



Asociación Argentina de Derecho de Alta Tecnología

Información
Institucional

Eventos

Disciplinas
Comisiones

Departamentos
Institucionales

Biblioteca

Publicaciones

Links

Suscripciones

Asociarse

Correo

Foros

Asociación Argentina de Derecho de Alta Tecnología

LA LIBERTAD DE EXPRESIÓN Y EL DERECHO DE INTIMIDAD EN INTERNET

Por Gabriela Guerriero.

Literalmente traducida la palabra **Internet** significa "entre redes" Técnicamente podríamos definirla como una red global de equipos informáticos que se comunican mediante un lenguaje común, donde nadie posee ni controla todo el conjunto.

Pero **Internet** es mucho más que un medio de intercomunicación mundial, ya que se presenta como un naciente paradigma de la relación humana, en el que se manifiestan desde expresiones artísticas y culturales hasta celebración de contratos de las más diversas características.

En este sentido John Perry Barlow^[i] (1) utilizó el término **ciberespacio**^[ii] (2) para referirse a Internet no como un mero conjunto de ordenadores, sino como un lugar donde se establecen interrelaciones entre personas libres de ataduras físicas.

Una de las características "invisibles" de Internet, es la estrecha vinculación existente entre el mundo virtual y el mundo jurídico. Y al decir *mundo jurídico* no estoy haciendo referencia a leyes u ordenamientos positivos nacionales o internacionales, sino a la **autorregulación** que proviene de cientos de contratos (la mayoría innominados y hasta tácitos) que sustentan la existencia de la red.

Dentro del **ciberespacio** existen normas, reglas que le son propias y que no han emanado de autoridad legislativa alguna, ni nacional ni supranacional. Internet se autorregula mediante prácticas que se van elaborando progresivamente por grupos de usuarios o asociaciones profesionales que tratan de definir y difundir reglas de uso leal y responsable.

La autorregulación, que descansa en el marco normativo de casi todos los ordenamientos jurídicos donde se contempla la autonomía de la voluntad^[iii] (3) como fuente creadora de derechos y obligaciones, aporta una respuesta totalmente satisfactoria en numerosos sectores que desarrollan su actividad en el ciberespacio (comercio electrónico, marketing, publicidad, etc.). Esta realidad podría llevar a la conclusión que no es necesario legislar específicamente sobre Internet, permitiendo que la misma funcione sobre los carriles de la autonomía de la voluntad y los principios generales contenidos en nuestro ordenamiento jurídico.

Pero teniendo en cuenta que Internet ha provocado una revolución tecnológica, cultural y económica que se caracteriza por la descentralización y globalización, surgen algunos interrogantes: La reglamentación de los derechos y garantías constitucionales que se encuentra vigente en nuestro ordenamiento jurídico ¿es suficiente para regular el ejercicio de las mismas en el campo de Internet?, ¿Cómo funcionan las garantías constitucionales de libertad de expresión y privacidad en la red?. La normativa vigente ¿brinda seguridad jurídica frente a los actos lesivos que se producen mediante su utilización?. En resumen: **¿Es necesario regular Internet?**

La intención del presente trabajo es acercar alguna respuesta a los interrogantes planteados.

II.- LOS LLAMADOS CIBERDERECHOS

En el campo de Internet aparece una nueva visión de algunos derechos y libertades humanas, que la terminología en boga ha denominado **ciberderechos** y entre ellos destacan, por ser los más importantes para el correcto desarrollo de Internet y ser los más amenazados:

La libertad de expresión: entendida como la garante de una Internet formada por una comunidad libre que pueda expresar sus pensamientos y difundir su cultura sin trabas.

El derecho a la privacidad: que permite comunicarse sin interferencias ajenas.

A estos dos derechos recientemente se ha sumado otro grupo de derechos, los que se denominan **derechos materiales** (para diferenciarlos de los formales ya enumerados), cuyo ejercicio estaría íntima y exclusivamente relacionado con Internet. Ellos son:

El derecho a acceso libre a Internet y derecho de tarifa plana telefónica. Ambos derechos se refieren al acceso universal a la red. Y encuentran su fundamento en que todos los seres humanos tienen que tener igualdad de posibilidades para conectarse a la red, ya que, de que serviría garantizar en la red la libertad de expresión cuando es demasiado caro conectarse.

En defensa de estos derechos se instituyó la **Huelga de internautas** o **cibernautas**. España fue uno de los primeros países donde se llevó a cabo este tipo de huelga, hecho éste que fue imitado

luego en otros países de la Unión Europea y en Latinoamérica(4)[iv]. Este tipo de huelga, mas parecido a un boicot, consiste en no utilizar el teléfono ni conectarse a Internet durante 24 horas. La huelga de España fue la primer acción política conjunta de internautas que se dio en forma masiva y también una advertencia de que en el futuro los cibernautas podrían ser una comunidad con ideas y programas propios. Esta acción fue apoyada por muchos simpatizantes y organizaciones, secundada incluso por portales, buscadores y otros lugares de la Internet Hispana.

III.- LA LIBERTAD DE EXPRESION Y SU EJERCICIO EN INTERNET

1.- Encuadre conceptual.

La **Libertad de expresión** es un derecho humano fundamental, de carácter crucial para una sociedad libre y democrática. Las constituciones democráticas y los Tratados internacionales que afirman la vigencia de los derechos humanos garantizan a todo individuo el pleno uso y goce de esta libertad(5)[v].

La libertad de expresión tiene plena vigencia en el medio cibernético y garantiza que cualquier ser humano pueda expresar sus pensamientos y difundir su cultura en la red sin trabas ni censura. Y se puede sostener que la libertad de expresión tiene un mejor ámbito de vigencia en Internet que en los medios tradicionales de comunicación. La frase muchas veces mencionada "La libertad de expresión es para quien puede pagarla" - que hace alusión a los obstáculos financieros que provocan que la mayoría de los individuos no tengan la posibilidad de emitir sus opiniones a través de una emisora de radio, un periódico o una emisora de TV- ha quedado en el pasado ya Internet cambia radicalmente la situación. Con pocos recursos económicos cualquiera está en condiciones de crear su propia publicación en la World Wide Web o jugar un papel de emisor activo en los múltiples foros de discusión existentes.

Otra característica esencial y diferencial de Internet es que en la red las funciones de emisor y receptor son plenamente intercambiables, se hace posible la comunicación "muchos a muchos".

Todo ello hace que Internet permita expandir la vigencia de la libertad de expresión y por otro lado también posibilite que esta libertad sea utilizada indebidamente para fines espurios que atenten contra la dignidad humana.

2.- Encuadre normativo. Límites a su ejercicio.

La mayor parte de los activistas defensores de los ciberderechos no conciben la existencia de límites en el ejercicio de esta facultad. Reclaman la libertad absoluta de expresión, no condenan sólo la censura previa sino todo tipo de censura aunque sea posterior a la publicación de la página.

Cada vez que los gobiernos o corporaciones han intentado censurar una pagina de Internet han sufrido el efecto boomerang de la red(6)[vi]. Este efecto, conocido como **efecto Gilmore**, consiste en que la red a través de las ONGs virtuales responde al intento de silenciar un documento con la creación de copias y mirrows de la página prohibida, que le otorgan mucha más publicidad que la que tenía antes de ser censurada. Este mecanismo se activa cuando la libertad de expresión está en peligro, entendiendo que ésta es absoluta, innegociable, y sin interesar cual es el contenido de la página Web censurada. Estas organizaciones encuentran sustento filosófico en los principios kantianos donde las libertades son absolutas, y cualquier restricción sería considerada maquiavélica. Es decir que permitir la censura para ciertas páginas sería, desde este punto de vista, aseverar que "el fin justifica los medios".

La defensa de las libertades en Internet así considerada puede ocasionar graves perjuicios. Analizaré brevemente dos casos de páginas censuradas en España que provocaron polémica, por tratarse de páginas que contenían lo que se conoce como **listas negras en la red**. Una de ellas es la lista de la ACT (Asociación contra la tortura) que contenía una nómina de agentes policiales de diversos cuerpos que habían sido juzgados por tortura o malos tratos y policías que estaban en investigación. España prohibió dicha página por ser violatoria de la Ley de Protección de Datos(7)[vii]. El otro caso es el de la lista NUREMBERG, sitio dirigido por grupos antiabortistas que ofrecía una lista de médicos que practicaban abortos y se incluían datos personales de los mismos, hasta su dirección y número de teléfono.

Hubo organizaciones que, con una visión formalista de la libertad de expresión, hicieron mirrows de ambas páginas censuradas, sin importar las consecuencias que la publicación de dichos datos pudiera ocasionar. Nos encontramos en ambos casos con un verdadero conflicto ético: estamos ante un conflicto de derechos básicos, donde diversos derechos se enfrentan entre sí y tenemos que decidir cual es más importante.

La existencia de estas listas constituyen una violación al derecho de privacidad de las personas incluidas (e incluso agresiones potenciales a derechos más básicos como la vida o la integridad física por los eventuales ataques a que se podrían ver expuestas las personas publicadas). En el enfrentamiento entre la libertad de expresión de la entidad antiabortista que puede sobrevivir perfectamente sin la necesidad de la lista negra y el derecho de intimidad y privacidad de los médicos, debe primar este último. De esta valoración ética surge la justificación de la censura a posteriori de la página, e incluso debería haber primado esta valoración en las organizaciones que – so pretexto de defender los derechos- han realizado las copias de la misma.

Si bien la censura contra la red es casi fácticamente imposible, sobre todo por el efecto

Gilmore, no se puede partir de la base de que el derecho de libertad de expresión es absoluto, sino que éste debe ceder cuando su ejercicio ocasione colisión con otros derechos humanos que se encuentran por encima en la escala de valores universales.

En nuestro ordenamiento jurídico se encuentra vigente el **decreto 1279/97** que se refiere al derecho constitucional de libertad de expresión, el cual tomando como base el **artículo 14 , 32 y 42 de la Constitución Nacional** declara que el servicio de Internet se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión correspondiéndole en tal sentido las mismas consideraciones que a los demás medios de comunicación social.

Esta norma ampara la libertad de expresión en Internet y condena la censura previa, al control previo de contenidos sobre las páginas web, propugnando la autocensura mediante la utilización del software adecuado que califica los contenidos de los sitios. Pero la citada norma no da legalidad previa a todo contenido en la web, lo que implica que si mediante la publicación de una página web se cometiese alguna conducta antijurídica, el responsable sería pasible de las sanciones respectivas y por aplicación de las normas de derecho común el damnificado podría solicitar a los tribunales que ordenen el levantamiento de la misma, tanto como medida cautelar o como definitiva, e incluso los jueces podrían establecer la pena conminatoria o de astreintes al servidor que sostiene la página por cada día de demora en el cumplimiento de la sentencia. Todo ello al margen de la reparación que por daños y perjuicios el damnificado pudiera reclamar apoyado en el art 1109 del C. Civil.

En este sentido la Corte Suprema ha resuelto(8) [viii] que "el aludido derecho a la libre expresión no es absoluto en cuanto a las responsabilidades que el legislador puede determinar a raíz de los abusos producidos mediante su ejercicio, sea por la comisión de delitos penales o actos ilícitos civiles.(...) el derecho de expresión de ideas u opiniones no puede extenderse en detrimento de la necesaria armonía con los restantes derechos constitucionales, entre los que se encuentran el de la integridad moral y el honor de las personas(art 14 y 33 CN). Es por ello que el especial reconocimiento constitucional de que goza el derecho de buscar, dar, recibir y difundir información e ideas de toda índole, no elimina la responsabilidad ante la justicia por los delitos y daños cometidos en su ejercicio."

La Convención Americana sobre Derechos Humanos, la cual tiene jerarquía constitucional en virtud del artículo 75 inc 22 , establece en su art. 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 y 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..." .

De las fuentes citadas podemos concluir que el ejercicio de la libertad de expresión en Internet no es absoluto para nuestro ordenamiento jurídico, ya que si bien no hay normas que regulen específicamente sus contenidos existe un límite genérico impuesto a esta libertad que es el respeto de los demás derechos constitucionales y una sanción por los abusos producidos por su ejercicio que consiste en la imputación de responsabilidad civil o penal.

3.- Contenidos ilegales y contenidos inconvenientes.

Convendría determinar que tipo de contenidos pueden considerarse como un producto del ejercicio abusivo del derecho de libre expresión en Internet. Para ello, siguiendo dos documentos de la Comisión Europea(9) [ix], podríamos hacer una diferenciación entre contenidos ilegales y contenidos perjudiciales o inconvenientes para menores dentro de la red.

El Libro Verde establece que "... el acceso a determinados tipos de material puede ser prohibido para todos, independientemente de la edad de la audiencia potencial o el medio utilizado. Aquí es posible, al margen de las diferencias en las legislaciones nacionales, identificar una categoría general de material que viola la dignidad humana, consistiendo principalmente en pornografía infantil, violencia extrema gratuita e incitación al odio, discriminación y violencia racial o de otro tipo. En segundo lugar, el acceso a determinados materiales que pueden afectar el desarrollo físico y mental de los menores está permitido sólo a los adultos (...) El objetivo está limitado, por lo tanto , a evitar que los menores encuentren, por accidente o por otras razones, materiales que puedan afectar a su desarrollo físico y/o mental. Estos temas se confunden a veces por una u otra razón, pero es esencial mantener la distinción entre estas diferentes cuestiones: son objetivos diferentes que plantean problemas diferentes y exigen soluciones diferentes. Claramente, las medidas necesarias para imponer una prohibición total son diferentes de las que se necesitan para restringir el acceso de los menores o para evitar el acceso casual de los adultos".

Del Texto transcrito surge clara la diferenciación. Se identifican los contenidos ilegales: pornografía infantil, pornografía violenta, incitación al odio y la violencia, etc., tema éste que se amplía en la Comunicación sobre contenido ilegal señalando dos ámbitos de actuación para evitar su publicación y difusión: la cooperación judicial y policial internacional y la definición de responsabilidades de las partes que intervienen en dicha publicación o difusión de los materiales.

En cuanto a los contenidos perjudiciales o inconvenientes para menores, la Comisión recomienda la autocensura, partiendo del principio de autonomía individual mediante la utilización de un software de filtrado adecuado.

En nuestro derecho vigente no existe esta diferenciación. Si bien ya hemos dicho que el Estado no interfiere ni regula sobre los contenidos en Internet, si lo hace en materia de radiodifusión en los artículos 14 a 25 de la ley 22.285. Dentro de este articulado protege el derecho a la intimidad de las personas, estableciendo en su art. 16 que "las emisiones de radiodifusión no deben perturbar en modo alguno la intimidad de las personas", y luego enumera emisiones que quedan prohibidas, tales como las que atenten contra la salud o estabilidad de los destinatarios del mensaje y las que tengan contenidos prohibidos para menores de 18 años. Incluye entonces tanto los contenidos ilegales como los perjudiciales dentro del mismo tratamiento legal.

En su artículo 18 la ley de radiodifusión impone los límites a la libertad de expresión al establecer que "La libertad de información tendrá como únicos límites los que surgen de la Constitución Nacional y de esta ley. (...) La información no podrá atentar contra la seguridad nacional, ni implicar el elogio de actividades ilícitas o la preconización de la violencia en cualquiera de sus manifestaciones."

Por otro lado, nuestro Código Penal sanciona como delito el suministro de material pornográfico a menores de 14 años (art 128 in fine), lo que implica que quien permitiera el acceso a menores de 14 años a una página de Internet de contenido pornográfico estaría cometiendo una conducta ilegal y tipificada. Esto nos aleja aún más de la diferenciación entre contenidos ilegales y contenidos perjudiciales.

Analicemos a la luz de las normas vigentes en nuestro ordenamiento cuáles son las conductas antijurídicas que podrían cometerse por el uso abusivo del derecho de libre expresión en Internet:

- Violación de la privacidad o intimidad (por ejemplo mediante la publicación de las llamadas "listas negras") **(10)** [\[x\]](#)
- Configuración del delito de calumnias o injurias. **(11)** [\[xi\]](#)
- Configuración del delito de publicación de imágenes pornográficas en las que se exhiban menores de 18 años. (art.128 Código Penal primera parte) **(12)** [\[xii\]](#)
- Configuración del delito de suministro de material pornográfico a menores de 14 años (art. 128 Código Penal in fine) **(13)** [\[xiii\]](#).
- Contenidos que impliquen discriminación de cualquier tipo, o inciten a la violencia, o perpetren apología del delito.

Las normas citadas no mencionan específicamente a Internet, pero en todos los casos, la normativa sería aplicable a cualquiera de los actos que se realizaran utilizando a la red como medio de transmisión, ya que el hecho de levantar un contenido determinado a una página encuadra en los términos "reproducir por cualquier medio", "producir imágenes", "suministrar material". Además sería asimilable a publicar.

3.- Responsabilidad Civil y Penal por contenidos ilícitos en Internet.

Cuando alguno de los actos ilícitos antes mencionados se realiza mediante publicaciones en los medios tradicionales (prensa, radiodifusión, etc) el responsable es de fácil identificación, pero cuando se realizan mediante la red nos encontramos ante el problema fáctico y jurídico de establecer quienes serían los autores responsables. En primer lugar y por aplicación del art 1109 el autor ideológico de la página web es sin lugar a dudas el primer responsable de la acción antijurídica. Pero para que ese contenido se encuentre "publicado" en Internet, es necesaria la intervención de otras personas. Podríamos esquematizarlo de la siguiente manera:

1. Autor intelectual del contenido de la página
2. Autor material de la página (diagramador web)
3. Servidor en cuyo sistema informático se encuentra alojada la página web.
4. Internet Service Provider (ISP) quien transmite la información a la red.
5. Internet Access Provider (IAP) quien provee el acceso a Internet.
6. Network Provider (NSP) proveedor de red.

Qué responsabilidad civil o penal tienen estas personas que han intervenido de alguna forma para que el acto antijurídico se halla llevado a cabo? ¿El Servidor, el ISP y el NSP, son responsables de la acción antijurídica? ¿Es equiparable la figura del ISP a la del editor de un medio de prensa? En caso de considerárselos responsables, ¿se les debe imputar una responsabilidad objetiva o subjetiva? En otras palabras: ¿podemos considerarlos responsables por el sólo hecho de permitir que la página mediante la cual se comete la acción antijurídica sea transmitida o debe existir culpa o dolo por parte del ISP?. Este problema ya ha sido planteado tanto en el common law **(14)** [\[xiv\]](#) como en el marco de la Unión Europea **(15)** [\[xv\]](#) no existiendo a la fecha criterios uniformes respecto de la atribución de responsabilidad a los ISP.

Algunos gobiernos, como el alemán y el británico han intentado inconsistentemente responsabilizar

a los proveedores de acceso a Internet de los contenidos que circulan por sus ordenadores. Los defensores de la corriente contraria oponen que los Proveedores de acceso son simples transportadores de bits y por tanto responsabilizar a un IAP por el contenido ilegal de una comunicación que circula por sus ordenadores, es tanto como acusar al cartero o a la oficina de correos del carácter delictivo de una carta de un usuario de ese servicio postal

Pero si bien la responsabilidad de los que únicamente proveen acceso a Internet sería cuestionable, no lo es tanto con relación a los Servidores que alojan páginas web . Ya que un ISP podría decidir no admitir en su servidor páginas con determinados contenidos. Respecto de este tema la comunicación citada del Libro Verde establece que "La responsabilidad de un usuario que carga material ilícito en la red y la liberación de responsabilidad de los operadores que simplemente transportan datos por la red parecen claramente aceptadas. Pero la cuestión de la responsabilidad de los estadios intermedios (en especial donde se almacena el material, incluso temporalmente, en formato legible) no está claramente establecida. La cuestión es averiguar lo que es técnicamente factible y económicamente viable y observar un equilibrio entre la protección de la libertad de expresión y de la privacidad, por un lado, y la protección de los menores y de la dignidad humana por otro."

Por su lado la Comunicación sobre contenidos ilegales ut supra mencionada pone el acento en la responsabilidad de los autores del contenido y secundariamente en los proveedores de los mismos, advirtiendo que un régimen restrictivo, que exija a los proveedores de acceso que restrinjan sitios que contengan contenidos ilegales sería inconcebible en Europa, pues interferiría severamente con la libertad del individuo.

Nuestro sistema de responsabilidad se basa en principio en la imputación subjetiva de la misma a causa de culpa o dolo, y excepcionalmente y en los casos previstos por la ley se imputa responsabilidad objetiva. No existen normas que contemplen específicamente este tipo de conflictos, obligando a los jueces a realizar la aplicación analógica de principios generales que puede llevar a una jurisprudencia contradictoria y crear un desconcierto general, lo cual redundaría en un entorpecimiento del desarrollo de la red. Así algunos fallos podrían excluir todo tipo de responsabilidad a los proveedores y servidores de Internet, poniendo la culpa solo sobre el autor de los contenidos, o bien podrían imputar responsabilidades mediante asimilaciones a los editores de los medios de prensa o a las emisoras de radiodifusión(16)[xvi]

Un reciente caso resuelto por la Corte Suprema(17)[xvii] expone el tema de las responsabilidades en los medios de comunicación, específicamente referido a la responsabilidad de la licenciataria del servicio de televisión por los daños ocasionados a través de un programa emitido por canal 13. La cámara Nacional de Apelaciones en lo Civil, sala L había resuelto que Artear S.A. tenía el deber de reparar, fundando dicha imposición en el art. 1113 del código civil, o sea que extendía la responsabilidad objetiva para la licenciataria, sosteniendo por un lado que el deber de resarcir de la emisora se sustentaba en el carácter riesgoso de la actividad desplegada por el medio, pero por otro lado afirmó que los medios de comunicación debían extremar los recaudos para ejercer regularmente sus derechos sin agraviar a terceros a raíz de los abusos producidos mediante su ejercicio. Este último fundamento derivaría de la atribución de culpa a la emisora. La cámara afirmó que en virtud de la situación especial en que se producían determinados daños se presumía la culpa de ciertas personas a quienes se indicaba como responsables, permitiéndoles exonerarse si demuestran que obraron con una diligencia normal. Esta conclusión es incompatible con el régimen de responsabilidad objetiva invocado por la misma sentenciante.

La Corte confirmó la sentencia apelada, aunque por distintos fundamentos y con tres votos en disidencia. La sentencia de la Corte afirma que "las responsabilidades ulteriores previstas en el texto constitucional - necesarias para asegurar la integridad de los derechos personalísimos comprometidos - se hacen efectivas mediante el régimen general vigente en nuestra ley común, que tiene su fuente sea en la comisión de un delito penal o un acto ilícito civil (art 114 cod. Penal, arts 1071 bis , 1072, 1089 y 1109 cód. Civil). En el específico campo resarcitorio, se trata pues de una responsabilidad subjetiva por lo cual, en virtud de los principios que rigen la materia, no es dable presumir la culpa o el dolo del autor del daño, y quien alega estos únicos factores de imputación debe demostrar su concurrencia"... La Corte hace mención a fallos anteriores en los cuales ha resuelto que no existe en el ordenamiento legal de nuestro país un sistema excepcional de responsabilidad objetiva para aplicar a la actividad supuestamente riesgosa de la prensa, que, por el contrario, es imprescindible probar aún el factor de imputabilidad subjetivo - sea la culpa o el dolo - de la persona u órgano que dio la noticia o publicó la crónica. Finalmente imputa responsabilidad a la licenciataria del servicio por culpa, por haber infringido el deber de contralor que le compete a fin de evitar que las emisiones difundidas por su frecuencia perturben la intimidad de las personas o comprometan su buen nombre y honor.

Los Doctores Belluscio y Bossert, en su voto en disidencia, refuerzan la declaración de que nuestro ordenamiento legal no contempla un sistema excepcional de responsabilidad objetiva para aplicar a la actividad de la prensa y de otros medios de comunicación masiva.

La actual ley de radiodifusión imputa responsabilidad a los titulares de los servicios de radiodifusión por el contenido y desarrollo de las transmisiones, pero por la redacción del artículo y su ubicación en el texto de la ley, parecería que sólo se refiere a la esfera penal y sancionatoria(18)[xviii] frente a la autoridad de aplicación .

El anteproyecto de reforma de la ley de radiodifusión contiene una cláusula de responsabilidad más amplia para las licenciatarias, que incluye su responsabilidad civil frente a terceros por el contenido de los programas o emisiones que realicen, creando de esta forma un sistema de responsabilidad objetiva para las mismas(19)[xix].

De lo expuesto surge que aún dentro del plano de las responsabilidades por daños ocasionados por los medios de comunicación tradicionales, no existe en nuestro ordenamiento una normativa precisa, en consecuencia la dilucidación de este tema en el campo de Internet trae aparejado un desconcierto mucho mayor. Sin adentrarme en el análisis de cual sería la postura más adecuada para determinar el tipo y grado de responsabilidad de los servidores de Internet, considero que es indispensable legislar sobre este punto, para evitar que la carencia de normas produzca inseguridad tanto en los ISP como en los particulares damnificados.

IV.- LA PRIVACIDAD: EL DERECHO A LA INTIMIDAD Y SU EJERCICIO EN LA RED.

1.- Encuadre conceptual y normativo.

La intimidad, como manifestación de los derechos personalísimos, protege al individuo en su integridad espiritual, constituyendo una materia sobre la cual convergen diferentes valoraciones la proyección personal en su sustancia incorpórea. El derecho a la intimidad es también conocido como derecho a la privacidad, o a la vida privada, derecho sobre la propia esfera individual

Este derecho es de raigambre constitucional, reconocido en el Pacto de San José de Costa Rica en su artículo 11 que dispone "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia.... toda persona tiene derecho a la protección de la ley contra esas injerencias". Similar texto se incluye en el artículo 12 de la Declaración Universal de los Derechos Humanos.

El artículo 1071 bis del código Civil regula este derecho al establecer que "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, modificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias..."

Al igual que la libertad de expresión, no se trata de un derecho absoluto, y en muchas ocasiones su ejercicio choca con otras garantías como la misma libertad y con la seguridad.

2.- Particularidades de su ejercicio en Internet.

El derecho a la privacidad comprende muchos aspectos diferenciados dentro de la red. Desde la posibilidad de cifrar los mensajes que se transmiten por correo electrónico utilizando la criptografía, el derecho al anonimato en la red, derecho de acceder a un correo electrónico anónimo (remail), derecho de no recibir correo no solicitado (spam).

La CRIPTOLOGIA(20) [xx] permite garantizar de forma eficaz la protección de la información y de las comunicaciones que se transmiten por las redes informatizadas. Se podría decir jurídicamente es una medida de prevención con múltiples aplicaciones basada en una tecnología que tiene la consideración legal de *tecnología de doble uso*. Su empleo provoca dificultades en la investigación, persecución y prevención de actos delictivos en general, por tal motivo surge la regulación legal de la Criptología. En algunos países se prohíbe el uso de la misma, mientras que en otros se establece la obligación legal de dar a conocer a los organismos gubernamentales las claves privadas y algoritmos utilizados. El fundamento es evitar el traspaso de información secreta por narcotraficantes y terroristas en la red.

Un caso concreto de regulación de la criptología lo constituye la ley 11/1998 General de Telecomunicaciones española, que introduce una normativa que afecta al uso del cifrado. El citado cuerpo legal contiene entre sus disposiciones las condiciones de uso de la criptología, disponiendo que el cifrado es un instrumento de seguridad de la información. Establece la obligación de notificar a un organismo público los algoritmos o cualquier procedimiento de cifrado utilizado, a efectos de su control. Esta obligación afecta a los fabricantes que incorporen el cifrado a sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo emplean.

El fundamento que lleva a regular sobre criptología es la tensión que existe en ciertos casos entre el ejercicio del derecho de privacidad y la seguridad y prevención del delito. Así las organizaciones gubernamentales, tanto a nivel nacional como internacional, limitan legalmente su ejercicio apoyados en el principio de que si se busca evitar el crimen hay que ceder parte del derecho a la intimidad.

Existen incluso redes de espionaje internacional como ECHELON que violan el derecho de privacidad en la red y se encuentran sustentadas por el plus valor del principio de seguridad.

En Abril del 2000 se publicó el borrador del Convenio de la Unión Europea sobre "Crimen en el Ciberespacio" (21) [xxi] donde se hace referencia al crimen en la red y a la necesidad de cooperación internacional, pero no se hace mención alguna a los derechos de los individuos, a la intimidad, privacidad y protección de datos. Este proyecto de convenio ha suscitado innumerables críticas desde todos los foros de protección de los ciberderechos, ya que su aplicación haría desaparecer los correos

anónimos, los poseedores de contraseñas deberían darlas a conocer, los ISP tendrían la obligación de dar todos los datos personales de los usuarios, etc.

Pero no sólo los Estados Nacionales u organismos internacionales coartan el derecho de privacidad sino también algunas empresas privadas. Un caso reciente de invasión de la privacidad en Internet es el de BLIZZARD ENTERTAINMENT que posee un web site donde se puede jugar contra otras personas sin necesidad de dejar los datos del jugador. Este empresa lanzó al mercado un nuevo juego llamado STARCRAFT en un CD que para hacerlo interactivo debía conectarse a la red en el web site de la empresa . Esta había instalado dentro del programa del juego una rutina que permitía averiguar el e mail y el nombre de los participantes. Durante 7 días la compañía reunió la información de todos los jugadores que se conectaban con el servicio, sin siquiera informar a los participantes que lo estaba haciendo. El motivo aducido a posteriori para justificar el programa espía era el de facilitar la solución problemas de conexión por parte de los usuarios y detectar las copias piratas. La empresa alega haber destruido todos los archivos luego de solucionado el problema de acceso de los participantes, pero el abogado Donald P Driscoll inició una demanda en San Francisco para evitar futuros abusos por parte de la empresa, violatorios de la privacidad.

Si esto hubiera sucedido en la Argentina la acción judicial no hubiera tenido sustento jurídico, ya que este tipo de actividades no constituyen delito. Tampoco podrían dar lugar a una acción por responsabilidad civil, ya que habría que probar los daños sufridos y esto es muy difícil ya que probablemente el único perjuicio es la intromisión indebida en la vida privada de una persona sin su autorización.

Como vemos también el derecho de privacidad o intimidad tiene un perfil muy particular en la red y carece en muchos casos de apoyo normativo.

Muy relacionado con el derecho a la intimidad se encuentra el *derecho a la autodeterminación informativa* que consiste en la facultad que tiene todo individuo de saber quien, cuando y con que motivo sabe algo sobre él. Es el derecho a la protección de los datos personales del individuo.

La publicidad comercial ha variado con el transcurso de los años, hoy día se estila la venta one by one, que es una técnica refinada de propaganda que requiere como presupuesto conocer los gustos, aficiones, ganancias, estado civil, etc de los posibles consumidores, a los que se define como "clientes diferenciados". Surgen entonces las bases de datos para marketing, que antes se almacenaban mecánicamente, luego electrónicamente y ahora telemáticamente. Es esta última etapa el problema se agrava ya que la capacidad de registro de las computadoras, la rapidez de consulta y de transferencia de datos genera para quien posee dicha información una enorme fuente de poder.

A veces ni siquiera tenemos conciencia que estamos revelando datos, así determinadas páginas de Internet registran con nuestro paso cuales son las paginas que hemos visitado, que tipo de sistemas operativos estamos utilizando y quien es nuestro servidor y hasta cual es nuestro correo electrónico (mediante un link oculto en la pagina, que con solo ser tocado con el mouse provoca que nuestra PC envíe automáticamente un mail a la dirección predeterminada por la página)(22) [xxii]

Uno de los remedios procesales más recientes destinado a la defensa de este derecho es el HABEAS DATA que permite que cada persona pueda solicitar la actualización, rectificación, confidencialidad y supresión de los datos personales que se encuentran en poder de terceros.

Nuestra constitución recepta este instituto con la reforma de 1994 en el artículo 43, en la sección correspondiente a Nuevos Derechos y Garantías. Esta facultad ha sido reglamentado por ley 25.326 .

Tampoco este derecho es absoluto, ya que el individuo tiene que aceptar determinadas limitaciones de su derecho a la autonomía informativa en aras del interés preponderante de la comunidad. Dichas restricciones deben surgir de leyes que respeten las garantías de claridad normativa, proporcionalidad en la restricción, adecuación de los medios a la finalidad y garantías organizativas.

3.- Ataques contra el derecho a la intimidad.

La tecnología de Internet posibilita que el derecho a la intimidad sea lesionado fácilmente. La legalidad de las cookies(23) [xxiii] podría ser cuestionada, ya que la información que reúnen de nuestras computadoras es revelada a la web visitada, otorgando a sus administradores datos tales como el historial de los sitios visitados, el número de transacciones realizadas en la web, los anuncios que el usuario ha visto, etc. Esta forma de producir información, sin que el usuario dé su autorización y ni siquiera haya tomado conocimiento, puede convertirse en una violación a los derechos de privacidad y de la autodeterminación informativa.

Otro ataque al derecho a la intimidad en Internet lo constituyen los ataques contra la privacidad e integridad de los datos que circulan por las redes. Uno de ellos es el "sniffing", que implica "husmear en la red", donde un ordenador diferente al de destino del mensaje lee los datos de la red. Otro peligro más grave aún se produce por la introducción de "Trojanos" o "Caballos de Troya", que son programas diseñados para obtener información del ordenador donde son ejecutados. Existen trojanos que únicamente consiguen contraseñas, otros que gravan secuencias y otros más peligrosos que abren puertas traseras al ordenador. (24) [xxiv]

No encontramos en nuestro ordenamiento jurídico una tipificación penal de los delitos informáticos,

motivo por el cual sólo son penalmente reprochables aquellas conductas realizadas mediante Internet que encuadren en alguno de los tipos penales ya existentes. Mientras el hacker o atacante se limite exclusivamente a mirar nuestros datos, y nuestras comunicaciones, no comete delito alguno. Para ejemplificar citaré brevemente un fallo judicial reciente: Un particular intentó ingresar al centro de cómputos de una Universidad Nacional valiéndose de una conexión vía Internet y cuyo servidor no se encuentra disponible al acceso del público en general por estar protegido por una clave de ingreso. El director del centro de cómputos formuló la denuncia penal a raíz de la cual se investigó el hecho determinándose fehacientemente la computadora desde la cual partió el ataque y el autor del mismo.

El Tribunal (Juez Federal de Primera Instancia, Río Cuarto 26/4/99 Denuncia formulada por UNRC) desestimó la denuncia concluyendo que el hecho investigado no constituye delito penal.

En consecuencia, si bien nuestro ordenamiento penal protege la privacidad de las personas, el domicilio y el secreto de las comunicaciones. en ninguna parte incluye como bien jurídico protegido a los datos o registros obrantes en computadoras u otro tipo de soportes. No tipifica ninguna acción en la cual se puedan encuadrar los accesos ilegales a sistemas de redes, y por el principio de tipicidad y especialidad del derecho penal los jueces no pueden condenar por aplicación analógica, si no existe el tipo penal adecuado. La necesidad de una legislación penal sobre los delitos informáticos se hace evidente.

V.- CONCLUSIONES

No es la intención de este trabajo confeccionar un listado completo de los temas relacionados con Internet que necesitan de una regulación específica, pero del breve análisis desarrollado en estas páginas surge como evidente la necesidad de regular algunos aspectos esenciales.

Se ha sostenido que por el carácter descentralizado y global de la red de redes, por la falta de límite en su alcance geográfico de las comunicaciones digitales y por carecer en su estructura organizativa de una autoridad central única, la regulación de Internet sería imposible. Pero es menester hacer una reflexión respecto de este punto, "todos los rasgos distintivos y únicos de Internet no son algo completamente inherente al medio técnico telemático, son obra humana. No conforman una naturaleza intrínseca e inalterable de las comunicaciones informáticas en red, sino que derivan de un diseño consciente y voluntario - aunque no planificado por una estructura central de mando - de la arquitectura del ciberespacio actual. La tecnología informática y digital hace posible este carácter único y revolucionario de Internet, pero es el quehacer de las personas que han desarrollado la red lo que ha determinado su actual estructura. Esta no es inmutable ni inevitable. De alguna forma podemos decir que forma parte del secular esfuerzo del ser humano por ampliar la esfera de su autonomía y libertad frente al medio natural y a los poderes e instituciones sociales"⁽²⁵⁾[xxv].

Es decir que la red es una obra humana y una realidad social, y como toda realidad social es regulable. Los derechos sólo pueden protegerse mediante la ley.

(1) Activista norteamericano fundador de la Electronic Frontier Foundation.

(2) Término proveniente de la novela de ciencia ficción de William Gibson "Neuromante".

(3) Art. 1197 Código Civil.

(4) En Argentina durante 1999 se realizaron dos huelgas de internautas.

(5) Declaración Universal de los Derechos Humanos (1948) art. 18 y art. 19. Pacto Internacional de Derechos Civiles y Políticos (1966) art 19. Convenio Europeo para la protección de los Derechos Humanos y de las libertades fundamentales (1950) art 10.1. Convención Americana sobre Derechos Humanos art. 13 inc 1 y 2.

(6) Efecto explicado por John Gilmore en la conferencia ante el foro de Computers, Freedom and Privacy.

(7) LORTAD. Ley orgánica sobre el tratamiento automatizado de datos personales.

(8) CS, setiembre 29-998.- Cencela, Omar J. C. Artear SA y otros. Doctrina Judicial La Ley 1988-3 pag 1019.

(9) Libro Verde sobre la protección de los Menores y la Dignidad Humana en los servicios audiovisuales y la Comunicación sobre contenido ilegal y perjudicial en Internet, aprobados por la Comisión Europea en octubre de 1996.

(10) A este tema nos hemos referido con anterioridad. En nuestro país la protección de los datos personales tiene raigambre constitucional - art . 43 párrafo 3° de la CN- y esta regulada por la ley 25.326.

(11) Art. 113. Código Penal " El que publicare o reprodujere, por cualquier medio, injurias o calumnias

inferidas por otro, será reprimido como autor de las injurias o calumnias de que se trate." Art. 114.Cód. Penal " Cuando la injuria o calumnia se hubiere propagado por medio de la prensa, en la Capital y territorios nacionales, sus autores quedarán sometidos a las sanciones del presente Código y el juez o tribunal ordenará, si lo pidiere el ofendido, que los editores inserten en los respectivos impresos o periódicos, a costa del culpable, la sentencia o satisfacción."

(12) art 128. Código Penal. "Será reprimido con prisión de seis meses a cuatro años el que produjere o publicare imágenes pornográficas en que se exhibieran menores de dieciocho años, al igual que el que organizare espectáculos en vivo con escenas pornográficas en que participaren dichos menores.

En la misma pena incurrirá el que distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de menores de dieciocho años de edad al momento de la creación de la imagen. "

(13)Art 128 C.P. in fine. "Será reprimido con prisión de un mes a tres años quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

(14)En el caso PlayBoycFrena el editor de un BBS fue hallado responsable por direct infringement (responsabilidad objetiva que no requiere beneficio o enriquecimiento del infractor) al derecho de autor de Play boy a pesar de la posibilidad de no estar enterado de ello. En Sega c Maphia el tribunal condenó al demandado por contributory infringement sugiriendo que es la persona que pone el material en infracción en el servidor quien es responsable por direct infringement (el contributory infringement requiere el conocimiento de la infracción y la inducción, causación o contribución material del infractor).En RCT v Netcom se desestimó el reclamo porque no se acreditó que el demandado Netcom recibía un beneficio directo de la infracción, porque el percibía una cuota fija de interconexión (vicarius liability, el demandado debe tener la posibilidad de controlar el acto del infractor y recibir un beneficio financiero directo de la misma)

(15)En Alemania la fiscalía general del estado de Baviera acusó a Compuserve, en abril de 1997 de distribución de pornografía infantil y transmisión de un juego informático que incluía fotografías de Hitler y símbolos nazis, cuya exposición publica es ilegal en Alemania. El director local de Compuserve fue arrestado bajo cargos penales.

(16)El artículo 80 de la ley 22.285 de radiodifusión establece que "los titulares de los servicios de radiodifusión y los actuantes serán responsables por el contenido de las transmisiones y estarán sujetos a las sanciones que establece dicha ley sin perjuicio de las que pudieran corresponder por la aplicación de la legislación penal...".

(17)CS, septiembre 29-998. Cancela, Omar J. C/Artear S.A. y otros.

(18)Artículo 80 de la ley 22.285, bajo el título Régimen sancionatorio

(19)El Artículo 31 del anteproyecto establece "Los titulares de los servicios de radiodifusión y los productores de los respectivos programas serán conjunta y solidariamente responsables ante la autoridad de aplicación y en su responsabilidad civil ante terceros por el contenido de los programas y emisiones que realicen. Ningún emisor podrá invocar, como eximente de su responsabilidad administrativa, que la autoría de las emisiones que realice pertenece a terceros."

(20)Mecanismo que permite que mediante el uso de algoritmos matemáticos se transformen (encripten) datos inteligibles en datos no inteligibles, para luego de la transmisión descryptarlos utilizando el mismo u otro algoritmo

(21)Texto del borrador de la Convención en <http://conventions.coe.int/treaty/en/projects/cybercrime.htm>.

(22)El sitio Criptonomicon nos ofrece una prueba en tal sentido.www.ies.csic.criptonomicon.com

(23)Las cookies son ficheros de datos guardados en un directorio específico del ordenador del usuario. Se crean por los servidores web con el objeto de ser enviados a los programas navegadores del usuario, y así recoger la información que dicho fichero ha reunido.

(24)Los troyanos más conocidos son el Back Orifice y el NetBus que abren una puerta trasera a un equipo basado en Windows permitiendo que el hacker que lo introdujo obtenga el control total de la máquina del usuario.

(25)Extraído del documento "La libertad de expresión en Internet: Retos y amenazas. Javier Villate. Documento de trabajo de Fronteras Electrónicas (FrEE) junio 1998.