba de "aplicación el régimen general de responsabilidad penal y civil"[106].

El Anteproyecto de Ley de Comercio Electrónico, que implementará la futura Directiva de Comercio Electrónico, recoge similares exoneraciones de responsabilidad tanto civil como penal.

Los proveedores de acceso quedan exentos siempre que no hayan originado o modificado ellos mismos los datos o seleccionado éstos o a sus destinatarios.

Las actividades de *caching* no comprometen la responsabilidad del intermediario que la lleve a cabo, en los casos en los que dicha actividad tenga como única finalidad la de hacer más eficaz la transmisión posterior de la información a otros destinatarios del servicio y siempre que éstos lo hayan solicitado.

Los proveedores de alojamiento quedan exentos de responsabilidad de los contenidos ilícitos almacenados a petición del usuario, excepto si tienen conocimiento efectivo de que la actividad es ilícita. En estos casos, el proveedor de alojamiento deberá retirar la información o hacer imposible el acceso a ella.

Al igual que la Directiva de comercio electrónico, el Anteproyecto libera a los proveedores de servicios de la obligación de controlar los contenidos que transmitan o almacenen, a no ser que lo soliciten las autoridades judiciales o policiales y la supervisión les resulte técnicamente posible. Sólo en estos casos quedan obligados a "supervisar el contenido de los datos e informaciones que constituyen el objeto del servicio de la sociedad de la información" (por ejemplo, el contenido de las páginas web, o el contenido de un mensaje enviado a un grupo de noticias) y a "realizar el

[106] El artículo 1902 del Código Civil Español establece que "el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

control respecto de los hechos o circunstancias contenidas en aquellos que pudiesen constituir actividades ilícitas".

Responsabilidad de los proveedores de contenidos. En los últimos años, los jueces y tribunales han tenido ocasión de manifestarse sobre la responsabilidad tanto civil como penal de aquellas personas que introducen contenidos ilícitos en la Red. Así, son numerosos los ejemplos de responsabilidad de los proveedores de contenidos en delitos relativos a la protección de la dignidad humana (racismo y xenofobia), infracciones de , los derechos de propiedad intelectual y sobre todo, relativos a la libertad e indemnidad sexual (difusión de pornografía infantil).

Responsabilidad de los usuarios. Finalmente, cabe preguntarse si los usuarios de Internet pueden llegar a incurrir en algún tipo de responsabilidad por descargar de la Red contenidos ilícitos. ¿Es ilícito descargar de la Red imágenes pornográficas? ¿Cómo es posible identificar al usuario si éste hace uso de los programas que permiten la navegación anónima? Efectivamente, muchos consumidores de pornografía infantil y otras perversiones pornográficas se ponen en contacto a través de grupos de noticias, amparándose en el anonimato y en el cifrado de sus mensajes, lo que hace que la persecución de estos delitos resulte una tarea compleja a la que deben enfrentarse las autoridades policiales. También los consumidores de materiales que infringen los derechos de autor utilizan la Red como fuente prácticamente gratuita de todo tipo de material ilícito (copias no autorizadas de programas de software, de archivos MP3, etc.).

La Unidad de Investigación de Delincuencia en Tecnologías (UIDTI) de la Información recibe las denuncias, que no pasan de ser comunicaciones de posibles delitos, son comprobadas por los agentes para constatar si el sitio web está albergado en un proveedor español o extranjero. Si sucede esto último, informan a la policía pertinente a través de la Interpol.

En este sentido, la Policía considera positivo que Europol, cuerpo policial para el continente, adopte competencias en materia de distribución de pornografía infantil, lo que facilitaría la investigación y persecución de este tipo de delitos.

En el caso de que las páginas estén en un servidor español, la Policía abre una investigación, que se debe enfrentar, según el Cuerpo, a la lentitud judicial y la relación posterior con los proveedores de servicios de Internet, entidades cuyo objetivo es desarrollar un negocio, no una operación policial[107].

La UIDTI se ha puesto en contacto con todas las empresas proveedoras de acceso a Internet (ISP) existentes en España, casi 1700, para que eliminen los canales de distribución de material pornográfico, ya que muchos de estos proveedores no saben que las tienen, debido a la gran cantidad de páginas que albergan.

Se han identificado y retirado de los ISPs cerca del 80 por ciento de estos canales, pero aún queda un 20 por ciento en activo.

Por ello, las autoridades policiales han de proporcionar a los ISPs los medios necesarios para eliminar este material pornográfico, quedando bajo su responsabilidad la no retirada del mismo.

4.2.3. ALEMANIA

Alemania cuenta con una ley específica determinando la responsabilidad de los proveedores o desarrolladores de contenidos ilícitos en Internet. La llamada *Ley Multimedia* de 1997[108] regula, entre otros extremos, el régimen de responsabilidad por los contenidos en Internet de los diferentes actores que participan en su transmisión. En virtud de esta ley, los proveedores o desarrolladores de contenidos son responsables de sus actos, sin limitación alguna, lo que significa que quedarán sujetos a medidas cautelares y a indemnizaciones por daños y perjuicios en los casos en los que el acto ilícito genere responsabilidad civil (violación de los derechos de autor, difamación, etc.) o a las sanciones que establezcan las normas penales cuando genere responsabilidad penal (por ejemplo, pornografía infantil o negación del holocausto judío).

En Alemania, la iniciativa autorreguladora realizada por el grupo de trabajo –ICTF-, conformado por un grupo de proveedores o prestadores de servicios de Internet fueron los responsables directos del bloqueo de la página web de XS4ALL en Holanda.

Fueron el instrumento para amenazar a los proveedores y obligarles a organizar bloqueos de las páginas, lo cual demostró la facilidad con lo que se puede coaccionar a un ISP.

---

[107] Consultar web www.delitosinformaticos.com. Noticias.

[108] "ley Multimedia" (*Federal Law to Regulate the Conditions for Information and Communications Services) K entró en vigor el 1 de octubre de 1997.*

Lastimosamente, los sistemas autorreguladores no respetan las garantías mínimas de un debido proceso ni el derecho de defensa del presunto infractor, simplemente el ISP a propia voluntad o voluntad de un tercero o de acuerdo a intereses meramente comerciales decide censurar el contenido y decide que es Ilícito no respetando el derecho del presunto autor del delito a defender la licitud de su contenido.

4.2.4. FRANCIA

En Francia con la reforma de la *Ley de Regulación de Telecomunicaciones* de 1996, que preveía una exoneración de responsabilidad penal y civil de los proveedores o prestadores de servicios cuando ofrecían a sus usuarios el acceso a contenidos ilícitos (por ejemplo, una página web con material pederasta, o un foro de discusión al que se enviasen mensajes racistas). Ahora bien, para que los proveedores de acceso a Internet pudieran beneficiarse de la exoneración, debían atenerse a las instrucciones dadas por el Consejo Superior de Telecomunicaciones. Dicho Consejo había sido creado específicamente para determinar cuáles eran los contenidos admisibles *y* cuáles debían ser bloqueados por los proveedores de acceso. En julio de 1996, no obstante, la Ley fue declarada inconstitucional[109] porque, al igual que había ocurrido en los Estados Unidos con la CDA, el legislador nacional pretendía imponer estándares nacionales para determinar qué es considerado ilícito o nocivo, plenamente incompatible con el carácter transnacional *y* global de Internet.

[109] Sentencia del Tribunal Constitucional francés de 23 de julio de 1996. El 3 de septiembre de 1997, el Gobierno francés presenta un *Proyecto de Ley* relativo a la prevención y a la represión de las infracciones sexuales y la protección de menores que establece como circunstancia agravante el uso de Internet (*Projet de loi rélatif à la prévention et à la represión des infractions sexuelles ainsi qu à la protection des mineurs)* que es rechazado. En marzo de 2000 se modifica la *Ley de lo Audiovisual.*

La primera propuesta detallada aparece en el Informe elaborado por el Consejo de Estado de julio de 1998. Las soluciones pasarían por las medidas siguientes: primera, imponer al proveedor de servicios la obligación de identificar al proveedor o desarrollador de contenidos. Segunda, imponer a los proveedores de acceso la obligación de identificar a sus abonados cuando, en el marco de una investigación, así les fuera requerido por la policía y la Justicia -en estos casos el anonimato seguiría siendo posible a través del uso de pseudónimos-. Para evitar el anonimato en las suscripciones gratuitas (cuenta de correo gratuita, alojamiento gratuito de páginas web, acceso gratuito a Internet, etc.), el Informe propone utilizar medios complementarios, como el envío de cartas de confirmación, para limitar la comisión de infracciones por parte del usuario amparado en el anonimato. Tercera, imponer a los proveedores de acceso el deber de conservar los datos de conexión. Son datos que los proveedores de acceso guardan de manera automática (el *login,* las horas de principio y final de la conexión, el número IP del que llama y los sitios web visitados) y poseen un gran valor informativo para la policía. Aunque es una medida difícilmente aplicable para el envío de mensajes de correo electrónico y para los foros de discusión.

Estas medidas se materializaron en marzo de 2000, cuando el Gobierno francés elaboró un proyecto de Ley que impone a los proveedores o prestadores de servicios de Internet la obligación de identificar al proveedor o desarrollador de contenidos, sancionando su incumplimiento con una multa de siete mil euros y pena de hasta seis meses de prisión. La disposición levantó las protestas de los grupos defensores de la libertad de expresión y de la privacidad de las comunicaciones, a las que se han sumado las quejas de los proveedoreso prestadores de servicios, que de nuevo amenazan con establecerse fuera del territorio nacional si se les impone la obligación de controlar los contenidos introducidos por los usuarios en sus sistemas informáticos y temen que disposiciones como éstas se generalicen a otros Estados miembros.

La jurisprudencia francesa ha abordado en varias ocasiones el alcance de la responsabilidad de los proveedores o prestadores de servicios de Internet. En apenas dos años se han producido cerca de una veintena de casos de responsabilidad por contenidos ilícitos y nocivos (racismo, xenofobia, pornografía y pederastia, negación del holocausto judío, vulneración del derecho a la intimidad y a la propia imagen, difamación, etc.). Un análisis de la jurisprudencia reciente pone de manifiesto la falta de uniformidad en las respuestas dadas por los jueces y tribunales franceses, que en unos casos establecían la responsabilidad del intermediario, y en otros le exoneraba, o incluso rechazaban el caso basándose en la generalidad de la demanda interpuesta[110].

En 1998, Estelle Halliday[111], como ya se veía, había demandado a *Altern-org.*, un proveedor de alojamiento gratuito de páginas web, por albergar un sitio web desde el que se difundían imágenes que vulneraban el derecho a la propia imagen de la demandante. El juez estimó que para que el proveedor de alojamiento pudiera eximirse de responsabilidad debía probar que había cumplido con sus obligación de informar al usuario sobre las normas de respeto de los derechos de la personalidad y a los derechos de propiedad intelectual e industrial. El juez consideró que el proveedor de alojamiento tiene la obligación de velar por la buena moralidad de los contenidos que aloja, respetar las reglas deontológicas que rigen en Internet así como las leyes, reglamentos y derechos de terceros.

La obligación de supervisión u "obligación de velar por la buena moralidad" de los contenidos, convertía automáticamente al proveedor de alojamiento en responsable

[110] Asunto *UEFJ c. Cavalcom*. Ordonance de référé de 12 de junio de 1996. Tribunal de Grande Instante de Paris. Affaire Union Étudiants Juifs de France c. Cavalcon et autres. Nueve proveedores de acceso a Internet fueron demandados por dar acceso a mensajes y documentos antisemitas que podían ser consultados en los sitios web y foros de discusión. La demanda fue rechazada por ser demasiado general e imprecisa. Los proveedores de acceso se comprometieron a efectuar una vigilancia de los servicios alojados y adaptar sus contratos de difusión para prohibir la difusión de mensajes contrarios a las leyes francesas.
[111] Asunto*Estelle Halliday c Valentin Lacambre*. Ordennance de référé de 9 de junio de 1998. Tribunal de Grande Instante de Paris. Affaire Estelle Halliday c. Valentin LaCambre et Daniel.

editorial por los contenidos que albergaba, del mismo modo que lo era el editor de un periódico en el que se contiene un artículo difamatorio.

La sentencia fue duramente criticada por las asociaciones de proveedores de servicios y las asociaciones defensoras de la libertad de expresión. Los primeros temían que la aplicación de los estándares de la prensa escrita supondría un grave obstáculo a su actividad en las redes digitales que expulsaría del mercado a las pequeñas empresas. Los segundos temían que los proveedores de servicios de Internet se convirtieran en censores -controlando los contenidos- con el fin de eludir la responsabilidad por los contenidos introducidos por sus usuarios.

Ambos colectivos respiraron aliviados cuando en septiembre de 1999, en el asunto *Axa c. Infonie,* en el que se demandó a un proveedor de alojamiento por una página web difamatoria, un juez francés dictaminó que la responsabilidad del proveedor de alojamiento no podía equiparse a la responsabilidad editorial. En la medida en que no cabía imponer una obligación de supervisión de los contenidos que transitaban por su sistema, tampoco podía ser considerado responsable por las informaciones ilícitas o nocivas introducidas por sus clientes. Fue así como *Infonie,* el proveedor de alojamiento de sitios web, no fue considerado responsable por los contenidos ilícitos albergados en su sistema.

En el caso de Francia, el usuario puede incurrir en responsabilidad penal al "descargar" de la Red material ilícito, y siempre que la conducta esté tipificada como delito.

El Instituto Nacional francés de Investigación en Informática (INRIA) ha elaborado un programa informático llamado "Surfimage", capaz de analizar imágenes informáticas a gran velocidad, el cual ha sido empleado a título experimental en los ordenadores de un organismo oficial dedicado a la protección de menores.

4.2.5. HOLANDA

En Holanda se creó una iniciativa autorreguladora: un hot line contra la pornografía infantil en Internet. Para ello, se formó un grupo compuesto por algunos proveedores de servicios de Internet, usuarios y algunos representantes de las autoridades, con la intención de mantener la independencia de la línea y que ésta no represente a los intereses de un sector. La forma de trabajo de la presente línea consistía en advertir a las personas que publican estos materiales y a decirles que están cometiendo un delito. Si no eliminaban esos materiales después de haber sido advertidos por la "línea caliente", ésta informaba de sus actividades a la policía y se abstenía de ulteriores actuaciones.

Se ha considerado que el caso de autorregulación en Holanda es uno de los pocos sistemas que funciona y que respeta dichas garantías.

4.2.6. REINO UNIDO

Algunos países optaron por modificar las leyes existentes para adaptarlas al entorno digital. En el Reino Unido, por ejemplo, la *Protection of Children Act* de 1978, reformada en 1994 por la *Criminal Justice and Order Act*, ampliaba el concepto de "publicación" para incluir el de "transmisión electrónica".

Dos años más tarde comenzaron las denuncias por distribución de pornografía infantil en Internet. En mayo de 1996, en el caso de la Universidad de Birmingham *(R* v. *Fellows y* R v *Arnold*[112]*)* se plantea por primera vez la cuestión de dilucidar si las imágenes almacenadas en el disco duro del ordenador *y* en disquetes podían ser consideradas "fotografías". Alban Fellows fue condenado a tres años de prisión por

distribución de pornografía infantil en la Red. Las fotografías se las proporcionaba Stephen Arnold que también fue condenado. El caso fue objeto de recurso y el Tribunal de Apelación confirmó la decisión dada en Primera Instancia. El juez consideró que las imágenes almacenadas en el disco duro del ordenador eran fotografías, mientras que las guardadas en disquetes eran una "copia de una fotografía indecente"; efectivamente, el disquete contenía datos no apreciables a simple vista pero que podían ser convertidos en una copia que reproducía con total fidelidad la fotografía original.

En el Reino Unido su proyecto de ley sobre *Regulation of Investigatory Powers Bill* de 2000 prevé estrictas medidas para localizar a los presuntos autores de conductas ilícitas en la Red.

Por otro lado, un grupo de «hackers» británico ha creado un peculiar virus informático llamado Noped que, sin causar daños en el sistema del equipo que se ven afectados por él, rastrea los ordenadores que almacenan imágenes de pornografía infantil y denuncia ante las autoridades a sus propietarios a través de un correo electrónico que se envía desde el ordenador del sospechoso hasta diferentes agencias gubernamentales, FBI y Scotland Yard incluidos.

Por el momento, la policía británica ha anunciado que no actuará a las alertas de este 'gusano', ya que consideran que la investigación de la pornografía infantil "es un área delicada". Por su parte, las compañías antivirus han anunciado que el virus no es muy dañino[113].

Existe otro virus denominado marras, de tipo gusano, se acompaña de un expresivo mensaje («Help us all to end illegal child porn now» —«Ayúdanos a acabar con la pornografía infantil ahora»—) así como de un documento adjunto en la que se

[112] *R v Fellows y R v Arnold* (mayo de 1996).
[113] Consultar web http://www.ciberestrella.com/010602/articulos/piratas.htm

recuerdan las penas legales reservadas a los pedófilos. Sin embargo, esta voluntariosa colaboración de la comunidad «hacker» no ha gustado demasiado a la Policía británica. De hecho, los agentes admiten que no están respondiendo a las denuncias que, de forma persistente, llegan a sus terminales informáticas en forma de mensaje de correo electrónico[114].

Scotland Yard considera que la lucha contra la pornografía infantil es un asunto demasiado serio y delicado como para aceptar el apoyo de los piratas informáticos en su afán por acabar con esta lacra, más cuando muchas veces los esfuerzos policiales se encaminan a evitar la comisión de alguna acción ilegal protagonizada por los propios «hackers». Éstos tampoco confían demasiado en su acción, salvo porque les puede granjear las simpatías de los usuarios de Internet. También porque muchos están hartos de que se les tilde de delincuentes —aunque sea informáticos— y de que incluso se les incluya en el mismo saco que a los pedófilos cibernéticos[115].

Cabe señalar que en el Reino Unido, se han elaborado códigos de conducta y se creó un organismo independiente -la Safety Net Foundation- que mantiene una línea telemática directa a la que se pueden denunciar aquellos contenidos que se consideren ilícitos.

El Gobierno británico se ha manifestado por las soluciones autorreguladoras en lugar de las soluciones legales. El gobierno ha favorecido algunas de éstas iniciativas, pero éstas se encuentran desarrolladas o aplicadas por organismos cuasi-gubernamentales como por ejemplo la Internet Wacth Foundation –IWF-.

IWF es un organismo autorregulador, que apoyado por el gobierno británico, fue en principio una *línea caliente* para abordar la existencia de contenidos ilegales en

[114] www.delitosinformaticos.com. HACKERS BRITANICOS CREAN UN VIRUS CONTRA LA PORNOGRAFIA INFANTIL EN INTERNET. 2 de junio de 2001.
[115] www.delitosinformaticos.com. ABC. MATERIA DELICADA

Internet. Luego la IWF se ha ocupado del desarrollo de sistemas de clasificación en el Reino Unido, y en 1998 recomendó estos sistemas como la mejor forma de tratar la disponibilidad del contenido nocivo de Internet, especialmente para los menores.

El problema radica que en el Reino Unido, éste tipo de autorregulación se ha visto distorsionado, pues, se ha llegado a censurar material sin un debate público en el parlamento o en otro lugar, y claro, suena tentador el identificar y tratar de bloquear newsgroups, sitios web y otros foros de Internet que parecen dedicarse a difundir material ilegal, pero ello implica una censura privatizada la cual no cumple con la legalidad de un debido proceso y vulnera el derecho de defensa del presunto infractor.

La tensión apuntada se refleja en un ejemplo, ocurrido en el Reino Unido y su proyecto de *Regulation of Investigatory Powers Hill*[116] de marzo de 2000, que autoriza a las autoridades policiales a solicitar de los usuarios su clave de acceso para investigar los contenidos de sus sistemas informáticos. El hecho de que el usuario no les proporcione su clave de acceso será considerado delito.

Las asociaciones a favor de las libertades públicas han acusado al Gobierno británico de criminal izar el uso de los ordenadores; de convertir a los intermediarios en entidades de control de los contenidos; de violar la presunción de inocencia; y perjudicar el desarrollo del comercio electrónico.

En el Reino Unido, el caso *Shetland Times vs. Wills* 1996[117] planteó la responsabilidad del proveedor o desarrollador de contenidos por vulneración de los derechos de propiedad intelectual. El demandado -el periódico *Shetland News*- incluía hipervínculos en su sitio web con los titulares del sitio web del *Shetland*

[116] *Regulation of Investigatory Powers Hill de marzo de 2000.*
[117] *The Shetland Times Limited vs. Wills and another*, de 24 de octubre de 1996. Decisión of the Court of Session, Outer House, Escocia (Reino Unido).

Times -el periódico de mayor difusión de la isla escocesa- vulnerando los derechos de autor de éste último.

En el Reino Unido también se plantearon tempranamente los casos de responsabilidad de los proveedores o prestadores de servicios por los contenidos ilícitos introducidos en Internet por los usuarios. De acuerdo con la legislación británica *(Defamation Act* de 1996), un proveedor de servicios queda exonerado de responsabilidad por los contenidos ilícitos que alberga si satisface dos requisitos: por una parte, que adopte todas las medidas razonables para evitar que el material ilícito sea introducido en la Red; por otra, que proceda a la retirada del material infractor una vez le sea notificada la existencia del mismo en su sistema informático. Este fue el caso de *Geodfrey c. Demon Internet*[118], en el que las partes se pusieron de acuerdo en marzo de 2000, dejando sin resolver la cuestión acerca de la responsabilidad del proveedor o prestador de servicios. A pesar de ello, fue la chispa que encendió los debates que enfrentarían a las autoridades públicas, industria, usuarios y asociaciones pro-libertad de expresión.

4.2.7. SUECIA

En Suecia, la Ley sobre los operadores de tablones de anuncios electrónicos (BBS), de mayo de 1997, imponía a los proveedores prestadores de servicios la obligación de controlar los contenidos con el fin de proceder a la retirada de materiales ilícitos como la pornografía infantil, el racismo y xenofobia o las vulneraciones de los derechos de autor. Curiosamente, la Ley sueca no menciona las violaciones del derecho a la intimidad, al honor y a la propia imagen. Esta Ley fue el resultado de la sensibilización del país tras unos sonados casos de pornografía infantil en Internet que conmocionaron a la opinión pública. La Ley, sin embargo,

[118] El Sr. Godfrey, profesor británico, demandó en 1997 a un PSI . *Demon*- por permitir que sus clientes difundieran mensajes difamatorios en uno de los grupos de noticias que albergaba (soc.cultura, thai). El Sr. Godfrey había solicitado a *Demon* que retirase los mensajes, a lo que *Demon* se opuso.

levantó numerosas protestas por parte de las empresas intermediarias, que amenazaron con emigrar a países vecinos para eludir la obligación de controlar los contenidos.

A pesar de esta tendencia, la propuesta de Directiva apuesta por la solución contraria, más en la línea de la DMCA de 1998. Los proveedores de servicios de Internet no están obligados a controlar o supervisar los contenidos que transitan por sus sistemas informáticos, El "deber de velar por la buena moralidad de los clientes" no es aplicable a un entorno digital en el que la información se traslada rápidamente de lugar y además, es difícil detectar el origen y el destino de la transmisión.

La solución satisface tanto a las asociaciones de proveedores o prestadores de servicios, que se liberan de instalar costosos sistemas y supervisión de los contenidos introducidos en la Red por sus usuarios, como a las asociaciones a favor de la libertad de expresión que, aliviadas, ven cómo desaparece la amenaza de censura que hubiera sido obligación de los proveedores de servicios. Otros colectivos (asociaciones que representan los intereses de los titulares de los derechos de autor, las asociaciones de padres y educadores y las asociaciones de protección de menores) lamentan que se haya perdido una oportunidad de combatir la difusión de material ilícito y nocivo en Internet.

La ausencia de obligación de control de contenidos no es absoluta. Las autoridades judiciales pueden imponer a los proveedores de servicios la obligación de supervisar, selectiva y transitoriamente, los contenidos presuntamente ilícitos cuando ello resulte necesario para garantizar la seguridad del Estado, la Defensa, la Seguridad pública, y para prevenir, investigar, detectar, y perseguir infracciones penales.

Finalmente, otros Estados europeos (Austria o Suiza) optaron por aplicar la legislación existente para sancionar las conductas delictivas cometidas en las redes digitales, a pesar de que la legislación no estuviera pensada para este tipo de delitos.

¿Cuál es el problema de las respuestas nacionales a los contenidos ilícitos en Internet? Las leyes cuya formulación era demasiado genérica han sido anuladas por los propios tribunales del Estado (Francia, Estados Unidos). Los países que han modificado su legislación para adaptarla al entorno digital sólo pueden perseguir los delitos que se cometan en su territorio (por ejemplo, sólo se persiguen en España si la persona que lleva a cabo la conducta tiene allí su domicilio). Entonces, ¿qué ocurre cuando el proveedor de contenidos ilícitos tiene su domicilio en el extranjero? Señalemos que suele ser lo más frecuente, pues, a lo largo del año 1999, la mayor parte de servidores de pornografía infantil detectados estaban establecidos en países de Europa del Este, Asia o en los Estados Unidos. Este motivo ha llevado a los Estados a buscar soluciones desde instancias internacionales que permitan afrontar con éxito los problemas que plantean las infracciones cometidas en Internet.

Austria va más lejos y tras la alarma social que generó el desmantelamiento de redes de pederastia en su territorio ha propuesto recientemente a sus socios comunitarios que endurezcan las sanciones a los proveedores de servicios cuando incumplan su obligación de identificar al usuario que ha llevado a cabo la actividad ilícita[119].

Otros ejemplos los encontramos en Irlanda[120] y en la República de Sudáfrica[121], que también han modificado recientemente sus leyes con el fin de ampliar el concepto de ciertas conductas delictivas, de manera que quedan englobadas las que

[119] Iniciativa de la República de Austria con vistas a la adopción de la Decisión del Consejo relativa a la lucha contra la pornografía infantil en Internet. 1999/C362/06 (DOC 362, de 16 de diciembre de 1999).
[120] En Irlanda fue aprobada, el 29 de junio de 1998, la *Child Trafficking and Pornography Act* 1998. La Ley condena la producción, difusión y posesión de pornografía infantil con multas de hasta 1 500 Libras irlandesas y/o hasta 12 meses de prisión.
[121] La República de Sudáfrica ha modificado el 30 de abril de 1999 la *Films and Publications Act* de 1996 para incluir la pornografía infantil a través de Internet, *Government Gazette*, núm. 19980, vol. 406.

tienen lugar en Internet (por ejemplo, la elaboración, posesión y distribución de pornografía infantil).

Las modificaciones introducidas en las legislaciones nacionales para luchar contra los contenidos ilícitos parecen escasas. Se limitan a ampliar el concepto de "publicación" y "fotografía" para adaptarlo al entorno digital y a castigar la elaboración, posesión y distribución de pornografía infantil.

4.2.8. CANADA

El gobierno canadiense aprobó nueva legislación, la más estricta del mundo, para combatir la pornografía infantil en la Internet. La misma establece como delito no sólo producir o publicar imágenes indecentes de niños, sino incluso acceder a ellas en un sitio de la red. También permitirá llevar ante los tribunales en Canadá a personas que cometieron delitos relacionados con la pornografía en cualquier lugar del mundo.

Las penas que acompañarán a la nueva clasificación de delitos consideran por ejemplo que abrir una página de Internet que contenga pornografía infantil sería castigado con una sentencia de hasta 5 años de prisión. Producir y transmitir pornografía infantil a través de correo electrónico o páginas de la red llevará una pena de hasta 10 años.

El ministro de Justicia canadiense, Anne MacLellan, explicó que la nueva legislación era necesaria para cubrir una nueva tecnología, la Internet, que "se está utilizando para cometer terribles delitos[122]".

[122] Consultar web Datosenlaweb.com.

En Internet, lo habitual es que un acto ilícito afecte a una pluralidad de víctimas que tengan su residencia o domicilio en Estados diferentes, o incluso que sean varios los proveedores de contenidos ilícitos provenientes de países distintos.

En estos casos, es evidente el conflicto entre la libre circulación de información y la necesidad de castigar y perseguir las conductas ilícitas. Los Estados deben tomar medidas[123] para aumentar la cooperación judicial y policial, especialmente en el ámbito de la formación tecnológica y la asistencia recíproca, con el fin de impedir y combatir los contenidos ilícitos.

4.2.9. BALANCE DE LA SITUACION EN MEXICO

El uso de Internet ha aumentado considerablemente en los últimos años, y las previsiones son de un crecimiento aún mayor. Por tanto, Internet -al igual que en el resto de los países europeos- va a tener profundas repercusiones en la sociedad y en el Derecho.

La Policía Federal Preventiva, que depende de la Secretaría de Seguridad Pública Federal, ha desarrollado en México la primera Unidad de Policía Cibernética, que cuenta con un área especifica en materia de investigación de delitos contra menores, al igual que se hace ya en los países industrializados[124].

La Policía Cibernética tiene como objetivos principales detectar las organizaciones criminales de pedófilos, las mafias de prostitución infantil que promueven y transmiten pornografía infantil, que operan desde México vía Internet[125], para combatir la explotación sexual infantil y la práctica de ritos satánicos donde se

[123] Principios y el Plan de Acción del G/8 en Diciembre de 1997 para luchar contra la delincuencia de alta tecnología.
[124] REYES, Jorge. Periódico Reforma. 11 de julio de 2001.
[125] OROZCO, Mónica. RASTREARA LA POLICIA CIBERNETICA BANDAS DE PORNOGRAFÍA INFANTIL. Periódico La Jornada. Julio 2001.

realizan sacrificios de menores y animales en sus ceremonias; asimismo desmantelar organizaciones que se dedican a la explotación y al reclutamiento de niños para abusar sexualmente de ellos. Más recientemente se han ampliado sus fuciones para recibir cualquier denuncia sobre contenidos ilícitos en la Red cuyo lugar de origen sea el pais.

La nueva Policía cibernética despliega operaciones, de manera encubierta, para detectar y erradicar sitios mexicanos en Internet donde se transmite pornografía infantil como ya también otros contenidos de carácter ilícito.

El personal que encabeza a la Policía Cibernética, son policías profesionales, jóvenes con conocimiento en sociología, derecho y son expertos en sistemas de cómputo, con la capacidad de detectar cuando los mensajes tienen algo que contacte al joven o al niño despertándole algún interés. En sus inicios fue Integrada con 60 elementos que realizan operaciones a diario en las páginas de la web, las 24 horas del día. El personal se prepara constantemente para poder obtener ese tipo de información y tener acceso a ella. Intentan identificar las líneas, los sitios donde tratan de enganchar a los niños o de poderlos involucrar en este tipo de delitos por ejemplo.

A través de la denuncia ciudadana (Centro de Nacional de Atención Ciudadana – CNAC-) la dependencia trabaja con jóvenes funcionarios en los sistemas de Internet, que navegan en él para detectar bandas de criminales que se dedican a la pornografía infantil y explotación de menores, buscan encontrar delitos que pudieran representar un riesgo para los menores.

Realizan operaciones de patrullaje antihackers en la Internet y se utiliza la web como instrumento para atrapar a los delincuentes que cometan fraudes y organicen sus actividades delictivas en la red.

Analizan la información recolectada en campo para combatir los delitos que tienen lugar en internet y que son cometidos de manera particular contra menores.

Despliegan operaciones en la red para detectar sitios donde se transmite pornografía infantil y/o donde un menor puede ser contactado por pedófilos.

Planean y desarrollan investigaciones en campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Alberto Caballero, Jefe de la Policía Cibernética y Delitos Menores Contra Menores de la Policía Federal Preventiva (PFP), durante su participación en el 9° Congreso de Internet, realizado por la Universidad Nacional Autónoma de México reconoció no ser superpolicía ni contar con equipo de alta tecnología. Las actividades de este grupo se limitan al "patrullaje" en Internet y a la colaboración con homólogos internacionales. Durante los primeros meses de trabajao se detectaron 13 mil sitios de pornografía en la Web.[126]

Dado que en la red se ofrecen y se ofertan todo tipo de servicios, la Policía Cibernética realiza una permanente lucha para detectar este tipo de mensajes por internet, así como localizar a los grupos encargados del reclutamiento de menores de edad en la calle, donde son convencidos con obsequios, drogados o alcoholizados, con el propósito de pervertirlos y de explotarlos sexualmente.

Las tareas de esta Unidad Cibernética se extenderán por todo el país, así la Policía Federal Preventiva de México puso en funcionamiento, en el Estado de Jalisco, una Unidad Cibernética especializada en prevenir y erradicar el comercio y la explotación sexual infantil a través de Internet.

---

[126] CARDENAS VALDEZ, Octavio. El Universal. Mediante un chat en 15 días pueden abusar de sus hijos. 12 de noviembre de 2001. Pág. 14.

Por ello, con base a las labores realizadas por los jóvenes en la PFP, encargados en este tipo de trabajos, se ha logrado con éxito desmembrar bandas, consignando personas implicadas, así mismo han detectado gente que delinque en este delito.

Respecto de sitios de Internet, se han reportado nueve casos, la mayoría en las llamadas comunidades, tanto en MSN como en Yahoo. Por medio del ciberpatrullaje se han localizado más de 10 mil comunidades de tipo lésbico-gay; destacan 4 que se organizan desde México (Morelos, D.F., Guerrero y Jalisco).

Nicolás Suárez Valenzuela Coordinador General de la Inteligencia para la prevención de la PFP, en reunión con la Comisión de Atención a Grupos Vulnerables, de la Cámara de Diputados, explicó que ese tipo de delitos electrónicos han sido calificados como "perfectos", ya que es difícil que la autoridad actúe en contra de los victimarios, de ahí que, por eso, señaló la necesidad de reforzar o reformar las leyes para brindar una mayor protección a los menores de edad y, sobre todo, penalizar severamente a los responsables de la comisión de esos ilícitos.[127]

La investigación, el estudio y hasta los casos frustrados para detener pederastas en flagrancia en México han dado a los agentes de inteligencia de la PFP elementos para determinar el *modus operandi* tanto de los integrantes como de las redes de crimen organizado dedicadas al robo, tráfico y uso de menores en actividades relacionadas con el negocio sexual y la pornografía infantil.

Antonio del Valle Martínez, Director General de Protección de los Derechos Humanos de la Secretaría de Seguridad Pública Federal anunció que con los datos recabados en las investigaciones se ha puesto en marcha el desarrollo del primer banco nacional sobre pedófilos (personas que buscan relaciones sexuales con menores de edad) en México, bandas de "robachicos" (dedicadas al robo de

menores) y de gente involucrada en delitos de alto impacto, como asesinos en serie, registrando su perfil, *modus operandi,* patrones y razgos, para establecer un registro de delincuentes. Cruzando la información con dependencias locales, federales e internacionales.

La carencia de un marco jurídico que regule la práctica ilegal de la pedofilia en internet llevó a las autoridades federales a la creación de la Unidad de Policía Cibernética, adscrita a la Coordinación General de Inteligencia de la Policía Federal Preventiva, para erradicar la propagación de *webs* de prostitución infantil, cuya labor es frenar a los hackers, habilidosos cibernautas proveedores de pornografía de menores, quienes roban las cuentas de correo de los servidores y envían los *links* a millones de usuarios, como ya se señaló.

Nicolás Suárez Valenzuela, Coordinador General de Inteligencia para la Prevención de la PFP, en una reunión con integrantes de la Comisión de Atención Especial a Grupos Vulnerables de la Cámara de Diputados, el funcionario hizo un llamado a los legisladores para que refuercen las leyes y den mayor protección a los menores de edad, así como castigos ejemplares a los responsables de la corrupción de menores. De acuerdo con Suárez Valenzuela, la pornografía infantil y la pedofilia en Internet está alcanzando niveles alarmantes en México y por ello es urgente crear una legislación en la que esos delitos sean catalogados como graves y de carácter federal[128].

Es urgente que las autoridades unifiquen esfuerzos con el Poder Legislativo, ya que la retroalimentación podrá disminuir el grado de impunidad con el que operan los delincuentes.

---

[127] REYES, Jorge. BUSCA LA PFP A PEDOFILOS EN INTERNERT. Periódico Reforma. 11 de julio de 2001.
[128] OROZCO, Mónica. RASTREARA LA POLICIA CIBERNETICA BANDAS DE PORNOGRAFÍA INFANTIL. La Jornada.

El funcionario solicitó a la comisión "legislar lo necesario" para que la policía pueda pedir a los proveedores de servicio de Internet los registros usados para cometer actividades delictivas en este medio y para que los jueces acepten como evidencia una prueba lógica presentada en cualquier medio magnético.

Del mismo modo, propuso la elaboración de convenios con los países de donde proviene el mayor número de turistas que buscan tener sexo con menores mexicanos, destacando que este punto parte del hecho de que al desmembrar una banda que operaba en Acapulco, Guerrero, detectaron que ésta tenía enlaces con organizaciones que operan en Estados Unidos, Canadá, Holanda, Rusia, Alemania, Australia y algunos países de Africa y Centro América.

Nicolás Suárez Valenzuela pidió a la sociedad estar al pendiente de los niños y jóvenes ya que México es un país joven y con grandes retos "por tal motivo los niños y los jóvenes significan el futuro de la nación y ante ello no se debe permitir que sea dañada nuestra sociedad" [129].

A modo de ejemplo cabe señalar que en España se envió al Congreso una nueva Ley de Telecomunicaciones, contiene un apartado sobre seguridad de los usuarios en los que se introducen novedosos esquemas para combatir y sancionar los delitos electrónicos como el fraude cibernético la utilización de las redes para fines ilícitos y espionaje virtual y telefónico.

La Comisión Federal de Telecomunicaciones (Cofetel) dijo que el ordenamiento contiene modificaciones jurídicas a fin de dar una mayor seguridad a usuarios y operadores mediante reglas más claras, ágiles y flexibles. Así además de la normatividad que se plantea en materia de seguridad, también hay un apartado sobre derechos del consumidor.

Se establece que es la primera vez que se plasma en un documento jurídico todo un esquema de protección a los usuarios, quienes ante el auge del comercio y los servicios electrónicos cada vez están más expuestos a ser victimas de delitos cibernéticos.

Este nuevo ordenamiento recoge lo nuevo de la actual ley, y llena vicios legales que se tienen por ejemplo en todo lo referente al comercio electrónico y transacciones financieras que se realizan por esta vía, a fin de establecer una legislación que norme y regule estas operaciones, asegurando fuentes de la cofetel.

De igual forma, en esta ley se trata lo referente a "seguridad y privacía" de los usuarios, lo cual es una novedad en el país y a la vez una necesidad, dado el auge de delitos de este tipo que se cometen.

Las fuentes consultadas resaltaron que por primera vez en un ordenamiento se tendrán previstos este tipo de ilícitos, ya que actualmente las víctimas tienen que recurrir a diversas leyes y amparos para proteger sus derechos. Pues existe un vacio legal en este sentido.

En la nueva ley se describen las operaciones electrónicas ilegales, como son el fraude, el abuso, el espionaje y otros, y un punto fundamental es que se prevén sanciones para estos delitos "modernos" que no estaban tipificados como tales en nuestro país. Pero "lo mejor" es que no sólo se identifican como tales y se les otorga características de actos culposos, sino también se les impone una sanción.

Los castigos, multas y sanciones a los ilícitos estarán contenidos en el Reglamento para Comercializadoras de Servicios de Telecomunicaciones, el cual acompañará a la iniciativa que será enviada a los legisladores para su análisis[130].

---

[129] Op cit.
[130] MUÑOS RIOS, Patricia. MAYORES SANCIONES PARA COMBATIR DELITOS ELECTRONICOS Y CIBERNETICOS.

Alberto Caballero, Jefe de la Policía Cibernética y Delitos Menores Contra Menores de la Policía Federal Preventiva(PFP), durante su participación en el 9° Congreso de Internet, "Internet en la encrucijada" realizado por la Universidad Nacional Autónoma de México reconoció que los delitos informáticos, como creación de virus, instrusión en páginas y hackeo, por ejemplo, no están tipificados en la legislación mexicana, lo que complica su tarea; por lo que trabajan de cerca con legisladores. "Incluso –dijo- la figura de "pedofilo", no aparece en ninguna ley del país".

Otra modificación necesaria es que proveedores de servicios de internet ofrezcan datos acerca de registros de usuarios, toda vez que "es muy fácil dar con una dirección IP, pero casi imposible conocer la dirección física de esa computadora. Operadores como TELMEX nos exigen órdenes judiciales para poder entregarnos esa información", acató Caballero.

Por último, el Jefe de la Policía Cibernética asentó que la mejor protección es educar a los menores sobre los usos y peligros de Internet vigilando sus actividades en línea y llevando prácticas de seguridad cotidiana como "no hablar con extraños", al mundo virtual.

Según un estudió, citó, realizado en cuatro chats, de cien usuarios menores de 13 años, 56% dio su número telefónico, 22% su dirección, 66% en que escuella estudiaba y 57% habló de la rutina de su familia, sin duda datos alarmantes[131].

No de balde a éstos crímenes se les ha tipificado como "perfectos", ya que resulta casi imposible que las autoridades puedan actuar en contra de los victimarios, por lo que los delitos quedan impunes.

[131] CARDENAS VALDEZ, Octavio. El Universal. Mediante un chat en 15 días pueden abusar de sus hijos. 12 de noviembre de 2001. Pág. 14.

Ante esa situación, la PFP y Diputados Federales coincidieron en que es necesario unificar esfuerzos, tanto legislativos como policiales, lo cual permitiría disminuir el desinterés de la policía para investigar estos casos, así como el grado de impunidad con que operan estos delincuentes.

Los diputados coincidieron en que es necesario reforzar las leyes que dan protección a los niños, así como legislar para que los castigos a los responsables de la comisión de este tipo de delitos no quede impune.

Al amparo de vacíos jurídicos y multiplicidad de legislaciones estatales que lo consideran "delito menor", el uso sexual de niños en México es "crimen en alarmante crecimiento", del cual la sociedad "es cómplice por omisión legal", afirma Angel, Agente encubierto de la Coordinación General de Inteligencia de la Policía Federal Preventiva (PFP), responsable del equipo que investiga la pederastia[132].

Esta omisión legal convierte al país en una especie de paraíso para traficante de menores y pederastras, entorpece el trabajo de la policía y, peor aún, mantiene en la orfandad jurídica a los niños.

Lamenta que exista una situación de falta de protección jurídica de los menores frente a sus victimarios, porque la llamada "pedofilia" no está considerada como un delito grave y en cada Estado el tratamiento es diferente" [133].

El robo de niños y el colateral abuso sexual de los menores en México, afirma, existe y aumenta. Es un fenómeno presente en la sociedad, pero sin respuesta articulada de las corporaciones policiacas y desatendido por el Congreso de la Unión y las legislaturas locales.

---

[132] Periódico La Jornada. MÉXICO, PARAÍSO DE LOS PEDERASTRAS. 18 de agosto de 2001.
[133] Ob cit.

El informe de la Coordinación General de Inteligencia, de la PFP, sintetiza: No existe un esfuerzo nacional que combata este tipo de crímenes y las legislaciones locales no son suficientes, lo que ocasiona falta de interés en la investigación policiaca y la consecuente impunidad de los depredadores.

"Tenemos las manos atadas pues no hay una verdadera autoridad para investigar delitos cibernéticos"; indicó el responsable de esta área, dependiente de la Policía Federal Preventiva (PFP). quien solicitó el anonimato por cuestiones de seguridad.

Si bien la Cámara de Diputados tiene en su haber varias propuestas para legislar el tema de la ciberdelincuencia (entre ellas la de la propia PFP), la mayoría sigue "en la congeladora".

El Director de la Policía Cibernética hizo un "llamado a la Cámara de Diputados para comenzar a legislar en estos temas "lo más pronto posible".

"Nosotros detectamos al delincuente pero no podemos arrestarlo si no existe una ley que sancione sus actividades", indicó[134].

Se debe resaltar que como muestra de una verdadera preocupación por parte de las autoridades y de la sociedad mexicana respecto a la pedofilia en Internet, el 4 de enero de 2000, fue reformado el Código Penal Federal, en la denominación del capítulo II, al igual que sus artículos, además de adicionársele lo relativo a la pornografía infantil, para quedar como sigue: *Corrupción de menores e incapaces. Pornografía infantil y prostitución sexual de menores.*

De igual forma el Código Federal de Procedimientos Penales fue reformado el 4 de enero de 2000 para incluir como "delito grave" la Corrupción de menores o

incapaces, previsto en el artículo 201; y *pornografía infantil*, previsto en el artículo 201 bis del Código Penal Federal.

Margarita Prieto señala que las principales características del delito informático que deben tenerse en cuenta al tipificarlo y sancionarlo son:[135]:

a) Que las consecuencias económicas son generalmente considerables, con un riesgo psíquico reducido para el autor del delito y sin violencia en la mayor parte de los casos.

b) Que la personalidad del delincuente y la preparación del delito son muy originales, debido a su creatividad y sofisticación técnica necesarias para realizar tales delitos.

c) Que las cuestiones de culpabilidad, tentativa y complicidad tienen un carácter menos concreto que en la criminalidad clásica; y

d) Que el delito informático es una realidad sociológica bien diferenciada, que tiende a convertirse en una categoría jurídica especial.

Aspectos que definitivamente deben ser considerados ante cualquier iniciativa legislativa para regular cualquier contenido ilicito en el Internet.

Así como en el sistema penal español se impulsó la modificación del Código Penal a fin de crear una nueva figura que castigara la simple posesión de material pornográfico que contuviera imágenes explícitas de explotación sexual de niños, pero siempre que aquella posesión estuviera orientada a la comercialización o exhibición, el acuerdo de los Quince también busca sancionar la simple tenencia de material pornográfico y unificar la descripción de los nuevos delitos incrementando las penas,

---

[134] Periódico La Jornada. 18 de agosto de 2001.
[135] MARGARITA GABRIELA PRIETO ACOSTA, *Informática Jurídica; el derecho ante un gran reto*, Tesis de Abogado Universidad Javeriana. Bogotá, 1984, pág. 46.

de esta manera mi propuesta también sería modificar la legislación penal mexicana en ese sentido.

Para el 31 de enero de 2000 se publica en la Gaceta Oficial del Distrito Federal la Ley de los Derechos de las Niñas y Niños en el Distrito Federal, en la que se señala de manera enunciativa mas no limitativa como derechos la vida, la integridad, la dignidad y a una vida libre de violencia entre otros (art. 5), posteriormente, el 29 de mayo de 2000 se publica en el Diario Oficial de la Federación la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, en la cual se establece el Derecho a ser protegidos en su integridad, en su libertad y contra el maltrato y el abuso sexual (art. 21), sin embargo considero que no es suficiente, pues los valores jurídicos protegidos son objeto de nuevas formas de ataque en las redes digitales, tal como los derechos al respeto a la vida privada o intimidad, al honor e incluso a la imagen propia, a través del Internet, los cuales son considerados ya como derechos humanos fundamentales, establecidos por diversos instrumentos internacionales, ya expuestos en el apartado 3.5 de esta tesis.

Dado que a tráves del Internet se han visto vulnerados muchos derechos tales como a la intimidad personal y familiar, al honor, a la propia imagen, a la privacidad informática, a la indemnidad sexual, a la propiedad intelectual, asimismo como a la libertad de expresión y de información se están utilizando herramientas tecnológicas para combatir determinada páginas web cuyos contenidos violan o rebsan dichos derechos. Organizaciones no gubernamentales apoyadas por el FBI de Estados Unidos "inyectan virus" a los sitios en la red, para combatir este problema, reveló el Comité Nacional de Consulta y Participación de la Comunidad en Seguridad Pública, -CONSEGU-[136].

[136] FERRER, Gladis. Periódico Reforma. México

Dicho comité presentó una campaña que comprende spots en televisión y radio, así como una página en Internet, con la cual se pretende hacer frente al problema de la explotación de menores en México por ejemplo.

"Que no ocurra en público, no quiere decir que no pasa. No contribuyas a la pornografía infantil", es uno de los lemas de la Campaña contra la Pornografía y Prostitución infantil que arrancó hace mas de un año.

Considerados entre los delitos más ocultos y que lesionan la integridad de un sector de la población sumamente vulnerable, como son los menores, la campaña pretende inhibir el consumo y concientizar a la población de la magnitud de este problema[137].

Salen sobrando los cuestionamientos sobre si ¿es necesario reformar el Derecho para adaptarlo a los nuevos tiempos? y ¿es preciso crear nuevos tipos penales para sancionar las nuevas conductas?. Los conceptos jurídicos tradicionales se ven cuestionados en el entorno digital y reclaman nuevas disposiciones.

CAPITULO V

MEDIDAS PARA EVITAR EL CONTENIDO ILICITO Y NOCIVO EN INTERNET

5.1. FILTRADO, BLOQUEO DE LOS CONTENIDOS Y SISTEMA DE CALIFICACION MORAL DE LOS CONTENIDOS

A principios de los años 90's muchas empresas informáticas[138] comenzaron a desarrollar programas de filtrado y bloqueo de los potencialmente nocivos para el normal desarrollo de los menores. De este modo, padres y educadores se sentirían más cómodos cuando los niños navegasen por la Red.

Estos programas permiten al usuario decidir cuáles son los contenidos de Internet a los que se puede acceder y cuáles no. El filtrado es un programa de software que se instala en el navegador de los ordenadores y constituye, a juicio de la Comisión Europea, una poderosa herramienta en la lucha contra el acceso a los contenidos nocivos.[139] Por ejemplo, el filtrado permite a los padres impedir que *sus* hijos accedan a contenidos violentos, al empresario bloquear el acceso de sus empleados a los *chat* en horas de trabajo, o a las asociaciones filtrar determinadas páginas web a sus miembros.

Existen distintos tipos de filtros: Unos se basan en las llamadas "listas negras", otros, en las "listas blancas", *y* finalmente, los que se basan en "listas neutras". En los primeros, el programa instala por defecto un listado de lugares prohibidos. Hay numerosos productos en el mercado que incluyen este tipo de listas de sitios web a los que se impide el acceso. Algunos de estos productos se especializan en temas

---

[137] Consultar web Reforma.com.mx.

[138] Net Sheperd, NetNanny, CyberPatrol, SurfWatch, Internet Watchdog, SOS Kidproof, Cyber Setter, WebChaperone, Bess, X-Stop, I-Gear, Internet Retriever, etc.

[139] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y social y al Comité de las Regiones sobre contenidos ilícitos y nocivos en Internet. COM (96) 487 Final, de 16 de octubre de 1996 (DO C 70, de 6 de marzo de 1997).

concretos, por ejemplo, el programa *ADL* filtra únicamente contenidos racistas, violentos y xenófobos, mientras que el programa *CyberPatrol* filtra contenidos sexuales. Éste último instala por defecto una lista secreta que se actualiza todas las semanas por lo que el usuario no sabe a que sitios web o grupos de noticias tiene restringido el acceso. El programa clasifica cerca de diez mil sitios web en doce categorías: violencia, lenguaje malsonante, representaciones obscenas, drogas, controversia/ilicitud, desnudos, racismo/tratamiento impropio de las razas, militancia/extremismo, alcohol/tabaco, acto sexual, cultos satánicos y juego.

Otros tienen como fundamento las "listas blancas". Son programas de software que permiten el acceso a los lugares expresamente enumerados en el listado. Por ejemplo, un profesor puede elegir los lugares a los que sus alumnos pueden acceder durante la lección beneficiándose de las posibilidades educativas que ofrece la Red.

Finalmente, los programas basados las "listas neutras". El más conocido es el mecanismo de filtrado PICS (Plataforma para la Selección de Contenidos de Internet) promovido en 1997 por el Consorcio del *World Wide Web*[140] (W3). Este programa permite al usuario establecer su propio sistema de filtrado de contenidos. Así, por ejemplo, los padres pueden elaborar un listado propio de lugares prohibidos para sus hijos, en función de los niveles que seleccionen en el programa, el cual les permite elegir el grado de sexo, violencia, o desnudez tolerable. Los centros educativos también pueden bloquear el acceso a los video-juegos o a los servidores de conversaciones en tiempo real durante las horas de clase.

La mayor ventaja de los filtros basados en listas neutras es su flexibilidad, puesto que permiten al usuario tomar decisiones individualizadas en función de sus valores éticos, morales, políticos o religiosos, que no tienen por qué coincidir con los de otra persona.

[140] Coalición que tiene el respaldo de fabricantes de software y de hardware, de proveedores de acceso y de servicios comerciales en línea, de editores y de proveedores de contenido. El Consorcio de la World Wide Web se ocupa de investigar las nuevas tecnologías relacionadas con la Red de Telaraña Mundial y tiene su sede en los Estados Unidos.

En los últimos años han surgido empresas que proporcionan una calificación moral de los contenidos de Internet a partir de un etiquetado *(/abel),* por ejemplo, sistemas como *RSACi* o *Safe Surf.*

El *RSACi,* o sistema de calificación de contenidos en Internet del Consejo Asesor sobre Programas Informáticos de Carácter Recreativo *(Recreational Software Advisory Council),* selecciona los sitios web y les atribuye una etiqueta en función de cuatro niveles: sexo, desnudez, lenguaje malsonante y violencia. Este sistema ha sido creado en los Estados Unidos, por la *Internet Content Rating Alliance,* que aplica un sistema de clasificación de contenidos de Internet similar al que utiliza respecto de los videojuegos. Los padres y educadores eligen el nivel y lo incorporan al navegador de su ordenador para bloquear los contenidos a los que no quieren que sus hijos accedan. A pesar de sus ventajas, el sistema *RSACi* no se ha generalizado entre los padres y educadores, quienes echan en falta una mayor cobertura de sitios web, pues el sistema *RSACi* etiqueta una pequeña porción de los millares de sitios web que existen en la Red.

El programa *SaftSurf* clasifica los contenidos de un modo contextual, por ejemplo, la clasificación de "materia sexual" abarca desde contenidos "artísticos" o "eróticos" hasta "pornografía explícita.

Ambos sistemas de calificación moral de los contenidos pueden ser incorporados a los programas de filtros basados en "listas neutras" (como el estándar PICS que se ha mencionado en el apartado anterior). Es el usuario quien decide cuál es el estándar que va a emplear para efectuar el filtrado.

Los sistemas de calificación moral de los contenidos plantean algunas cuestiones difíciles de responder, por ejemplo, ¿cuáles son los criterios en los que se basa la calificación moral de los contenidos? ¿quién determina estos criterios, el proveedor o

desarrollador de contenidos o un tercero? ¿qué consecuencias tendría sobre los proveedores de contenidos profesionales el hecho de que su sitio web sea objeto de una calificación moral? ¿en qué medida ese tercero podría convertirse en censor? Si el tercero fuese una empresa extranjera, por ejemplo, estadounidense, ¿sus criterios responderían a la sensibilidad mexicana o de cualquier otra? ¿sería adecuado elaborar sistemas de valoración moral diseñados específicamente para los mexicanos? ¿sería posible conseguir el consenso europeo para elaborar un sistema que abarque las diferentes sensibilidades culturales americanas, europeas? Estas y otras preguntas han frenado la expansión del uso de estos programas entre padres y educadores de todo el mundo.

Aunque los navegadores más populares, como las últimas versiones de Internet Explorer, incluyen una opción que limita los contenidos, esto no se considera un filtro, ni tampoco una amenaza contra la libertad en la Red. Al fin y al cabo sólo afectan a aquellos que deseen autolimitarse.

Los que se entiende por filtros, y los que son realmente polémicos por su potencial uso censor, son programas como Cyber Patrol, Net Nanny, Surf Watch, Cyber Sitter, WatchDog, X-Stop, Cyber Sentinel, SOS Kid Proof.

Los filtros limitan el acceso a Internet de diferentes maneras. La mayor parte funcionan como el corrector de Word, e impiden el acceso a las páginas en las que encuentra determinadas palabras malditas.

También incluyen otras funciones limitadoras: se puede programar el tiempo máximo de navegación, en qué momento del día se puede navegar, guarda el recorrido y las páginas visitadas, impide que se faciliten teléfonos y direcciones.

Y luego están las polémicas listas negras. Si una URL está fichada en la lista negra (diferente para guardián) el filtro la bloquea.

Dejando a un lado a los particulares, los principales usuarios de los filtros son las escuelas, universidades e instituciones con afán protector, algunos proveedores de acceso, y aquellas empresas especialmente preocupadas por la moral de sus empleados, o porque estos no pierdan el tiempo en determinados sitios.

Por una parte, los padres y educadores preocupados por lo que los niños visiten y hagan en sus horas de navegación. Por otra parte, y empujados por esos adultos tan preocupados por la inocencia infantil, han surgido numerosas asociaciones e iniciativas que presionan para filtrar los contenidos de la Red.

La protección de los menores frente a los contenidos ilícitos y nocivos en la Red requiere respuestas específicas. Los padres y educadores pueden hacer uso de mecanismos técnicos que permiten filtrar y bloquear los contenidos, de tal forma que los padres, por ejemplo, puedan decidir cuáles son los contenidos de Internet a los que sus hijos pueden tener acceso y cuáles no. La clasificación moral de los contenidos, la creación de espacios seguros -portales o navegadores- y el control de edad de los usuarios son otras alternativas complementarias.

En diciembre de 1997 más de 650 participantes (entre los que se encontraba el vicepresidente Al Gore), representantes de unas 300 organizaciones se unieron bajo la Internet Online Summit: Focus On Children, que exigía herramientas tecnológicas de control, un endurecimiento de la ley y un programa de concienciación para padres y escuelas.

En febrero de 1997 las Naciones Unidas se movilizaron para proteger a los niños de los riesgos de la Red bajo una iniciativa llamada "Inocencia en Peligro" apoyada por compañías como Lycos, Microsoft, AT&T, AOL, el FBI y la Federal Trade Commission entre otros. Bajo esta bandera se convocan conferencias, estudios y movilizaciones.

Los filtros están estrechamente vinculados a la Communications Decency Act (CDA) y la Child Online Protection Act (COPA). La primera CDA levantó numerosas protestas a finales de 1995 y en 1996 entre los internautas, e inundó la Red de lazos azules, símbolo de la libertad en Internet (frente al que estaba el lazo blanco[141], que se vio bastante menos). Tras ser aprobada por el Congreso y ratificada por Clinton, finalmente fue tachada de inconstitucional por el Supremo en junio de 1997 y descartada. En 1998 se intentó resucitar con una nueva versión, la CDA II.

La Child Online Protection Act (COPA) es la segunda tentativa de legislar los contenidos de Internet, esta vez mucho más centrada en la protección de la infancia. Ya ha sido aprobada por el Congreso, pero lleva más de un año paralizada aguardando a que se resuelva el debate sobre si atenta contra la primera enmienda de la Constitución norteamericana.

Algunos filtros incorporan terceros sistemas de control de contenidos como Recreational Software Advisory Council (RSAC) o SafeSurf, ambos basados en el estándar PICS de la World Wide Web Consortium (W3C) ,que clasifica los nodos igual que las películas dependiendo de cuatro categorías: desnudo, sexo explícito, violencia y palabras malsonantes, y que permiten al usuario escoger su nivel de libertad de navegación.

[141] Organización de hombres de todas las edades que han sumado sus esfuerzos para ayudar a poner fin a la violencia de los hombres contra las mujeres.

El miedo de muchos es que los filtros de Internet empiecen cuidando de la infancia y acaben censurando determinados contenidos basándose en intereses particulares. Precisamente por esto son la pieza más codiciada por hackers y programadores libertarios.

La historia de los filtros por tanto es un tira y afloja constante. Por una parte una serie de individuos sobradamente preparados se dedican a intentar romperlos, por la otra se potencian y se mejoran constantemente para resistir estos envistes.

La última escaramuza de este tipo la han protagonizado Cyber Patrol de Mattel y Cphack, una utilidad con la que dos programadores querían demostrar que en la lista negra del filtro se incluían nodos que no eran pornográficos ni violentos.

En contra de los filtros, y de cualquier tipo de limitación al crecimiento y al acceso a la Red, hay asociaciones, grupos e iniciativas que no descansan.

Como guardianes de los guardianes, destacan Electronic Privacy Information Center (EPIC), Peace Fire, Center For Democracy & Technology (CDT), Citizen Internet Enpowerment Coalition (CIEC) o Censorware.

Por ello, cabe resaltar que los filtros no son el medio más seguro y eficiente de protección de los menores frente al contenido obsceno que puedan encontrar en la Red; dada la misma naturaleza abierta y global de Internet, es imposible clasificar todos los contenidos pornográficos, además, de que la mayoría de los filtros de contenido están centrados en la WEB no filtrando el contenido que circula por el IRC - Internet Relay Chat y/o newsgroups.

No obstante, los filtros presentan algunos inconvenientes[142]:

Primero, pueden llegar a bloquear el acceso a otros sitios que no tienen por qué necesariamente ser ilícitos o nocivos, como por ejemplo a contenidos literarios, artísticos o científicos. Eso fue lo que ocurrió cuando al elaborar el listado de sitios web que contenían la palabra "seno" se incluyó un sitio web creado por una asociación de víctimas del cáncer de mama.

Segundo, el filtrado es un mecanismo de control de la recepción de la información, no de su distribución. *CyberPatrol,* por ejemplo, puede situarse a varios niveles: el ordenador personal, a nivel de *proxy,* o incluso a nivel nacional. Esto permite, por ejemplo, que determinados gobiernos corten el acceso de sus nacionales a páginas de contenido político democrático, de consumo, religioso, de libertad sexual y de opinión, etc. En consecuencia, las asociaciones a favor de la libertad de expresión han calificado el programa de filtrado como una nueva forma de censura.

Tercero. el filtrado no garantiza una seguridad total. El 17 de marzo de 2000 la empresa Mattel, propietaria del programa *CyberPatrol,* denunció en Estados Unidos a dos especialistas en criptografía por haber creado el programa *CyberrPatrol Hack* que muestra las contraseñas empleadas por los padres o los educadores para configurar el filtro, inutilizando el programa. Por otra parte. son dispositivos que los propios menores pueden fácilmente desconectar y por tanto inutilizar, sobre todo teniendo en cuenta los conocimientos de informática de los menores internautas, que suelen superar a los de sus progenitores.

Finalmente, también se ha acusado a los filtros de ser estándares americanos que no tienen por qué coincidir con los valores de otros países, especialmente los basados en listas negras y listas blancas.

[142] www.activobank.com. 3 de abril de 2002.

A pesar de estos inconvenientes, lo cierto es que países como Estados Unidos han promovido desde las instancias públicas el uso de los dispositivos de filtrado. La mencionada *Children's On Line Protetion Act* de 1998 (que fue objeto de recurso de inconstitucionalidad) obligaba a los colegios y bibliotecas públicas a instalar en sus ordenadores los programas de filtrado. Esta política encontró la oposición de los grupos a favor de la libertad de expresión, las asociaciones de bibliotecas y los profesores, que preferían ser ellos mismos, y no el gobierno, quienes decidiesen si debían implementarlos.

También el seno de la Unión Europea se han levantado voces en contra de la utilización de los programas de filtrado de contenidos. En la *Cumbre sobre los contenidos en Internet,* celebrada en Munich en 1999, organizada por una ONG alemana (Fundación Bertelsmann) se elaboró un memorando sobre la Autorregulación en Internet[143] que recomendaba el desarrollo de los sistemas de filtrado. Pero algunos grupos (educadores, abogados, organizaciones a favor de la defensa de la libertad de expresión) se opusieron, porque ello conllevaría un mayor intervencionismo estatal y la imposición de estándares morales nacionales en Internet[144].

Estos estándares morales son incompatibles con la salvaguarda de las diversidades culturales de Internet y con la posibilidad de que sean las propias familias las que decidan cuáles son los contenidos a los que pueden tener o no acceso sus hijos.

[143] Conferencia internacional celebrada los días 8 –10 de septiembre de 1999 en Munich, Alemania. *Internet Content Suummit. Self-regulation of Internet Content,* organizado por la fundación Bertelsmann.
[144] Véase el comunicado de prensa elaborado por la asociación a favor de la libertad de expresión *electronic Privacy Information Center* (EPIC).

5.2. LA CREACION DE ESPACIOS SEGUROS

La creación de espacios seguros es una forma de promover el lado positivo de Internet. Se trata de que las empresas de Internet elaboren "guarderías virtuales" en los que los niños sean destinatarios de contenidos que fomenten su sano desarrollo moral. Por ejemplo, a partir de la creación de portales especializados en contenidos para menores, donde los niños pueden encontrar todo tipo de contenidos educativos, lúdicos, etc. En Estados Unidos hay muchos ejemplos *(SurfMonkey, Your Own World, Kiddonet, Kahootz, Juniomet,* etc.). O bien, a partir del uso de navegadores especialmente diseñados para niños, que acogen los sitios web indicados para los menores.

Quizás la dificultad fundamental de estos espacios seguros consista en diseñarlos de tal manera que los menores se sientan cautivados por estos portales o navegadores específicos para ellos " y distraigan su interés por los portales a los que tienen acceso, sólo los adultos.

5.3. EL CONTROL DE EDAD

El control de edad es otro mecanismo que permite controlar el acceso de los menores a determinados sitios web. En la práctica, es difícil aplicar esta medida. El usuario de Internet puede fácilmente proporcionar datos falsos acerca de su edad. Incluso en los servicios de Internet que exigen al usuario el número de una tarjeta de crédito (por ejemplo, comprar un libro, o participar en casinos virtuales, o pujar en subastas), el proveedor o prestador del servicio no tiene posibilidad de saber si el contratante es el titular o su hijo. Además, el control de edad implica elevados costos económicos para los proveedores de contenidos y de servicios. Los proveedores "no

comerciales" dejarían de ser competitivos y se verían borrados del mercado al no poder afrontar los costos de los dispositivos de control de edad.

Es posible incrementar la seguridad en el uso de las redes digitales mediante iniciativas de los propios usuarios y de la industria. Los primeros deben ser informados sobre los riesgos y beneficios que entraña Internet; también deben estar a su disposición los mecanismos de protección de los menores. La industria puede ajustar su conducta a códigos deontológicos libre y voluntariamente elaborados.

Las medidas analizadas hasta ahora (filtrado, bloqueo, calificación moral de los contenidos, espacios seguros y control de la edad del usuario) no protegen por sí solas eficazmente a los menores frente a los contenidos ilícitos y nocivos de Internet. Por desgracia, determinados contenidos ilícitos y nocivos son tremendamente atractivos para los jóvenes, no tanto por su contenido, sino por lo que comporta el hecho de transgredir una prohibición. De poco sirve defender la casa con rejas si el habitante desea que el extraño entre.

Las soluciones que se exponen a continuación convierten en protagonistas a los sujetos que participan en la transmisión de la información en línea. Para aumentar la seguridad en la utilización de las redes digitales es necesario informar a los usuarios de los riesgos que implica la navegación en Internet, así como de las medidas de prevención de que disponen (filtrado, calificación, portales y navegado res seguros, etc.), educar a los niños y adolescentes en valores, que los actores elaboren códigos deontológicos y habilitar vías de denuncia para hacer efectivas las sanciones.

5.4. EDUCAR A LOS USUARIOS PARA UNA UTILIZACION RESPONSABLE DE INTERNET

La educación, instrucción y enseñanza como herramientas primordiales para poder proteger a los menores de cualquier tipo de abuso -la pornografía infantil en la red es una de las tantas variantes de abusos que pueden llevarse a cabo en contra de los niños- pues aunque no haya contacto esa forma burda, grosera y chocante de ver el sexo deja secuelas.

La información, la educación y la toma de conciencia de los riesgos de Internet es esencial para lograr una protección eficaz de los menores y de la dignidad humana. El *Libro Verde sobre la protección de los menores y de la dignidad humana*[145] de 1996 insta a padres e hijos a desarrollar una nueva relación con los medios audiovisuales, basada en el conocimiento de los riesgos que implica la navegación en la Red y la información acerca de los medios de protección existentes. En este punto, la educación de los usuarios es esencial. Los padres deben aprender a hacer uso de las redes digitales al igual que hacen sus hijos, siendo conscientes de los beneficios y riesgos que entraña navegar por Internet. Pero la responsabilidad de educar a los menores en el uso seguro de las nuevas tecnologías no reside únicamente en sus padres y educadores, sino que como indica el Consejo de Europa, en la *Recomendación R* (97) 19 *la violencia en los medios electrónicos*[146] es una tarea que debe ser compartida por los gobiernos y los proveedores o desarrolladores de contenidos. Sólo de este modo los menores pueden desarrollar una actitud crítica que les permita autoprotegerse. En el mismo texto se contienen líneas de actuación concretas para proteger a los menores frente a los contenidos

[145] Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información. COM (96) 483 Final, de 16 de octubre de 1996. La necesidad de informar a los usuarios de los riesgos que entraña la navegación por las redes digitales y de proporcionar a los padres las herramientas adecuadas para proteger a sus hijos de los contenidos ilícitos y nocivos en Internet se reitera en la Comunicación de la Comisión sobre los contenidos ilícitos y nocivos en Internet de 16 de octubre de 1996 y, más recientemente, en la Recomendación del Consejo de 24 de septiembre de 1998.

[146] Recomendación del Comité de Ministros del Consejo de Europa núm. R (97) 19 sobre la violencia en los medios electrónicos, de 30 de octubre de 1997.

violentos en los medios electrónicos, perfectamente válidas y aplicables a cualquier otro tipo de material ilícito y nocivo. Los padres y educadores deben desarrollar y mantener una actitud crítica frente a la violencia; promover el uso consciente y selectivo de los medios digitales, exigiendo al mismo tiempo calidad en los productos y servicios; estimular a los menores a desarrollar un criterio selectivo; y analizar las posibles vías de restringir el acceso de los menores a la violencia gratuita cuando ésta sea susceptible de afectar el desarrollo físico, mental o moral del menor. Se trata, por tanto, de promocionar un uso responsable de la Red a través del compromiso de todos los sectores implicados.

Las herramientas de filtrado, clasificación, navegación segura y portales para niños no sustituyen la tarea que les corresponde a los padres y educadores. Éstos deben ofrecer a los menores recursos suficientes para que puedan identificar comportamientos que trasciendan los límites tolerables; que no acepten insinuaciones de desconocidos en los *chat;* que no den sus datos personales cuando visitan una página web; que conozcan la existencia de las líneas directas u otros lugares adecuados para denunciar los abusos de que puedan ser objeto, como destinatarios de contenidos ilícitos (por ejemplo, el envío de mensajes obscenos) o como objeto de abusos directos en la vida real. El acceso a informaciones inadecuadas puede evitarse si los menores son educados para que se protejan frente a los abusos que existen tanto en el mundo real como en el mundo virtual.

Los padres y educadores deben tomar un papel activo en el aprendizaje de los menores y adolescentes en el uso de la Red a través del intercambio de experiencias y opiniones. Los padres pueden sentarse delante de la pantalla del ordenador con sus hijos y aprender a navegar con ellos por Internet. De lo contrario, se produciría el absurdo de que, si los padres no adquieren conocimientos de informática, acaben pidiéndoles a sus hijos que sean ellos mismos quienes instalen los programas de filtrado.

Una educación en valores, información suficiente y la atención necesaria por parte de los padres convertirán a Internet no en un sustituto de la educación, sino una herramienta complementaria.

A modo de ejemplo, en España, la Asociación de Usuarios de Internet dispone de una página web dedicada a los padres que les informa acerca de los beneficios y riesgos de Internet, cómo se pueden prevenir y reducir los riesgos así como algunos consejos prácticos para los padres.

5.5. LOS CODIGOS DE CONDUCTA

Los códigos de conducta suponen la autorregulación de los actores frente a la regulación estatal de los contenidos en Internet. El Estado, consciente de su imposibilidad de regular las redes digitales, se inhibe a favor de los actores -proveedores de contenidos y proveedores de servicios-, que reclaman la autonomía para ajustar su actividad a un código moral.

Los códigos deontológicos son un conjunto de normas elaboradas por los propios participantes en la transmisión de la información en línea en los que se establecen las obligaciones respecto de su actividad en Internet.

Ha habido numerosas iniciativas de autorregulación tanto en foros internacionales como en los propios Estados.

El primer Estado que llevó a cabo una propuesta relativa a la deontología de contenidos en Internet fue Francia, en la reunión celebrada en el seno de la OCDE en Seúl de octubre de 1996. La idea, sin embargo, no fue acogida por el resto de los Estados participantes.

En las reuniones posteriores de la OCDE[147] y octubre de 1997 y marzo de 1998[148] la posibilidad de autorregulación cobraba más fuerza. En estas reuniones hubo consenso en considerar que los códigos de conducta *(softlaw)* eran complementarios a la regulación estatal de los contenidos *(hardlaw)*. Asimismo, hubo consenso en otros puntos: la importancia de la formación y de la educación de los actores; la necesidad de colaboración entre los gobiernos, los usuarios y la industria en la lucha contra los contenidos ilícitos; y finalmente, la toma de conciencia respecto de la interdependencia de todos los países y la necesidad de la cooperación internacional.

El informe elaborado en septiembre de 1999 por la Fundación Bertelsmann en la *Cumbre sobre los contenidos en Internet*[149] da un paso adelante y dicta recomendaciones específicas para los gobiernos y la industria así como para las acciones conjuntas en materia de autorregulación.

Sin embargo, la Unión Europea es la instancia que ha mostrado la voluntad más firme de fomentar el uso de los códigos de conducta con el fin de luchar eficazmente contra los contenidos ilícitos y nocivos en Internet. Concretamente, la *Recomendación relativa a la competitividad de la industria europea*[150] de 24 de septiembre de 1998 contiene las directrices indicativas para la aplicación, a escala nacional, de un marco de autorregulación para la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información en línea.

El contenido del código de conducta deberá cubrir tanto las medidas destinadas a proteger a los menores como las destinadas a salvaguardar la dignidad humana.

---

[147] Declaración ministerial de la OCDE en la reunión de Bonn sobre "las redes mundiales de información" celebrada los días 6 – 8 de julio de 1997.

[148] Conclusiones del Foro sobre la Autorregulación de los contenidos en Internet, celebrado bajo los auspicios de la OCDE en París, el 25 de marzo de 1998.

[149] Conferencia internacional celebrada los días 8 – 10 de septiembre de 1999 en Munich, Alemania.

[150] Recomendación del Consejo de 24 de septiembre de 1998 relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana (DO C L.270, de 7 de octubre de 1998).

Para evitar que los menores accedan a contenidos que pueden perjudicar su desarrollo físico o emocional, el código de conducta deberá incluir, al menos, los siguientes extremos: la información a los usuarios -cada vez que sea posible- de los riesgos derivados de los contenidos potencialmente nocivos y los medios de protección de los que pueda hacer uso; la indicación de los contenidos que aun siendo legales, pueden resultar nocivos para los menores (por ejemplo, a partir de advertencias o sistemas de comprobación de la edad); la puesta a disposición a los padres y educadores de herramientas de uso sencillo para filtrar y clasificar de los contenidos que puedan resultar nocivos para que los menores puedan acceder incluso sin supervisión; finalmente, la gestión de las reclamaciones de los usuarios a través de las líneas directas.

Además de estos extremos, y en lo que se refiere a la lucha contra los contenidos ilícitos, el código de conducta deberá garantizar la cooperación con las autoridades judiciales y policiales a través de la indicación del procedimiento de cooperación entre los operadores y las autoridades públicas, respetando en todo momento el principio de proporcionalidad y de libertad de expresión, dentro del marco jurídico nacional de cada Estado miembro.

Finalmente, y con el objetivo de aumentar la credibilidad de los códigos de conducta, éstos deberán incluir normas que establezcan las infracciones en caso de incumplimiento, procedimientos de recurso y de mediación.

Los códigos de conducta incumben a todos los participantes en la transmisión de la información a través de la Red. En la actualidad se constata que colectivos de distinto signo han adoptado códigos de conducta por los que rigen su actuación. Por ejemplo, las asociaciones de protección de la infancia como la ONG británica *Internet Watch Foundation;* las asociaciones de proveedores de servicios de Internet como la AFA *(Association des Fournisseurs Francais),* que incluye declaraciones como: "los miembros de la AFA no son autores o productores de contenidos puestos en línea

por terceros; que tampoco lo son para las páginas personales de sus abonados, pero se comprometen a detectar los contenidos eventualmente ilegales con técnicas de líneas de llamada, de vigilancia de las páginas más consultadas y de filtrado de las palabras sospechosas; para los foros, la AFA considera que sus miembros pueden actuar y suspender la difusión de foros contrarios a sus condiciones de utilización". O finalmente, los proveedores de contenidos -en este caso, no profesionales- como la Universidad de Alicante que, en su Código Ético, prohíbe a los integrantes de la comunidad universitaria introducir en la red informática contenidos que vulneren los derechos de terceros (propiedad intelectual, derecho a la intimidad, al honor y a la propia imagen). Las actividades de sus usuarios deben ajustarse a los fines últimos de la entidad: la investigación y la docencia.

5.6. LAS LINEAS DIRECTAS

Las llamadas *hotlines*, o líneas directas, permiten al usuario notificar a las autoridades competentes la existencia de contenidos que, a su juicio, sean ilícitos o nocivos en la Red.

Las líneas directas son gestionadas por organizaciones públicas, privadas o mixtas, que reciben las reclamaciones de los usuarios sobre contenidos que no respeten las normas de protección de menores, atenten contra la dignidad humana o infrinjan el código de conducta en la materia. Las reclamaciones pueden realizarse a través de una llamada telefónica, fax, correo ordinario o electrónico durante 24 horas al día. La organización remite la reclamación, bien a las autoridades policiales competentes (como es el caso de Dinamarca o Noruega, o el de Francia, pero sólo cuando así lo exige la ley), bien a los prestadores de servicios de Internet (como ocurre en Alemania), o bien a ambos (Reino Unido). La persecución y castigo de los responsables sigue siendo competencia de las autoridades nacionales. Pero éstas se enfrentan con un problema. La mayoría de los contenidos denunciados suele tener

su origen en un país extranjero. En estos casos, la cooperación internacional entre las líneas directas se hace imprescindible, de tal forma que la organización pueda, al recibir la notificación del usuario, ponerse en contacto e intercambiar información con la línea directa del país de origen del contenido para que ésta adopte las medidas necesarias.

Por este motivo, se demanda la creación de redes internacionales de líneas directas, no sólo desde el Consejo de Europa[151], sino también desde la Unión Europea. La Comisión, en su *Plan Plurianual de Acción Comunitaria* de 1999[152], enfatiza que las líneas directas son un factor esencial para limitar el flujo de los contenidos ilícitos en Internet, e invita a los Estados miembros a crear una red europea de líneas directas que pongan al descubierto la existencia de contenidos ilícitos, respetando al mismo tiempo las diferencias culturales y jurídicas existentes entre los diferentes Estados. Para lograr este objetivo, el Plan Plurianual de Acción Comunitaria adjunta una convocatoria de propuestas para el establecimiento de una red europea de líneas directas, establecer vínculos entre ésta y las líneas directas de terceros países e intercambiar información y experiencias sobre las prácticas más adecuadas.

A pesar de las grandes ventajas de las líneas directas como mecanismos de notificación de los contenidos ilícitos en Internet, quedan por resolver algunas cuestiones.

Las líneas directas tienen un alcance limitado porque la mayoría de las *hotlines* que se han creado en Europa se circunscriben a las denuncias de pornografía infantil, únicamente los Países Bajos han creado una línea directa para denunciar los contenidos racistas y xenófobos.

---

[151] Declaración Ministerial de Bonn sobre "Las redes mundiales de la información", Reunión de la OCDE, celebrada en Bonn, los días 6-8 de julio de 1997.

[152] Decisión núm 276/1999/CE del Parlamento Europeo y del Consejo de 25 de enero de 1999 por la que se aprueba el Plan Plurianual de Acción Comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales (DO L 033, de 6 de febrero de 1999).

No quedan claros los criterios en virtud de los cuales se administran las líneas directas. Las organizaciones que las gestionan podrían convertirse en censores, poniendo en peligro otro valor jurídico que debe ser protegido: la libertad de expresión, derecho fundamental que no debe mermar otros valores jurídicos igualmente necesitados de garantía en las redes digitales:

la protección de menores y la dignidad humana. Las líneas directas deben contrapesar estos dos valores con el fin de equilibrar la balanza para que ninguno de ellos se vea menoscabado.

Para lograr este equilibrio, resulta indispensable: suscribir los principios recomendados en la *Cumbre sobre contenidos en Internet* de 1999[153]: el principio de disponibilidad -que el usuario de Internet tenga conocimiento de la existencia de las líneas de urgencia-; el principio de transparencia en la gestión de las líneas; y el principio de confianza del usuario -mediante el establecimiento de un procedimiento de notificación que garantice que al usuario se le comunicará el resultado de la operación-.

Por ejemplo en España, por el momento, sólo la Guardia Civil dispone de una línea directa en su sitio web desde el que se pueden denunciar los contenidos ilícitos en la Red.

[153] Conferencia internacional sobre la Autorregulación de los contenidos en Internet, celebrada en Munich, Alemania, los días 8-10 de septiembre de 1999.

5.7. LOS JUECES Y MAGISTRADOS FRENTE A LAS REDES DIGITALES

Los jueces y magistrados se enfrentan con nuevas formas de vulneración de valores jurídicos. En la jurisprudencia comparada se advierten decisiones tomadas sin los suficientes conocimientos técnicos, lo que ha generado sentencias en las que los jueces, responsabilizando a los intermediarios, les imponen deberes de vigilancia y supervisión de los contenidos que transitan por las redes digitales. Por ello, se hace necesario impulsar la formación en nuevas tecnologías de jueces y magistrados.

Considero importante lograr despertar un gran interés entre los juristas, magistrados y jueces mexicanos en adquirir conocimientos sobre las características técnicas y las peculiaridades de Internet para resolver adecuadamente los problemas jurídicos que se plantean. En este sentido, resultan altamente positivas las propuestas de colegios de abogados y de las universidades, que ofrecen cursos de especialización y la formación que se ofrece desde las propias instituciones de Justicia.

5.8. ALTERNATIVAS DE SOLUCIONES CONTRA LOS CONTENIDOS ILICITOS EN EL INTERNET

5.8.1. COOPERACION POLICIAL EN EL USO SEGURO DE INTERNET

Por regla general, la conducta delictiva tiene su origen, o despliega sus consecuencias, fuera de las fronteras del territorio nacional, siendo imprescindible que las autoridades policiales nacionales colaboren en materia de investigación con organismos policiales internacionales como Europol o Interpol. Para perseguir a los *ciber-infractores,* la policía requiere de un marco jurídico que permita la interceptación de las comunicaciones electrónicas sin conculcar el derecho de los usuarios a la privacidad de sus comunicaciones.

5.8.2. LA ESPECIALIZACION DE LA POLICIA FRENTE AL CIBERDELINCUENTE

España, por ejemplo, cuenta con el Grupo de Altas Tecnologías de la Guardia Civil y con la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, constituida en marzo de 2000 a partir de la antigua Brigada de Investigación de la Delincuencia Tecnológica de la Policía Nacional. Ambos tienen encomendada la función de vigilancia de los sistemas informáticos de los principales organismos públicos y la investigación y persecución de los delitos informáticos (intromisiones no autorizadas, estafas electrónicas, descubrimiento y revelación de secretos, etc.), comprendidos los contenidos ilícitos y nocivos en la Red. Desde su creación en 1996 al año 2000, han sido resueltos 221 casos, 49 de ellos relacionados con la pederastia en Internet.

La creación de departamentos policiales especializados ha sido reclamada tanto desde organismos supranacionales[154] como desde los propios Estados miembros de la Unión Europea. Fue el caso de Austria que, alarmada por el incremento del número de delitos relacionados con la pornografía infantil en Internet, instó a sus socios comunitarios, en su Iniciativa de diciembre de 1999,[155] a proceder a la creación de unidades policiales especializadas. Éstas debían tener conocimientos específicos y recursos necesarios para tratar con celeridad la información sobre supuestos casos de producción, tratamiento, difusión y posesión de pornografía infantil.

[154] Desde el seno del Consejo de Europa e incluso de la Unión Europea como se ha tenido ocasión de señalar al inicio de este epígrafe.
[155] Artículo 2.1 de la Iniciativa de la República de Austria con vistas a la adopción de la Decisión del Consejo relativa a la lucha contra la pornografía infantil en Internet. 1999/C 362/06 (DO C 362 de 16 de diciembre de 1999).

Los organismos policiales especializados ven dificultada su labor por la escasez de medios técnicos; la dilación en las concesiones de mandamientos de interceptación de las comunicaciones electrónicas; y por las ventajas tecnológicas y las contramedidas que utilizan los delincuentes profesionales, como el cifrado de la información y el anonimato.

Estas demoras pueden ser neutralizadas incrementando la asignación de recursos por parte de la Administración, agilizando los procedimientos judiciales y optimizando la formación de los cuerpos policial es (como el ofrecido en el marco del Proyecto Falcone de la Unión Europea, destinado a acomodar los conocimientos de los policías a las necesidades de Internet).

En otros países, las actividades de los organismos policiales especializados se re fuerza con la labor que desarrollan algunas ONGs. En el Reino Unido, por ejemplo, la asociación británica *Internet Watch Foundation* asesora a la policía para detectar material pornográfico dirigido a niños. La Fundación retiró en el año 1999 diez mil fotografías de la Red y está sirviendo de modelo a otras organizaciones europeas.

Lamentablemente en México sólo se cuenta con la Unidad de Policía Cibernética, como ya se exponía, la cual únicamente tiene como objetivos principales detectar las organizaciones criminales de pedófilos, las mafias de prostitución infantil que promueven y transmiten pornografía infantil, que operan desde el país vía Internet, para combatir la explotación sexual infantil y la práctica de ritos satánicos donde se involucran a menores y animales en sus ceremonias; asimismo desmantelar organizaciones que se dedican a la explotación y al reclutamiento de niños para abusar sexualmente de ellos.

5.8.3. LA INVESTIGACION INTERNACIONAL DE LOS CONTENIDOS ILICITOS EN INTERNET

Los Estados miembros de la unión europea disponen de dos mecanismos para prestarse asistencia mutua en materia de investigación de los delitos que tienen implicaciones fuera de sus fronteras: la investigación oficial a través de comisiones rogatorias, *y* la investigación oficiosa a través de organismos policiales internacionales.

La investigación oficial se muestra ineficaz en una lucha que reclama una mayor agilidad *y* rapidez. Y que reclama, más que nunca, la cooperación entre los Estados, tal como manifestó el Consejo de Europa en su *Recomendación núm.* R (95) 13 *sobre los problemas de procedimiento penal relacionados con la tecnología de la información*[156], en casos en los que el sistema informático desde el que se comete la infracción esté localizado en el extranjero y así lo requiera la urgencia de la situación.

De ahí la enorme importancia de dos organismos: la Europol *y* la Interpol. La Europol materializa la cooperación policial en el ámbito de la Unión Europea *y* su actividad se nutre de las bases de datos del Sistema de Información Schengen, lo que permite una mayor eficacia en las investigaciones. La Interpol, organización intergubernamental, se ocupa de la cooperación policial internacional para las actuaciones que requieren la intervención de las autoridades policiales de Estados de fuera de la Unión Europea. Ambas instituciones salvan las trabas que retardan la actuación de los mecanismos de investigación oficiales porque, gracias a las nuevas tecnologías, pueden obtener más rápidamente información sobre los presuntos *ciber-infractores y* además, permiten la creación de redes internacionales de cooperación en materia de persecución.

[156] La Recomendación del Comité de Ministros del Consejo de Europa núm. R (95) 13 sobre los problemas de procedimiento penal relacionado con las tecnología de la información de 11 de septiembre de 1995.

El uso de las redes digitales no sólo posibilita nuevas formas de vulnerar la protección de los menores y la dignidad humana y otras garantías como la libertad de expresión y de información, sino que también se nos ofrece como una herramienta nueva y más sofisticada con la que perseguir el crimen.

La tensión que se produce entre la necesidad de proteger a los menores y la dignidad humana en las redes digitales mediante la persecución y castigo de los culpables, de un lado, y la protección de la privacidad, de otro, ha sido la causa de que las Instituciones europeas propongan mecanismos menos costosos y más eficaces, como son los mecanismos de filtrado y bloqueo de contenidos, la utilización de las líneas directas y el fomento de los códigos de conducta de los actores implicados en la transmisión de la información en línea.

A este estatuto represor le corresponde tutelar el derecho a la soledad, a la intimidad, al anonimato, al honor y a la honra, derechos que, debido a los logros informáticos y telemáticos, cada día se ven más amenazados por el derecho a informar, a ser informado y a opinar. Por estas razones, debe sancionarse penalmente a quienes ilícitamente empleen los bancos de datos. Además de los posibles atentados a la integridad moral o a la libertad individual, pueden presentarse conductas atentatorias de la fe pública, del derecho al sufragio o del patrimonio económico. Tales actos podrían consistir en la alteración de cuentas, traslado de fondos y sustracción de información, todo ello electrónicamente; contrabando, copiado, plagio y tergiversación de programas.

Los servicios a través del Internet envuelven una gran variedad de actividades que conllevan riesgos provenientes de la conducta de los suscriptores o terceros. Estos servicios se transmiten internacionalmente y es difícil conocer las leyes que les aplican. Hay personas que piensan que tratar de regular el contenido presentado en el Internet es un proyecto muy difícil, y hasta podría no tener solución como tal.

Actualmente el 60% de las personas conectadas en la red de Internet están en los Estados Unidos. Ellos podrían tomar algún tipo de control sobre el contenido en los "host" de esta parte de la red, pero el problema es que la transmisión de información corre a través de todo el mundo y el Internet cada día crece más y más. Surgen más enlaces, más portales llevan a otros lugares, y de esos a su vez a otros lugares pudiendo terminar en otros más, y así sucesivamente. Este es un asunto global que requiere de una respuesta global.

5.9. PROPUESTA SOBRE LOS CONTENIDOS ILICITOS Y NOCIVOS QUE PUEDEN SER REGULADOS

El Internet es una red compuesta de muchas redes que corren a través del mundo entero. No tiene un origen, ni tiene un creador, ni un dueño. Han habido ciertas regulaciones que han puesto un tipo de control, pero, regular todo tipo de contenido explícito es un proyecto muy fuerte. Es por esto, considero que los proveedores de servicio tienen que colaborar en la responsabilidad de velar por el material que se publique y por establecer regulaciones que ayuden a evitar daños a terceras personas. Por otro lado, los gobiernos locales y los organismos internacionales también deben contribuir para que se promulguen leyes que ayuden a tomar acción contra aquellos que hagan uso indebido de estos servicios. Por eso, en muchas ocasiones, hay personas que opinan que las leyes no lo deben regular, que se deben regular por sí solos, por iniciativa de cada individuo.

Los Estados deben proporcionar un marco jurídico adecuado para que la policía disponga, con el fin de perseguir a los presuntos delincuentes, de mecanismos de interceptación de las telecomunicaciones, en particular, de las comunicaciones que tienen lugar en Internet (correo electrónico, *chat,* grupos de noticias, etc.)

En seguida, se describen aquellos contenidos en el Internet que considero pueden ser regulados:

A) MATERIAL PROMOCIONAL

Por lo general, se envía a múltiples usuarios indiscriminadamente y es material no solicitado ni deseado ("Spam"). En ocasiones, es material anónimo y tiene el propósito de hacer promociones comerciales para que visiten web sites.

Se calcula que el 30% de los "emails" que reciben los usuarios de Internet son de este tipo.

La mayoría de las direcciones son robadas o compradas y el problema mayor es que sustraen recursos de los usuarios y proveedores de servicio sin compensación y sin autorización.

Se debe regular por que las comunidades "on-line" manejadas por los proveedores de servicio no son un foro público para propósitos que garantcen la libertad de expresión y de prensa.

Las partes envueltas en el desarrollo de comunidades "on-line" son las que pueden hacer valer las regulaciones estando atentos a las consideraciones del "Antitrust Act" e implementando políticas y reglas que gobiernen el funcionamiento de esas comunidades. Considero que las Comunidades on line no son foro público para libertad expresión. El contenido puede ser inadecuado y se da la Invasión propiedad ajena.

Si no se regula, el Internet no va a ser un medio confiable ni efectivo para los negocios electrónicos y no va a poder desarrollarse al máximo por falta de mecanismos de seguridad relacionados a información personal.

Si son anuncios dirigidos a menores, hay que estar alerta por que el contenido puede no ser apropiado.

Los reguladores pueden ser:

Los individuos (Por sí mismo, Filtrando por software instalado en la PC.); las Organizaciones (Sistemas de control de acceso o Passwords o Verificar edad, Filtrando por software instalado en las PC's; Filtrando por software en el hardware del ISP; Filtrando por software instalado en gateways; Filtrando y rastreando direcciones de IP); el Estado o Gobiernos (Leyes Estadounidenses tales como: "Communications Decency Act" del 1996 y "Children online protection Act" del 1998); Organizacionres jerárquicas no gubernamentales (Auto-regulaciones de la Industria, Código de conducta).

Se puede hacer valer las regulaciones incluyendo notas y requisitos para el consentimiento de acceso por parte de los padres.

Como una consecuencia a su regulación posiblemente podría debilitarse la protección a la propiedad intelectual y privacidad y afectarse la seguridad de los sistemas y robo de recursos a las organizaciones.

Actualmente, el proveedor de servicio AOL es uno de los más pro-activos en el control del Spam. Ha tenido demandas sin causa probable y sigue firme en mantener este control. Sus clientes están satisfechos y sirve de ejemplo a otros.

B) PROPAGANDAS QUE INCITAN O INSTRUYEN AL CRIMEN O A LA VIOLENCIA, TERRORISMO, CULTOS SATANICOS, ODIO

Este contenido deber ser regulado, ya que es un claro ejemplo de lo que no se debe hacer, al ser regulado, se pretende proteger el derecho a la vida y seguridad, a proteger valores de la sociedad. Esta regulación podría ser apoyada por un Organismo internacional (creando leyes) y el Estado mismo.

Pues el no regularse pudiera producir un cambio desfavorable en la moral y valores de la sociedad, así como la probabilidad de aumentar el terrorismo e incidencias de crímenes

C) ANUNCIOS FRAUDULENTOS O CONFUSOS

Son ofertas a los consumidores "online" entre las cuáles están: cartas en cadena ("on-line chain letters"), ofertas de seguros, inversiones o becas o anuncios relacionados a la salud.

Se deben regular por que pueden ser perjudiciales a la salud y atentar contra la seguridad económica de los individuos.

El que se regulen garantizaría la seguridad y protección de los consumidores, así como la protección al comercio lícito.

Además, puede afectar los comercios relacionados a la bolsa de valores y a los que están en el Internet ya que crearía desconfianza por parte de los consumidores.

Se puede hacer valer mediante regulaciones y haciendo responsable a los

proveedores de Internet por el contenido, con apoyo en un Organismo Internacional el Estados mismo.

Una vez regulado posiblemente se afectaría la economía, se viola al derecho de seguridad, se frenaría un poco la liberalización de mercados de telecomunicación a nivel mundial

D) MATERIAL DIFAMATORIO

Material difamatorio por razón de: Raza, Sexo, Orientación sexual, Limitación física o mental, Odio. Envuelve dos tipos: culpa del publicador primario ya sea proveedores del "Web site" o autores de correo electrónico, o culpa del proveedor de servicio u operadores del "Bulletin Board". El material difamatorio se debe regular para no convertir el Internet en un foro de comunicación mediocre. Se debe limitar el daño emocional y social que este medio pueda causar a terceras personas ya que llega a miles de personas en el mundo entero y no es lo mismo que los medios de comunicación tradicionales de prensa, TV y radio que sólo llegan a un población particular. Estas publicaciones pueden llegar a todos los suscriptores que el ISP le da servicio y en este caso se convierte en "bulk mail".

Los publicadores y el ISP, si conoce o sabe de la naturaleza del material, son los principales responsables puesto que las leyes no son iguales en todas las naciones. Se puede hacer valer esta regulación revisando el contenido de los mensajes por medio de programas para filtrar los "email" y removiendo los mismos. De no tomarse la acción de regular:

Los ISP son considerados distribuidores debido a que trabajan con numerosas publicaciones para distribución y acceso público. Tienen la misma responsabilidad que cualquier otro medio de comunicación.

Con su regulación podría verse un poco mermada la libertad de expresión.

Su regulación trambién debe estar en manos y vigilancia de un Organismo Internacional, con apoyo del Estado mismo.

E) MATERIAL OBSCENO, PORNOGRAFIA, DUDOSA REPUTACION, DE ORIENTACION SEXUAL

La definición de obscenidad varía de acuerdo a los estándares de las comunidades e internacionalmente. En algunos lugares, este material está protegido por las leyes del gobierno. En otros, es uno de los temas más controversiales y del cual se ha hablado mucho ya que se trata de regular el material de índole sexual y pornográfico. Muchas personas creen que el material de contenido sexual debería establecerse con unas medidas y unas limitaciones, y hasta en algunos casos, no hacer ningún tipo de publicación del mismo. La comunidad en general y las figuras religiosas ven tal contenido como obsceno, inmoral y fuera de toda enseñanza cristiana. Los padres quieren proteger a sus hijos de exposición prematura a este tipo de material. Por otro lado, las personas que publican este tipo de páginas ven una oportunidad de ingreso al haber una regulación con las mismas.

Otro asunto que es aún más severo, es el de material que envuelve pornografía infantil. La pornografía infantil se trata de niños maltratados sexualmente, y se proyectan imágenes que podrían causar traumas o traer recuerdos a estas personas de experiencias similares. La pornografía infantil se debe regular en todos los lugares.

Existe una completa serie de normas que limitan la circulación de contenidos como la pornografía infantil. Estos son ilegales en muchos países, por ejemplo en la mayoría de los Estados de Europa la transmisión así como la tenencia de archivos sobre pornografía infantil se encuentra tipificada como delito, en cambio no es así en otros países como Perú que no cuenta con una norma que tipifique este tipo de conducta, lo que ira coadyuvando a la unificación de tipos penales en la mayoría de los Estados.

Considero que se debe regular en sitios donde las leyes no lo protegen. Si es infantil, regularlo por completo. Afecta moralmente y religiosamente, pues no se pretende afectar la libertad de expresión, ya que existen culturas que lo permiten.

Cabe la posibilidad de que con su regulación se debilite la protección a la propiedad intelectual, privacidad y seguridad, y darse un cambio desfavorable en la moral y valores de la sociedad.

La regulación es responsabilidad de la organización (ISP y del operador del "Bulletin Board"). El ISP deberá remover el material del "site" y ser pro-activo para que los operadores del sistema monitoreen efectivamente y actúen cuando vean material obsceno o indecente ya que son los responsables por el material distribuido. Deben tener "softwares" para filtrar "emails" y facilitárselo a los clientes que lo soliciten, así como proveer mecanismos de control para la restricción de acceso antes de poner el material "on-line.

Los reguladores de este contenido son los Individuos, el Estado, las Organizaciones, y las Fuerzas sociales no jerárquicas (normas sociales, códigos de conducta).

F) MATERIAL QUE REFLEJE ATRIBUTOS NACIONALES O CULTURALES EN UN MEDIO DE DIVULGACION O PROHIBIDO COMO ADVERSO EN LA CULTURA

Se debe regular para evitar confrontaciones entre países o naciones, las consecuencias de no ser regulado generaría causar desprestigio y discrimen.

La regulación debe ser respalada por Estado, Organizaciones, Organismo internacional, Fuerzas sociales no jerárquicas.

G) MATERIAL RELACIONADO A PROPIEDAD INTELECTUAL

Incluye trabajos artísticos y literarios, ya sea videos, audio, texto, imágenes, reproducción no autorizada, bancos de datos, programas de computadora, trabajos digitales. Se puede hacer valer las regulaciones revisando las fuentes de información del material disponible "on-line" para asegurarse que no se violen los derechos de autor. Se debe incluir notas e instrucciones describiendo el material y el uso autorizado. Los mismos individuos son responsables por sus acciones pero el gobierno y los organismos internacionales deben ejercer mayor control.

Se debe regular para evitar piratería, dar protección al comercio lícito, protección propiedad intelectual y derechos autor y garantizar seguridad consumidores.

Se publicó un artículo en FindLaw.com relacionado a un caso de un publicador de Internet en el que la Corte Suprema de EE.UU. podría permitir que las imágenes de las mascotas de Disney puedan utilizarse en dominios públicos. Esto puede resultar en millones de dólares en ingresos para los estudios de cine y los autores, si este material se puede obtener gratis. Disney Co. hace referencia a una ley de 1998, la cual extiende la protección de "copyright" a 20 años para trabajos culturales y 70 años luego de la muerte del autor o por 95 años luego de publicar trabajos creados por corporaciones. El demandante alega que la legislación es muy estricta ya que es

demasiado tiempo y que la medida responde a los grandes intereses y no a la realidad de nuestro mundo actual. La resolución del caso puede sentar un precedente para que otras personas puedan amparase de esta decisión y pedir que la legislación sea revisada ya que encuentran que es injusta. Tarde o temprano, habrá que legislar para que esta ley cambie y el material protegido se pueda utilizar sin tener que pagar regalías a quien tiene los derechos casi por tiempo indefinido.

Para poder regular el contenido en el Internet y hacer valer las regulaciones, hay que primero que nada, tomar este asunto del Internet y la era tecnológica como un mundo completamente nuevo. La tecnología cada día avanza mas rápido de lo que nos podemos imaginar, y simplemente hay que crear una educación sobre todos estos asuntos. Hay que crear programas y aplicaciones que puedan regular los contenidos y crear departamentos exclusivos para monitorear a los navegantes del Internet y a las personas que publican material.

Se debe regular contenido relacionado a: 1) Todo tipo de material que ofenda razonablemente a un adulto ya sea contenido pornográfico, propaganda de cultos satánicos, violencia, terrorismo y discrimen. 2) Propaganda que dañe a los niños (pornografía infantil, violencia, palabras soeces) o los perjudique de alguna manera. 3) Toda práctica que fomente el violar la ley (tipo de personas, copia de música para distribución y beneficio propio, violar los derechos de autor, distribución de virus en los "e-mail"). De no hacerlo, estaríamos derrumbando al suelo todos los fundamentos morales y éticos sobre los cuáles está construida la sociedad.

Como miembros de una sociedad, debemos tomar cartas en el asunto. Dado que al gobierno se le hace difícil establecer leyes sin violar otras, las organizaciones tienen que tomar un papel protagónico en este asunto y se debe establecer vigilancia de lo que los usuarios depositan en los servidores utilizando filtros para la pureza de lo que viaja en la red, no fomentar ni permitir que material ofensivo resida en sus servidores y de tener problemas para establecer los controles, exigir que se

identifique antes de acceder las páginas de su anuncio o producto.

Las organizaciones internacionales deben establecer políticas globales que regulen lo que viaja en la red, ya sea que los servidores residan en el país o que la información entre a ese país. Hay países como Australia, que ya han aprobado leyes que regulan, a través de clasificadores de información, lo que entra y sale de la red. Estos deben de ser tomados como ejemplo o base para poder legislar en otros países para establecer los controles necesarios.

Si no regulamos, habrá un caos en el comercio electrónico donde no tendremos control sobre nada ya que no se respetarán las leyes como patentes y derechos de autor ni los derechos de los individuos y se estará fomentando la anarquía virtual en el mundo. Todo será para beneficio individual y no de la sociedad. Todo nuestro aparato social, económico y legal se derrumbará.

CONCLUSIONES

Internet ha creado nuevas formas de comunicación e intercambio de información. Su naturaleza ha hecho que este intercambio se realice de forma inmediata y sin control. Internet no tiene un centro rector que dirija o apruebe el contenido que libremente circula en ella. Es controlada por todos los usuarios y son los usuarios los que deciden pasar de un servidor a otro y elegir el contenido que desean ver. Esto lo pueden realizar sin ser identificados y por tanto es imposible determinar las características del usuario (edad, sexo, idosincracia, etc); de igual manera, dada su naturaleza implica que no se puede censurar desde un Estado determinado una realidad virtual que normativamente y en teoría sólo podría llegar a regularse mediante controles tecnológicos y esfuerzos legislativos de carácter nacional e internacional.

A lo largo de estas páginas se ha tenido ocasión de exponer cómo algunos de los contenidos que el usuario encuentra en la Red son lícitos y sumamente útiles y, al igual que sucede en la vida real, otros son ofensivos o ilegales. Los contenidos ilícitos son considerados generalmente como delitos (vgr. la pornografía infantil) y como tales, merecedores de una sanción penal. Los contenidos nocivos son, por su parte, ofensivos para el destinatario que tiene concepciones éticas, morales, raciales, religiosas o políticas distintas de las de la persona que los introdujo en las redes digitales, o perjudiciales para el normal desarrollo de un individuo, pero sobre todo de los menores.

Cualquiera de los sistemas, aplicaciones y herramientas de Internet son susceptibles de constituir el soporte de informaciones ilícitas o nocivas. Desde sus fases iniciales de desarrollo, Internet ha sido el campo abonado para usuarios que han abusado de las especiales características de ella; en particular, de su carácter descentralizado, de la posibilidad de la descarga anónima de archivos, de la

navegación anónima y de la ausencia de regulación de las redes digitales. En la mayoría de los casos, los usuarios hacen un uso lícito de las fabulosas posibilidades que ofrece la red. En otros, sin embargo, no es así. Todo depende de la responsabilidad y el respeto que los usuarios muestren hacia los demás usuarios. Los sistemas, herramientas o aplicaciones de Internet son, por otra parte, continuamente desarrolladas y mejoradas. Aparecen nuevas aplicaciones y herramientas que mejoran la transmisión de las informaciones en línea y las redes siguen creciendo.

El Internet, a fin de cuentas es una herramienta tecnológica o telemática, mediante la cual pueden transmitirse datos, documentos, imágenes y sonidos de diversa naturaleza o contenido, sean lícitos o ilícitos, morales o inmorales, permitidos o prohibidos, benignos o nocivos. (Hay quienes distinguen entre "contenidos ilícitos" y "otros contenidos nocivos". Ejemplo de los primeros -que a nivel de cada Estado o localmente se consideran delitos- sería el acceso de los adultos a pornografía infantil, la trata de blancas o redes de prostitución, y la difusión de contenidos racistas; ejemplo de los segundos sería el acceso de niños a contenidos pornográficos para adultos) ahora bien, hay quienes también señalan que la protección a la indemnidad sexual de los menores; al honor, a la intimidad personal y familiar y a la propia imagen; la dignidad humana; o los derechos de propiedad intelectual no puede justificar la censura de contenidos legales pero obscenos o nocivos, en virtud de que no se puede llegar a vulnerar otros derechos como los de la libertad de expresión e información de personas de todas partes del mundo que, perfecta y legalmente pueden ver contenidos obscenoso nocivos o dejar de ver contenidos que por su cultura no lo son.

Por ello, considero que es una necesidad regular especialmente el contenido ilícito y en lo posible el contenido nocivo que ciurcula en Internet, sin que por ello se vean vulneradas las garantías de libertad de expresión y correlativamente la libertad de información. Existen limitaciones jurídicas a estas libertades, precisadas

en diversas Constituciones e Instrumentos internacionales a fin de asegurar la adecuada convivencia, el respeto mutuo, la moral, los derechos de tercero, el orden público, el bienestar y la seguridad de la vida comunitaria; ya que de no existir límites jurídicos para éstas libertades; bastaría con alegar que se habría hecho uso de dichas libertades para llevar a cabo una conducta ilícita, pero el problema se presenta cuando estas dos libertades son revasadas aprovechandose de las características del Internet.

Así, se debe recordar que hasta 1990 los gobiernos no se preocupaban por regular los contenidos que circulaban en Internet; dado que muy pocas personas en el ámbito internacional tenían acceso a ella. Posteriormente, el acceso a Internet se incrementó, aumentando también los contenidos que circulan en ella, aumentando de esa manera este tipo de contenido nocivo e inclusive ilegal como la pornografía infantil. Al darse cuenta los gobiernos de la cantidad de contenido de esa índole que circulaba libremente en Internet, surgieron intentos para su control.

El primero intento, se dio con la US Communications Decency Act- CDA en 1996 la cual prohibía la transmisión del contenido de tipo "obsceno o indecente" en Internet. Esta ley desató una gran polémica, pues vulneraba el derecho a la libertad de expresión e intercambio de información plenamente garantizado en la primera enmienda de la Constitución de Estados Unidos, así como pretendía normar lo que es decente o no en una sociedad mediante una norma que se intentaba aplicar a una realidad como Internet. El 12 de junio de 1996, los oponentes a la CDA consiguieron una primera victoria, puesto que, tres jueces federales de Filadelfia la declararon inconstitucional. Finalmente el Tribunal Supremo de los Estados Unidos declaró su inconstitucionalidad.

Otro intento para controlar el contenido ilícito del internet fue la introducción de sistemas de etiquetado y filtrado, para evitar que el usuario vea un determinado contenido encontrado en Internet. Destacando de este proceso sus dos

componentes: La clasificación: en el cual se utiliza un juicio de valor para categorizar sitios web sobre la base de su contenido: "permitido / no permitido", y El filtrado como el mecanismo de control de la recepción de la información, no de su distribución.

Sin embargo, los filtros no son quizás el medio más seguro y eficiente de protección frente al contenido nocivo que pueda encontrarse en la Red; ya que existen muchos problemas con relación al etiquetado y filtrado de contenidos principalmente por la misma naturaleza abierta y global de Internet, la dificultad para definir la obscenidad o lo nocivo del contenido que se quiere clasificar, así por ejemplo, el contenido nocivo para menores resulta, casi imposible de realizar pues la obscenidad es un concepto subjetivo que depende de los usos y costumbre de una sociedad en un tiempo y espacio determinado y quien clasifica es una empresa del país en cuestión, que lo realiza en virtud de lo que ella considera obsceno; sin embargo, el sistema es utilizado por personas de todas partes del mundo, cada una con sus propios usos y costumbres, que pueden ser diametralmente diferentes; además, la mayoría de los filtros de contenido están centrados en la WEB no filtrando el contenido que circula por el IRC - Internet Relay Chat y/o newsgroups; Del criterio de clasificación del contenido pueden resultar alegaciones de censura arbitrarias; dadas las diferencias culturales, morales entre una sociedad al momento que una empresa clasifica el contenido pues la empresa lo hará en virtud a su moral y buenas costumbres; sin embargo, quien utilice el sistema no necesariamente tiene la misma moral, por lo tanto, el sistema a veces nos puede conducir a absurdos de "filtrar contenido no obsceno" o "no filtrar el contenido obsceno"; Se pueden llegar a bloquear el acceso a otros sitios que no tienen por qué necesariamente ser ilícitos o nocivos, como por ejemplo a contenidos literarios, artísticos o científicos. Eso fue lo que ocurrió cuando al elaborar el listado de sitios web que contenian la palabra "seno" se incluyó un sitio web creado por una asociación de víctimas del cáncer de mama. *CyberPatrol,* por ejemplo, puede situarse a varios niveles: el ordenador personal, a nivel de *proxy,* o incluso a nivel

nacional. Esto permite, por ejemplo, que determinados gobiernos corten el acceso de sus nacionales a páginas de contenido político democrático, de consumo, religioso, de libertad sexual, de opinión, etc. En consecuencia, las asociaciones a favor de la libertad de expresión han calificado el programa de filtrado como una nueva forma de censura; El filtrado no garantiza una seguridad total, son dispositivos que los propios menores pueden fácilmente desconectar y por tanto inutilizar un programa, sobre todo teniendo en cuenta los conocimientos de informática de los menores internautas, que suelen superar a los de sus progenitores, entre otros factores.

En el seno de la Unión Europea se han levantado voces en contra de la utilización de los programas de filtrado de contenidos. En la *Cumbre sobre los contenidos en Internet,* celebrada en Munich en 1999, organizada por una ONG alemana (Fundación Bertelsmann) se elaboró un memorando sobre la Autorregulación en Internet que recomendaba el desarrollo de los sistemas de filtrado. Pero algunos grupos (educadores, abogados, organizaciones a favor de la defensa de la libertad de expresión) se opusieron, porque ello conllevaría un mayor intervencionismo estatal y la imposición de estándares morales nacionales en Internet.

Finalmente, también se ha acusado a los filtros de ser estándares americanos que no tienen por qué coincidir con los valores de otros países, especialmente los basados en listas negras y listas blancas.

Considero que que si los usuarios pueden contar con programas que les permitan filtrar los contenidos, se hace plenamente factible permitir la libre circulación de la información reclamada por la libertad de expresión y el respeto a las preferencias personales, por ejemplo de los padres que quieran controlar el material a que acceden sus hijos.

Se trata de un nivel de censura o más bien de autocensura totalmente aceptable que, pragmáticamente, permite respetar la diferencia de criterios, valores o costumbres morales entre comunidades, países y culturas diversas. Ya no hay eventual censura en la fuente o alguna restricción o prohibición legal, administrativa o judicial previa para publicar virtualmente determinados contenidos, sino que el control o filtrado se produce a nivel de usuario final en la computadora donde se recibe la información.

Otro de los intentos por controlar el contenido que circula en Internet, es el tema de la autorregulación o co-regulación de los contenidos ilícitos.

La co-regulación (concertación entre las autoridades públicas y el sector privado) parece una solución viable y apropiada, ya que el Estado no puede llegar a controlar todo; y la autorregulación por sí sola no garantiza el cumplimiento efectivo de los objetivos perseguidos en esta materia, por lo que la co-regulación parece la fórmula adecuada.

El equilibrio entre regulación y autorregulación en cada país debe establecerse atendiendo a la tradición existente en el mismo en esta materia.

La co-rregulación en teoría pareciese la opción perfecta, pues tendría a la autoridad competente que solicite se investigue y se sentencie procediendo legalmente la censura.

Sin embargo, en éstos mecanismos de autorregulación existen demasiados intereses políticos y económicos en juego detrás de la regulación de contenidos. En principio, la autorregulación pareciese la opción mas viable, sin embargo, la

aplicación de este sistema ha sido totalmente distorsionado, ya que las empresas proveedoras de servicios de Internet y los intereses comerciales que se ponen en juego, dada la presion que ejercen algunos gobiernos sobre ellos, no toman en cuenta al usuario o consumidor sino que las empresas toman decisiones en función a sus intereses censurando el contenido y evitando que el nombre de su empresa se vea perjudicado al estar envuelto en algún proceso de esas índole; osea, se toman la atribución de ser la autoridad oficial procediendo a retirar arbitrariamente el contenido ilícito, sin que se cumpla con un debido proceso ni se respete el derecho de defensa de la persona que alojó o transmitió el contenido ilícito. Se debe sancionar pero con un debido proceso y garantías mínimas como el derecho de defensa del presunto infractor a defender la legalidad del contenido, donde se justifique el orden público y no los intereses de particulares disfrazados en una defensa a la dignidad humana.

En este tipo de mecanismos, considero que las organizaciones o empresas deberían limitarse a detectar contenidos de ilícitos y denunciarlos a la autoridad competente con el fin que se realice la investigación correspondiente y sea ésta la autoridad oficial competente quien proceda a dictar sentencia censurando legalmente dicho contenido ilícito y no realizando una censura ilegal y arbitraria.

El control de edad es otro mecanismo que permite controlar el acceso de los menores a determinados sitios web. En la práctica, es difícil aplicar esta medida. El usuario de Internet puede fácilmente proporcionar datos falsos acerca de su edad.

Además, el control de edad implica elevados costos económicos para los proveedores de contenidos y de servicios. Los proveedores "no comerciales" dejarían de ser competitivos y se verían borrados del mercado al no poder afrontar los costos de los dispositivos de control de edad.

Las líneas directas han sido otro intento por parte de los Estados para eliminar el contenido ilícito en Internet, consistente en que a tráves de éstas líneas directas, algunas de ellas a cargo de organismos cuasi-gubernamentales, otras compuestas por algunos proveedores de Internet, usuarios y algunos representantes de las autoridades, se advierte a las personas que publican contenidos ilícitos en Internet que están cometiendo un delito y si a pesar de la advertencia no eliminan esos materiales de la red, la línea directa informa de sus actividades a la policía para que proceda, terminando así su objetivo.

Sin embargo, de manera muy semejante al mecanismo de co-regulación, dentro de las facultades otorgadas a las líneas directas, en muchos Estados de la comunidad europea, esta también el de poder restringir, bloquear o eliminar de circulación las páginas con contenido ilícito, a propio criterio del proveedor de servicios.

A nuestro juicio debió agregarse, que ésta restricción debe realizarse a petición de autoridad competente, ya que como se mencionaba, no se estan respetando las garantías mínimas de un debido proceso ni el derecho de defensa del presunto infractor, simplemente el ISP a propia voluntad o voluntad de un tercero o de acuerdo a intereses meramente comerciales decide censurar el contenido y decide que es Ilícito, no respetando el derecho del presunto autor del delito a defender la licitud de su contenido.

Algo cercano a la autoregulación es la existencia de verdaderas "entidades de coordinación". Efectivamente Internet no es controlada directamente por ninguna empresa u organización específica, pero, en el seno de entidades internacionales se han ido generando políticas para permitir un desarrollo sustentable y la interoperabilidad entre redes regionales y nacionales, analizar la implementación de

nuevos estándares, y evitar el crecimiento explosivo, por ejemplo, del flujo de datos en la red o del número de usuarios.

Deben por ende considerarse como una opción jurídica viable las modalidades de autoregulación. Por su propio peso e importancia el desarrollo y los conflictos jurídicos en Internet pueden traducirse en el surgimiento de normativas que, impulsadas por algún país u organismo internacional, tengan acogida y sean aceptadas mundialmente por los usuarios de la red. Así ha ocurrido con la reglamentación desarrollada por la IANA (La sigla corresponde a la Internet Assigned Numbers Authority) un organismo contratado por el Gobierno de Estados Unidos de América, para administrar técnicamente el sistema de direcciones o nombres de dominio en la red y la ICANN (La sigla corresponde a la Internet Corporation for Assigned Names and Numbers,) en relación a la asignación de direcciones virtuales o de los nombres de dominio.

Finalmente quiero señalar que con la finalidad de controlar el contenido ilegal que circula en Internet, los Estados requieren por un lado, intervenir en su regulación y de otro, propiciar la autorregulación por empresas privadas y/o co-rregularlo, entre otros, además considero que uno de los mecanismo más adecuado para evitar la existencia de contenidos ilícitos es la existencia de medios técnicos que en la práctica, limiten o impidan el acceso sólo a dichos contenidos mas no a otros, en conjunción con apoyo en los sistemas jurídicos nacionales y la cooperación internacional.

Asimismo, se dio algunos intentos en responsabilizar a los proveedores de servicios de Internet de los contenidos ilícitos que terceros alojen en su servidor.

Todos los actores que participan en la transmisión de la información en las redes digitales (proveedores o desarrolladores de contenidos, intermediarios técnicos,

usuarios) están expuestos a tomar parte en la difusión de contenidos susceptibles de ser calificados como ilícitos o nocivos. Sin embargo, resulta importante distinguir el concreto papel que desempeñan en la transmisión por cuanto que el régimen de la responsabilidad que les puede ser impuesto es diferente en cada Estado.

Los distintos sujetos que participan en la transmisión de la información en las redes digitales tienen una parcela de responsabilidad por los contenidos ilícitos o nocivos. Resulta importante clarificar el alcance de la responsabilidad de cada uno de los actores para combatir eficazmente los contenidos perniciosos de la Red.

Es imprescindible que todos los países tengan claro la responsabilidad del proveedor o desarrollador de contenido; asimismo, debe también quedar claro la no responsabilidad de los proveedores o prestadores de servicio o acceso a Internet de los contenidos que terceros alojan en sus servidores o de la empresa que le brinda el acceso a Internet; y que la responsabilidad al proveedor o prestador de servicios que suministra contenido originado por un tercero, establecen su responsabilidad sólo si es físicamente posible y técnicamente factible identificar dicho contenido.

Los autores de los contenidos ilícitos -profesionales o no profesionales- responden por sus actos; también los usuarios de Internet que llevan a cabo conductas delictivas.

Los intermediarios, sin embargo, plantean mayores problemas. Sólo pueden ser responsables de los contenidos ilícitos y nocivos "introducidos" por sus clientes en la medida en que tengan una obligación de supervisión y además, les sea técnicamente posible saberlo.

El régimen de responsabilidad propuesto para los intermediarios es el resultado de un sutil equilibrio de intereses entre las partes implicadas, y pretende garantizar a los proveedores o prestadores de servicios la libertad en Internet, haciendo posible al mismo tiempo la persecución de los abusos.

Así entonces, se concluye que existen diversas posturas sobre la atribución de responsabilidad por los contenidos introducidos en Internet. Por un lado, comparan a los proveedores de servicios con los editores, pues ambos brindan el soporte que permite a los autores la divulgación de sus contenidos. En ese sentido, la responsabilidad se dirige al proveedor de servicios al igual que se responsabiliza a los editores con relación a sus obras. De otro lado, tenemos la comparación entre el proveedor de servicios de Internet con las librerías, donde se reconoce la irresponsabilidad por la imposibilidad de controlar la gran cantidad de información que se aloja en su servidor.

En algunos casos, los proveedores de acceso han sido sometidos a investigación debido a la existencia de contenidos ilícitos a los que se acceden a través de su servidor. El tema merece de una clarificación legislativa. Es imprescindible que todos los países tengan claro la responsabilidad del proveedor de contenido; así mismo, debe también quedar claro la irresponsabilidad de los proveedores de servicio o acceso a Internet de los contenidos que terceros alojan en sus servidores o de la empresa que le brinda el acceso a Internet, como regla general, pero algunos juristas consideran que como los propios proveedores de servicios son los que proveen del contenido, son éstos los responsables. En el caso de que los contenidos sean suministrados por un tercero, los proveedores de servicios no son responsables.

Sin embargo, considero que el criterio más acertado es el adoptados en algunos países en donde la posición es de responsabilizar limitadamente al proveedor de servicios sólo cuando un tercero aloja el contenido en su servidor y se pueda

suponer que tiene conocimiento del contenido ilícito y/o no tome las medidas correspondientes para retirar ese contenido una vez que se les haya llamado la atención respecto a él.

Esperamos que las convenciones internacionales, normas que adopten cada país y/o jurisprudencia al respecto se unifique y logre prevalecer lo expuesto en el párrafo anterior, normas y/o convenciones que no deben dar lugar a interpretaciones de distinta índole.

Somos partidarios de evitar que Internet se transforme en lugar donde no se apliquen las normas que rigen la convivencia en sociedad, y especialmente creo importante instar por resguardar derechos tales como la indemnidad sexual, el derecho a la privacidad, el derecho de autor, entre otros, en el ciberespacio. Pero la restricción de derechos y el control público de actos ilícitos en el mundo virtual es difícil y no puede derivar en excesos desproporcionados e injustificados o en prácticas de censura.

Las exoneraciones de responsabilidad propuestas para los intermediarios deben completarse con medidas dirigidas a localizar al infractor, es decir, que proveedores de servicios de internet ofrezcan datos acerca de registros de usuarios, toda vez que "es muy fácil dar con una dirección IP, pero casi imposible conocer la dirección física de esa computadora, respaldada por una legislación nacional que los obligue a solicitar los datos de los proveedores de contenidos y a proporcionarlos a la autoridad competente que los requiera respetándose las garantías de legalidad: los proveedores de contenidos -profesionales o no- y los propios internautas cuando llevan a cabo actividades prohibidas según las leyes de su país. Estas medidas son, en la actualidad, objeto de intensos debates entre las partes afectadas: aquellos que defienden medidas policiales para investigar y perseguir los contenidos ilícitos y aquellos que reclaman la protección de la libertad de expresión, el derecho a la información y derecho a la intimidad.

Uno de los esfuerzos más importantes de lucha contra los contenidos ilícitos y nocivos que circulan en Internet es el tratamiento jurídico de dichos contenidos en Europa, ahí se han dado una serie de propuestas con el fin de solucionar el problema del contenido nocivo que afecta el desarrollo a menores o el contenido ilícito que atenta contra la dignidad del hombre.

Tal es el caso del "Libro verde de la comisión europea acerca de la protección de menores y la dignidad humana en servicios audio visuales e informativos", y la consulta a la comisión de trabajo con relación a la protección de menores del contenido obsceno; este libro promueve el uso de los sistemas de control familiar. Igualmente deja claro que dichos sistemas no son del todo suficientes;

Posteriormente, se emitió la resolución sobre el Libro Verde relativo a la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información (COM(96)0483 - C4-0621/96). En esta norma se acuerda, que todos los Estados miembros deben disponer en sus legislaciones nacionales toda la normativa que tipifique delitos como la pornografía infantil, pero deja claro, que las normas nacionales no ofrecen por sí solas una respuesta satisfactoria a los problemas jurídicos planteados por la universalización y el carácter transfronterizo de Internet.

La comisión transmitió al Parlamento Europeo "La comunicación sobre contenidos ilícitos y nocivos en Internet" (COM (96) 0487 - C4 0592/96), con fecha 17 de Febrero de 1997 que fue adoptada formalmente en "La Resolución del Consejo de Telecomunicaciones sobre contenidos ilícitos y nocivos en Internet". En ambos documentos se insta a los Estados miembros a que pongan en marcha medidas tales como fomentar y facilitar sistemas de autorregulación, que incluyan instancias representativas de los suministradores y usuarios de los servicios de Internet, códigos de conducta eficaces y, eventualmente, mecanismos de

información de emergencia accesibles al público; Fomentar el suministro a los usuarios de mecanismos de filtro y alentar la creación de sistemas de evaluación; por ejemplo, debería fomentarse la norma PICs.

La resolución de la comunicación de la comisión en relación a contenidos ilegales y nocivos en Internet" (COM 96 - 0487) y (C4 0592/96) adoptada por el Parlamento Europeo con fecha 24 de abril de 1997, establecen entre otros: primar el equilibrio entre la garantía de la libre circulación de la información y la protección del interés público.

La Decisión N° 276/1999/CE del Parlamento Europeo y del Consejo del 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria, para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales, impulsa acciones como: Alentar al sector a que impulse el uso de medios de filtros y sistemas de clasificación, que permitan a padres y profesores seleccionar los contenidos apropiados para la educación de los menores a su cargo y a los adultos decidir que contenidos lícitos desean tener acceso y que tengan en cuenta la diversidad cultural y lingüística; Mejorar entre los usuarios el conocimiento de los servicios ofrecidos por el sector, especialmente entre padres, educadores y menores, para que puedan entender y aprovechar mejor las oportunidades que ofrece Internet.

La cumbre sobre contenidos en Internet promovida por la Fundación Bertelsman en cooperación con el grupo Internet Content Raiting for Europe - INCORE supuso uno de los primeros esfuerzos para la adopción de medidas reguladoras adecuadas a los contenidos en Internet, desde la perspectiva de la introducción de sistema de autorregulación compatibles con la protección de los menores en la Red.

La Directiva 2000/31/CE del parlamento europeo y del consejo sobre comercio electrónico de la Comunidad Europea en la que queda claramente establecida la posición de la comunidad europea con relación a la irresponsabilidad del proveedor que brinda el proveedor de servicio y acceso cuando el contenido es de un tercero y la empresa no tenga conocimiento de la ilicitud del contenido. Igualmente faculta a la empresa a retirar el contenido apenas tenga conocimiento.

Considero que debió señalarse que el retiro del contenido debe realizarse a solicitud de la autoridad competente para evitar cualquier tipo de censura privatizada.

Con fecha 15 de junio del 2000, la Comisión Europea publicó el Informe final INCORE sobre propiciar el uso seguro en Internet: Auto - Etiquetado y Filtros. Este informe tiene como finalidad evaluar la posibilidad de un auto etiquetado y filtro desde una perspectiva europea.

Con fecha 2 de Octubre del 2000, se publicó la Convención sobre el Ciber Crimen. Proyecto N° 22 REV 2. Este proyecto, establece entre otros puntos, que cada Estado parte debe normar y adoptar otras medidas como puedan ser necesarias para establecer como ofensas criminales en cada país, al que intencionalmente ayude o sea cómplice en la comisión del delito de pornografía infantil.

En cuanto a los contenidos ilícitos, son patentes los esfuerzos por la elaboración de textos internacionales que faciliten la investigación, persecución y castigo de los responsables. El más claro ejemplo se encuentra en el proyecto de *Convenio sobre la Delincuencia en el Ciberespacio de 2000,* elaborado en el seno del Consejo de Europa. Durante la elaboración de ésta tesis, la Unión Europea estaba negociando su adhesión. El Convenio tiene la virtud de unificar los distintos criterios de los Estados a la hora de sancionar determinadas conductas. Así, por ejemlo, será

perseguible y punible la pornografía infantil cualquiera que sea el Estado desde el que se cometa la infracción.

Mexico podría ser impulsor en la celebración de un convenio cuyo objetivo sea establecer mecanismos que coadyuven a lograr que Internet sea un lugar seguro a través de la disminución de contenidos ilícitos básicamente entre países latinoamericanos, así como con los Europeos. A nivel interno, México puede crear y/o modificar su legislación interna para también regular aspectos como: la difusión de programas destinados a suprimir sin autorización, o neutralizar, los dispositivos técnicos de protección de los programas de ordenador (los *cracks);* la difusión del material pornográfico a menores de edad; la comercialización de la pornografía infantil; los contenidos racistas y xenófobos; los contenidos que informen acerca de la fabricación de explosivos; las páginas web que incitan al suicidio; la vulneración de la protección de datos de carácter personal; las falsedades documentales; la difusión de mensajes injuriosos o calumniosos; o la venta de drogas o armas en Internet, especificar los límites de la libertad de expresión protegiendo de manera más clara los derechos a la intimidad personal y familiar, al honor y a la propia imagen, entre otros, como lo preve la legislación europrea (vgr. España).

El acuerdo de los Quince busca sancionar la simple tenencia de material pornográfico orientada a la comercialización o exhibición y unificar la descripción de los nuevos delitos incrementando las penas, así mismo considero que en México se debía reformar la legislación penal en este sentido.

Cabe resaltar la crucial la labor llevada a cabo por la Unión Europea, cuyas propuestas tienden a convertir Internet en un espacio seguro que concilie la protección del mercado interior y los valores jurídicos de los Estados miembros (protección de menores, indemnidad sexual y de la dignidad humana, libertad de expresión, derecho a la información y derecho a la intimidad).

Los documentos elaborados por las instituciones comunitarias apuntan, por lo que respecta a la lucha contra los contenidos ilícitos y nocivos, a una Decisión que inspirará las legislaciones de los Estados miembros y de todos los Continentes.

Todos los esfuerzos legislativos supondrá la armonización respecto de las exoneraciones de la responsabilidad penal y civil de los provedores de servicios de Internet, muy en la línea de las soluciones contenidas en la DMCA estadounidense e incluso cabría señalar también la CDA, que establece el régimen de responsabilidad de los intermediarios técnicos por la vulneración de los derechos de propiedad intelectual.

No menos importante es otro de los intentos, los códigos deontológicos como el conjunto de normas elaboradas por los propios participantes en la transmisión de la información en línea en los que se establecen las obligaciones respecto de su actividad en Internet; lo importante sería aumentar la credibilidad de los códigos de conducta, incluyendo normas que establezcan las infracciones en caso de incumplimiento, procedimientos de recurso y de mediación.

Ahora bien, si cierto es el acuerdo en los Estados miembros de la comunidad europea acerca de los comportamientos o las informaciones delictivas (pornografía infantil, terrorismo, vulneraciones de los derechos de autor, violaciones del derecho a la intimidad), no cabe decir lo mismo de los contenidos nocivos, ya que estos se basan en concepciones difíciles de medir en una idea global multirracial y multicultural como es la sociedad de la información del siglo XXI.

En cuanto a los contenidos nocivos las redes digitales y la información que por ellas transita plantea nuevos interrogantes: ¿cómo se pueden conjugar los diferentes estándares morales de los diversos países del mundo? ¿tendemos a una fusión de valores? ¿qué ocurre con los países de ámbitos culturales muy distintos? Es

necesaria una reflexión más profunda sobre el acercamiento de los valores éticos, religiosos, sociales y políticos del planeta en el que vivimos.

Sin embargo, creo que la educación a los padres, profesores y menores en el uso adecuado de estas nuevas tecnologías de la información es otra alternativa de solución muy eficaz, al problema del contenido nocivo que circula en la red, pues al ser éste perfectamente legal y circular libremente en la red, puede llegar a ser visto por un menor pudiendo afectarlo en su desarrollo. Pero cabe enfatizar, que es el usuario el que busca y/o solicita el contenido en la mayoría de casos.

La información, la educación y la toma de conciencia de los riesgos de Internet es esencial para lograr una protección eficaz de los menores y de la dignidad humana. El *Libro Verde sobre la protección de los menores y de la dignidad humana* de 1996 insta a padres e hijos a desarrollar una nueva relación con los medios audiovisuales, basada en el conocimiento de los riesgos que implica la navegación en la Red y la información acerca de los medios de protección existentes. En este punto, la educación de los usuarios es esencial. Los padres deben aprender a hacer uso de las redes digitales al igual que hacen sus hijos, siendo conscientes de los beneficios y riesgos que entraña navegar por Internet. Pero la responsabilidad de educar a los menores en el uso seguro de las nuevas tecnologías no reside únicamente en sus padres y educadores, sino que como indica el Consejo de Europa, en la *Recomendación R* (97) 19 *la violencia en los medios electrónicos* es una tarea que debe ser compartida por los gobiernos y los proveedores o desarrolladores de contenidos. Sólo de este modo los menores pueden desarrollar una actitud crítica que les permita autoprotegerse.

Otro intento pueden ser las Campañas de sensibilización a los usuarios: Por ejemplo la prevención adoptada por Australia, Malasia, Singapur, Reino Unido para evitar cualquier riesgo al menor y/o promover el uso de sistema de filtros dirigido a los padres. Muchos países también han implementado en los colegios

programas de entrenamiento en el uso de Internet, durante los cuales se educa precisamente a los menores en los riesgos que puede acarrear Internet y como se puede llegar a evitarse.

La labor desarrollada en los organismos internacionales es reflejo de la preocupación de los gobiernos, la industria y los usuarios por encontrar soluciones que pongan fin a las vulneraciones de los derechos de todos los usuarios.

La reflexión sobre la regulación de Internet debe realizarse tanto a escala internacional como nacional. Por lo que es vital importancia señalar que la necesidad permanente de una cooperación internacional para retirar el contenido ilegal como la pornografía infantil e incentivar el uso de filtros para evitar que los menores accedan al contenido nocivo que pueda afectar su desarrollo; así como para el eficaz funcionamiento de las líneas directas se hace imprescindible, de tal forma que la organización pueda, al recibir la notificación del usuario, ponerse en contacto e intercambiar información con la línea directa del país de origen del contenido para que ésta adopte las medidas necesarias.

Sería ideal que las numerosas conferencias internacionales en las que se aborda el problema de los contenidos ilícitos y nocivos, vean compensados sus esfuerzos y no se queden únicamente en una declaración de intenciones, ya que constituyen un punto de encuentro entre todas las partes implicadas, y buscan el equilibrio entre la libertad de expresión (derecho a comunicar y recibir información) y la protección de la infancia y la dignidad humana entre otros derechos, logrando fomentar en la red el respeto mutuo y la convivencia pacífica entre los usuarios.

Las autoridades públicas y los sujetos que participan en la transmisión de la información en las redes digitales han propuesto medidas de carácter preventivo para aumentar la seguridad de los menores cuando navegan por Internet. Si Internet es una herramienta para los delincuentes, también debe serlo para los que están en

del lado de la ley. Al igual que para las organizaciones que trabajan en la concientización de la opinión pública respecto a este grave problema, a modo de ejemplo, iniciativas como Stop-pedofilia.net, página que permite enviar denuncias a la policía y que moviliza a cientos de webmasters, deberían abundar y hacer que la lucha contra la pornografía infantil sea más fácil que su consumo; así como los virus que sin causar daños en el sistema del equipo que se ven afectados por él, rastrea los ordenadores que almacenan imágenes de pornografía infantil y denuncia ante las autoridades a sus propietarios a través de un correo electrónico que se envía desde el ordenador del sospechoso hasta diferentes agencias gubernamentales; la co-rregulación de los sectores privados y gubernamentales, el filtrado y la clasificación de contenidos así como la sensibilización, y sobre todo la celebración de Instrumentos Internacionales cuyo objetivo sea el combate de los contenidos ilícitos y nocivos en Internet mediante la colaboración internacional, al igual que la regulación interna de cada país al respecto, son por ahora la medidas más viables para lograr cuando menos una notable disminución de los contenidos ilícitos e incluso nocivos de la Red.

Queda claro que el contenido del Internet no se puede regular con un solo ordenamiento legal, como un todo integral, básicamente por dos cuestiones: la primera, por la diversidad de sus contenidos; y la segunda; por la dificultad de aplicar la legislación nacional desde un Estado a una realidad como Internet, más aún, si una determinada conducta no se encuentra tipificada en todas las normativas nacionales; por ello, el contenido de Internet debe regularse en distintos cuerpos normativos de acuerdo a la materia, y basándose en una unificación de definiciones, conceptos y criterios de determindas conductas consideradas como ilícitas por los Estados firmantes y en una cooperación internacional para fincar la responsabilidad y aplicar la sanción correspondiente al infractor.

Los jueces y magistrados se enfrentan con nuevas formas de vulneración de valores jurídicos. En la jurisprudencia comparada se advierten decisiones tomadas

sin los suficientes conocimientos técnicos, lo que ha generado sentencias en las que los jueces, responsabilizando a los intermediarios, les imponen deberes de vigilancia y supervisión de los contenidos que transitan por las redes digitales. Por ello, se hace necesario impulsar la formación en nuevas tecnologías de jueces y magistrados, en general a quienes ejercen la función jurisdiccional.

Considero importante lograr despertar un real interés entre los juristas, magistrados y jueces mexicanos en adquirir conocimientos sobre las características técnicas y las peculiaridades de Internet para resolver adecuadamente los problemas jurídicos que se plantean.

En los próximos años seremos testigos de cambios vertiginosos en el mercado de las comunicaciones. El uso de Internet crece a un ritmo que sus creadores no hubieran podido predecir. Se "cuelgan" en la Red miles de páginas web cada día, aparecen nuevos servicios y aplicaciones constantemente. Las nuevas tecnologías borran las fronteras entre los soportes: ahora es posible acceder a Internet desde un teléfono móvil o integrar la televisión y la radio en Internet. En este momento, los contenidos pasan a cobrar una importancia fundamental y son el elemento clave para atraer la atención del usuario. De ello son conscientes las empresas de Internet que junto a los servicios, ofrecen cada vez más contenidos.

Ciertamente, la existencia de contenidos ilícitos y nocivo en Internet preocupa, pero debemos confiar en que las soluciones propuestas atajen eficazmente el problema, Internet es global y todos tenemos el derecho a sentirnos seguros.

BIBLIOGRAFIA

- AKDENIZ, Y.; "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach", en *Law and the Internet: Regulating Cyberspace,* Hart Publishing, 1997, págs. 223-241. www.cyber-rights.org. Consultada el 14 de marzo de 2000.

- BARRIOS GARRIDO, Gabriela y O. "Internet y derecho en México", Ed. Mc Graw Hill. México.

- BORCHARDT, M.G.; "Taking Stock: Activities of the European Commission in the Fight Against Child Pornography". Conferencia de Viena de septiembre de 1999. Combating Child Pornography on the Internet". www.stop-childporn. Consultada el 3 de marzo de 2000.

- CADEN, M. y LUCAS, S.; "Accidents on the Information Superhighway: On-line Liability and Regulation", de 13 de febrero de 1996, www.urich.edul. Consultada el 12 de febrero de 1999.

- CALVO CARAVACA, Alfonso Luis, "Conflictos de Leyes y Conflictos de Jurisdicción en Internet", Ed. COLEX, Madrid, 2001.

- Consejo General del Poder Judicial, "Problemática Jurídica en torno al Fenómeno de Internet", Director Juan José Martín-Casallo López, Cuadernos del Poder Judicial, Madrid, 2000.

- CSONKA, P.; "Contribution to the Conference on combatting child pornography on the Internet", Conferencia internacional celebrada en Viena los días 29 de septiembre y 1 de octubre de 1999. www.stop-childpornog.at. Consultada el 03 de marzo de 2000.

- FERNANDEZ ESTEBAN, María Luisa, "Nuevas Tecnologías, Internet y Derechos Fundamentales", Ed. Mc Graw Hill, México.

- FOURNIER, A.; "Sexual Abuse of Children on Internet: A New Challenge for INTERPOL". *www.*unesco.org. Consultada el 1 de marzo de 2000.

- G. PARERAS, Luis, "Internet y Derecho", Ed. Masson, S.A., México.

- KREBS, B.; "Educate, don't Regulate", en *Computer Currents,* de 24 de febrero de 2000. www.currents.net. Consultada el 28 de febrero de 2000.

- Le TOQUIN, c.; "Relationships of Horlines with Law Enforcement". www.stop-childpornog.at. Consultada el 3 de marzo de 2000.

- LESSIG, L.; "Tyranny in the Infrasrructure", julio de 1997, www.wired.com Consultada el 2 de marzo de 2000.

- LUTZKER, A. LUTZKER, S. y SETTLEMYER, C.H.; "The Digital Millenium Copyright Act. Highlights of New Copyright Provisions Establishing Limitation of Liability for On-line Service Providers". www.arl.org. Consultada el 3 de febrero de 1999.

- LUTZKER, A.; "Primer on the Digital Millenium. What the Digital Millenium Copyright Act and the Copyright Term Extension Act Mean for the Library Community". www.arl.org. Consultada el 5 agosto de 1999.

- MARIN PEIDRO, Lucía, *Los Contenidos Ilicitos y Nocivos en Internet*. Ed. Fundación Retavisión, Madrid, 2000.

- OLSON, B.; "Application of American Legal Theories and Proposal of the Intellectual Capitalism Theory", diciembre de 1999. www.bc.edu. Consultada el 22 de marzo de 2000.

- PANETHIERE, D.; "On-Line Copyright Infringement Liabiliry and the Significance of Recent US Legislation". www.jura. Consultada el 23 de febrero de 1999.

- *Plaitform for Internet Content Selection* (PICS), "PICS: Internet Access Controls Without Censorship", www.w3.org. Consultada el 2 de marzo de 2000.

- RIBAS ALEJANDRO, J.; "Delitos en Internet". www.aui.es. Consultada el 25 de febrero de 2000.

- ROJAS AMANDI, Víctor Manuel, "El uso de Internet en el derecho", Ed. Oxford, Colección de Estudios Jurídicos, México.

- SANCHEZ TRUJILLO, Guillermo, "Internet para Abogados", Ed. Señal Editora, Tercera Edición, México, 2001.

- TELLEZ VALDEZ, Julio, *Derecho Informático*. Ed. Mc Graw Hill. Segunda Edición. México 1995. págs 283.

- TELLEZ VALDEZ, Julio, *Derecho Informático*. Ed. Mc Graw Hill. Tercera Edición. México 2003. págs 514.

- THOUMIRE, L.; "Abuses in the Cyberspace. The Regulation of Illicit Messages Diffused on the Internet", junio de 1996. Disponible en http://www.juriscorn.net, Consultada el 1 de marzo de 2000.

- TORNABENE, "Internet para Abogados", Ed. Universidad, México.

- WILLIAMS, N.; "The Contributions of Hotlines to Combating Child Pornography on the Internet". www.inhope.org. Consultada el 10 de febrero de 2000.

LEGISLACION

- CODIGO PENAL FEDERAL. Diario Oficial de la Federación del 14 de agosto de 1931 y reformas.

- CODIGO DE PROCEDIMIENTOS PENALES. Diario Oficial de la Federación del 30 de agosto de 1934 y reformas.

- CONSTITUCION POLITICA DE LOS ESTADOS UNIDOS MEXICANOS, Comentada y Concordada, Universidad Nacional Autónoma de México, Coord. Miguel Carbonell, Tomo I, Editorial Porrúa, Decimoquinta edición, México, 2000.

- LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACION Y COMERCIO ELECTRONICO. Boletín Oficial del Estado del 12 de Julio del 2002. España.

- LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA GUBERNAMENTAL. Diario Oficial de la Federación del 11 de junio de 2002.

- LEY SOBRE DELITOS DE IMPRENTA. Diario Oficial de la Federación del 12 de abril de 1917.

- LEY DE LA POLICIA FEDERAL PREVENTIVA. Diario Oficial de la Federación del 4 de enero de 1999.

- REGLAMENTO DE LA POLICIA FEDERAL PREVENTIVA. Diario Oficial de la Federación del 26 de abril de 2000.

HEMEROGRAFIA

- "Austria intenta (sin éxito) cortar la distribución de pornografía a través de Internet", Diario el Mundo, 1 de abril de 1997, disponible en http://www.el-mundo.es. Consultada el 3 de marzo de 2000.

- CARDENAS VALDEZ, Octavio. El Universal. "Mediante un chat en 15 días pueden abusar de sus hijos". 12 de noviembre de 2001. Pág. 14.

- JUÁREZ, María Estela, La jornada. "Fácil, La Promoción de Pornografía Infantil por Internet, Revela la PFP". Agosto 2001.

- MIGUEL ASENSIO, Pedro Alberto De, "Derecho Privado de Internet" Ed. Civitas, Segunda Edición, Madrid, 2001.

- NIETO, Leopoldo. Revista Epoca. Internet. "Trinchera predilecta de pedófilos". 6 de agosto de 2001. Págs. 28 – 31.

- OROZCO, Mónica. La Jornada. "Rastreara la Policía Cibernética Bandas de Pornografía Infantil". Julio de 2001.

- Periódico La Jornada. "El Paraíso de los Pederastras". Sección Sociedad y Justicia. 18 de agosto de 2001. Pág. 37.

- "Principales incidentes en Internet español" .Diario *El País.* Disponible en http://www.elpais.es. Consultada el 24 de febrero de 2000.

- Periódico Reforma. "Advierte Policía Cibernética Sobre Vacío Legal". 30 de julio de 2001.

- RODRIGUEZ GONZALEZ, Gustavo. Excelsior. "Atrapan a sujeto dedicado a la Explotación Sexual de Menores". 12 de julio de 2001.

- REA PRIETO, Martín. El Universal. "Policías Cibernéticos encubiertos van tras Productores de Pornografía Infantil". 11 de julio de 2001.

- REYES, Jorge. Periódico Reforma. "Busca la PFP a Pedofilos en Internert". 11 de
julio de 2001.

- SÁNCHEZ, Julian y Carlos Benavides. El Universal. "La Amenaza, en el Hogar. Sección Nación". 12 de julio 2001. Págs. 14 y 15.

PONENCIAS

- GUY DE VEL, ponencia impartida en el Congreso mundial contra la explotación sexual de los nifios de Viena en octubre de 1999, "Taking Stock of the Activities of the Council of Europe". www.stop-childpornog. Consultada el 3 de marzo del 2000.

- RODRIGUEZ PEREDA, Katitza. Tratamiento Jurídico de los Contenidos Nocivos e Ilegales que circulan en Internet. Memorias del VIII Congreso Iberoamericano de Derecho e Informática por la Universalización del Derecho. México. 21 a 25 de noviembre del 2000.

- JIJENA LEIVA, Renato Javier. Criterios Jurisprudenciales en Materia de Responsabilidades de los ISP. Memorias del VIII Congreso Iberoamericano de Derecho e Informática por la Universalización del Derecho. México. 21 a 25 de noviembre del 2000.

- DORREGO, Claudia Silvina. Hacia una Protección no Diversificada en dos Mundos Convergentes. Memorias del VIII Congreso Iberoamericano de Derecho e Informática por la Universalización del Derecho. México. 21 a 25 de noviembre del 2000.

DIRECCIONES CONSULTADAS

- www.obyron.com. Internet y la WWW. 21 de febrero de 2003.

- www.infoperu.com. Internet e Intranet. 21 de febrero de 2003.

- www.utem.cl. Manual de Internet. 21 de febrero de 2003.

- www.delitosinformaticos.com. Nuevo Programa que detecta la Pornografía Infantil en Internet. 24 de noviembre de 2000.

- www.delitosinformaticos.com. Descubierta una Red Pedófila en Internet. 1 de diciembre de 2000.

- www.delitosinformaticos.com. Espectacular aumento de la Pornografía Infantil en España a través de la Red. 17 de diciembre de 2000.

- www.delitosinformaticos.com. Detienen en Rusia a Traficantes Pornografía Infantil en Internet. 26 de diciembre de 2000.

- GARCIA, Noelia. www.delitosinformaticos.com. Estadísticas de Delitos en la Red. 9 de enero 2001.

- www.delitosinformaticos.com. Nueva ley sobre pornografía infantil en EEUU. 3 de febrero de 2001.

- www.delitosinformaticos.com. Stop a la Pornografía Infantil. 11 de febrero de 2001.

- www.delitosinformaticos.com. Combaten en la Web Pornografía Infantil. 24 de febrero de 2001.

- www.delitosinformaticos.com. Los "Ciberdelitos" serán más perseguidos por las Policías Nacionales. 8 de marzo de 2001.

- www.delitosinformaticos.com. ¿Es delito la pornografía infantil virtual?. 19 de marzo de 2001.

- www.delitosinformaticos.com. Canadá castiga con una fuerte ley la pornografía infantil en Internet .19 de marzo 2001.

- www.delitosinformaticos.com. Caen dos redes de Pornografía Infantil por Internet. 29 de marzo de 2001.

- www.delitosinformaticos.com. Instructor culpable de pornografía infantil. 11 de abril de 2001.

- www.delitosinformaticos.com. El FBI alerta sobre el aumento del Cibercrimen en los últimos meses. 14 de abril de 2001.

- VALDES, Frank. www.delitosinformaticos.com. La mayor red de pornografía infantil estaba organizada desde España. 21 de abril de 2001.

- www.delitosinformaticos.com. Desarticulan una Red Internacional de pornografía infantil en Internet. 21 de abril de 2001.

- www.delitosinformaticos.com. La mayor Red de Pornografía Infantil estaba organizada desde España. 22 de abril de 2001.

- www.delitosinformaticos.com. La distribución de pornografía infantil por Internet es el delito que más prolifera en el mundo. 25 de abril de 2001.

- www.delitosinformaticos.com. Cotino pide que se endurezca la persecución de la pederastia en Internet. 27 de abril de 2001.

- www.delitosinformaticos.com. Un experto en Internet afirma que uno de cada cinco niños que se conecta a un chat es requerido por pederastas. 28 de abril de 2001.

- www.delitosinformaticos.com. Clausurada una guardería que usaba a los niños como material pornográfico. 4 de mayo de 2001.

- www.delitosinformaticos.com. Se alerta de pedofilia en el portal MSN.es. 14 de mayo de 2001.

- www.delitosinformaticos.com. Andalucía encabeza la lista de detenidos por "ciberdelincuencia". 15 de mayo de 2001.

- www.delitosinformaticos.com. UCE alerta del "libre acceso" de menores a webs con contenidos pornográficos en ciber-cafés. 17 de mayo de 2001.

- www.delitosinformaticos.com.. Una nueva página de Microsoft alberga 436 fotografías de pornografía infantil. 17 de mayo de 2001.

- www.delitosinformaticos.com. Alto tribunal EEUU revisará ley de pornografía infantil online. 23 de mayo de 2001.

- www.delitosinformaticos.com. Estados Unidos aprueba becas para policías cibernéticos. 23 de mayo de 2001.

- www.delitosinformaticos.com. Una Web Porno colapsa a la Policía. 11 de mayo de 2001.

- www.delitosinformaticos.com. Documento de la Interpol sobre cibercrimen, 25 de mayo de 2001.

- www.delitosinformaticos.com. Cruzada «hacker» contra los pederastas. 2 de junio de 2001.

- www.delitosinformaticos.com. Informe de la Comisión Europea sobre el Cibercrimen. 02 de junio de 2001.

- www.delitosinformaticos.com. Preocupan a fundador de Internet los planes de lucha contra delito informático 5 de junio de 2001.

- www.delitosinformaticos.com. La UE propone impulsar un Sistema de Lucha contra el Ciberdelito. 7 de junio de 2001.

- www.delitosinformaticos.com. El Código Penal no es instrumento válido contra la pornografía en Internet, según el TSJ de Cataluña. 9 de junio de 2001.

- www.delitosinformaticos.com. El "Cuerpo de Policía Cibernética" luchará contra la pornografía infantil. 9 de junio de 2001.

- www.delitosinformaticos.com. McAfee crea un software para proteger a los menores de los peligros de Internet. 20 de junio de 2001.

- www.delitosinformaticos.com..La Policía precinta un ordenador en la Consejería andaluza de Economía, que contenía pornografía infantil bajada de Internet. 04 de julio de 2001.

- www.delitosinformaticos.com. Infiltrado en "chat" permite capturar pederastas en Costa Rica. 12 de julio de 2001.

- www.delitosinformaticos.com. PRODENI denuncia el fácil acceso de los menores a la pornografía en los "cibercafés". 12 de julio de 2001.

- www.delitosinformaticos.com. Desmantelan en EEUU empresa de Internet de pornografía infantil. 09 de agosto de 2001.

- www.delitosinformaticos.com. La Policía mantiene 300 operaciones abiertas contra la pedofilia en la Red y recibe veinte 'e-mails' al día de denuncias 10 de agosto de 2001.

- www.delitosinformaticos.com. Japón.-La delincuencia en Internet aumenta un 60 por ciento en el primer semestre empujada por los delitos de Pedofilia. 10 de agosto de 2001.

- www.delitosinformaticos.com. Espectacular aumento de los Cibercrímenes en Japón. 13 de agosto de 2001.

- www.delitosinformaticos.com. Busca la PFP a Pedófilos en Internet. 12 de diciembre 2001.

www.delitosinformáticos.com. *Regulación del Acceso a Internet por Menores.* Consultada el 18 de marzo de 2003.

- www.pfp.gob.com.mx

- www.pgr.gob.com.mx

- www.delitosinformaticos.com

- www.fbi.gov.com

- www.derechos.org

- www.aui.fr/Dossiersl Amend-fillonl analyse-amend.htm.

- www.aui.es/padres/familia

- www.hotbot.com

- www.ole.es

- www.yahoo.com

- www.w3.org

- www.cyber-rights.org

- www.epic.org

- www.europol.eu.int/home.htm

- www.adl.org/hate-patrol/info/HateFilterFAQ.html

- www.cyberpatrol.com

- www.guardiacivil.org

- www.unesco.org/webworld/innocence/events.html

- www.interpol.int

- jugendshutz.net

- www.fsm.de

- hotline.ispa.at

- www.info.fundp.ac.be/~mapi/mapi-fr.html

- www.redbarnet.dk

- www.missingkids.com/cybertip

- www.afapc.org

- childhouse.uio.no/redd_barna
- www.meldpunt.org
- www.internetwacht.org
- www.inhope.org
- www.oecd.org.
- www.w3.org/pub/www/PICS
- www.disney.com
- www.juniomet.com
- ww.actf.co
- ww.kiddonet.com
- ww.surfmonkey.com
- www.yourownworld.com
- www.nsbf.org/safe-smart/regulation.htm
- www.unesco.org
- www.ua.es/internet/cod_etico.html