

IMPACTOS SOCIALES Y JURÍDICOS DE INTERNET

Antonio-Enrique Pérez Luño. Universidad de Sevilla.

Resumen: 1. Internet: nueva frontera de la información y la comunicación. 2. Problemas y riesgos jurídicos de Internet. 3. Sistemas de seguridad en Internet. 4. El ciberespacio: ¿anarquía libertaria o libertad garantizada?. 5. Algunas respuestas jurídicas. 6. Iniciativas de la Unión Europea. 7. Hacia una ética jurídica ciberespacial. 8. Bibliografía.

Abstract: 1. Internet: the new frontier of the information and the communication. 2. Problems and legal risks of Internet. 3. Safety systems in Internet. 4. The cyberspace: libertarian anarchy or guaranteed freedom?. 5. Some legal answers. 6. Initiatives of the European Union. 7. Towards a legal ethics of cyberspace. 8. Bibliography.

1. Internet: nueva frontera de la información y la comunicación.

No parece lícito dudar que Internet (*International Network of Computers*) está siendo el fenómeno estelar de las Nuevas Tecnologías de la información y la comunicación en la década de los noventa. En el umbral de un nuevo milenio Internet se presenta como un paso decisivo en el avance de los sistemas de información y comunicación a escala planetaria. Gracias a Internet cada ciudadano, sin moverse de su casa, puede acceder a los centros de documentación más importantes del mundo, puede realizar las más diversas operaciones financieras y comerciales, gozar de una enorme oferta de entretenimientos de la más diversa especie, y se puede comunicar con otros usuarios de la red sin limitaciones de número ni distancia. Si hace algunos años parecía que la "aldea global" era el gran reto del futuro, hoy Internet ha convertido en realidad presente el "hogar global", en la medida en que cada domicilio de los usuarios de la red constituye la terminal de un sistema integrado universal.

Conviene no resbalar, por su importancia, en la extensión presente y perspectivas futuras -se dice que cada dos minutos se incorpora un nuevo usuario a la red- de este amplísimo vehículo de información e intercomunicación. Internet es una red de redes que conecta más de dos millones de ordenadores pertenecientes a instituciones académicas, entes públicos y empresas privadas. Se calcula que en la actualidad la emplean más de cuarenta millones de usuarios, cifra que aumenta en un diez por ciento cada mes. La explosión de su crecimiento se ha debido principalmente a la difusión del parque de ordenadores personales equipados con módem y con posibilidades de conectarse a la red telefónica. Con la aparición de herramientas de uso de la red accesibles a todos se ha multiplicado el número de usuarios no especialistas en informática, frente al carácter privativo para los expertos que Internet tuvo en sus inicios (cfr. Colom y Van Bolhuis, 1995; Moreno, 1995; Rico, 1995).

El ciberespacio es un microcosmos digital en el que no existen fronteras, distancias ni autoridad centralizada. Su conquista se ha convertido en meta obligada para quién desee sentirse miembro de la sociedad informática y es en la actualidad uno de los puntos de encuentro para el ocio y el negocio, que cuenta con mayores perspectivas de futuro (Rico, 1995).

2. Problemas y riesgos jurídicos de Internet.

No obstante, junto con esas incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permite la navegación por el ciberespacio, Internet ha hecho surgir en los últimos tiempos graves motivos de inquietud. El escándalo que meses pasados agitó a la opinión pública europea, en relación con el tráfico de imágenes de prostitución infantil a través de Internet, así como la utilización de la red para difundir propaganda de bandas terroristas, ha supuesto la confirmación de un peligro desde hace algún tiempo anticipado. Los miles de ciudadanos europeos, inmediata o potencialmente, agredidos por esas imágenes criminales, abren una brecha en la inconsciencia cívica y política sobre los peligros que entrañan determinadas manipulaciones de las

nuevas tecnologías. Ha sido preciso llegar a esta situación para que el conformismo cotidiano de quienes tienen como misión velar por la tutela de las libertades, y quienes tienen como principal tarea cívica el ejercerlas, se viese agitado por la gravedad del riesgo y la urgencia que reviste su respuesta.

No es admisible, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías. Desde hace tres décadas, quienes han evaluado el impacto de la informática en las libertades, han alertado sobre esos peligros, y cualquier especialista mínimamente avisado incurriría en negligencia inexcusable de haberlos desatendido. En las sociedades avanzadas con tecnología punta ya no se puede juzgar como una amenaza remota las advertencias y experiencias de asalto informático a las libertades, que con el descubrimiento de los abusos perpetrados a través de Internet se han convertido en una siniestra realidad (Branscomb, 1995; Cavazos y Morin, 1994).

Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión de sabotajes, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolable de *piratas informáticos*. Las "autopistas de la información" entrañan también un grave riesgo para la protección de los programas. Asimismo, la facilidad de intercambiar informaciones a distancia puede generar importantes peligros para la protección de los datos personales.

Internet implica, por tanto, el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos (Bensoussan, 1996; Iteanu, 1996; Ribas, 1996). Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra cuatro tipos de bienes jurídicos básicos:

- 1) *La intimidad, la imagen, la dignidad y el honor de las personas* (bienes que son tutelados en los artículos 197 ss. y 205 ss. del Código Penal español de 1995), al posibilitar la intromisión indebida en datos personales, su transmisión no autorizada, el acoso informático, la propagación universal de difamaciones, calumnias e injurias, la incitación al odio o la discriminación raciales...
- 2) *La libertad sexual* al permitir la propagación de imágenes o informaciones que entrañen formas de exhibicionismo, provocación sexual o fomenten la pornografía entre menores de edad (actividades penadas en los arts. 185, 186 y 189 del nuevo Código Penal español).
- 3) *La propiedad intelectual e industrial, el mercado y los consumidores* (bienes protegidos en los arts. 270 ss. del Código Penal español), ya que Internet puede contribuir a la distribución ilícita de obras registradas como propiedad intelectual o industrial, a la piratería de programas, así como a la difusión de contenidos publicitarios ilegítimos.
- 4) *La seguridad nacional y el orden público* (garantizados por los arts. 544 ss. del Código Penal), en cuanto que pueden contribuir a facilitar atentados y desórdenes públicos, e incluso actividades terroristas.

El carácter internacional e ilimitado de esas conductas hacen más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente. Existe una evidente dificultad para determinar la responsabilidad jurídica en un medio, como el de Internet, en el que existen diferentes operadores que concurren en la cadena de comunicaciones: el proveedor de la red, el proveedor de acceso, el proveedor de servicio y el proveedor de contenidos. Este problematismo se agudiza cuando los diferentes elementos de la cadena se hallan en países distintos con legislaciones, a su vez, diferentes. En la doctrina francesa se ha aludido al fenómeno de "*délocalisation*" de Internet (Piette-Coudol y Bertrand, 1997), para hacer hincapié en los problemas jurídicos que plantea establecer el Derecho aplicable a actuaciones realizadas en una red planetaria sin "localización" geográfica precisa y determinada.

Debe también tenerse en cuenta la dificultad que entraña establecer la responsabilidad derivada de determinados contenidos ilícitos transmitidos a través de Internet. A tenor de las diferentes regulaciones legislativas nacionales se tenderá a hacer recaer dicha responsabilidad en los *creadores* de la información, en los que han facilitado su *transmisión* y *acceso* a la misma, o en los *consumidores* que la aprovechan o utilizan (Piette-Coudol y Bertrand, 1997; Stuckey, 1995).

Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, mientras que la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean a los ordenamientos jurídicos nacionales y al orden jurídico internacional.

No huelga tampoco reconocer que la impunidad de determinadas formas de criminalidad informática no siempre constituye una negligencia imputable al legislador. Porque en un sector como el de las relaciones entre la Informática y el Derecho, constantemente, cada Feria tecnológica abre nuevas proyecciones informáticas al Derecho, o innova bienes informáticos que requieren nuevos procedimientos de tutela jurídica, o da a conocer dispositivos que condenan al anacronismo los medios de protección jurídica anteriormente existentes. La criminalidad informática se caracteriza, en suma, por las dificultades que entraña *descubirla, probarla y perseguirla*. Se ha hecho célebre la imagen de que los sistemas informáticos son como "queso de Gruyere", por las enormes oquedades y lagunas que quedan siempre abiertas a posibles atentados criminales.

3. Sistemas de seguridad en Internet.

Aunque Internet puede haber contribuido a crear nuevos riesgos las técnicas informáticas ofrecen también nuevas medidas de seguridad para oponerse a los atentados contra bienes e intereses jurídicos. Entre las medidas de seguridad más difundidas y eficaces se pueden citar las siguientes:

a) *Programas de encriptación*, que permiten la conversión de mensajes en lenguaje natural en textos que utilizan un lenguaje clave y que aseguran que nadie excepto quien posea la transcripción de esas claves podrá descifrar. Ha adquirido especial celebridad el programa de encriptación debido a Philip Zimmermann denominado PGP (*Pretty Good Privacy*), que está siendo utilizado por numerosos usuarios de Internet.

Si bien estos programas de seguridad, junto a sus logros para garantizar la confidencialidad de la transmisión de informaciones lícitas, tiene su reverso en haber contribuido a dificultar el descubrimiento de redes informativas ilícitas. La DEA, servicio norteamericano antidrogas, así como otros servicios policiales, han denunciado sus dificultades para perseguir a los narcotraficantes entre los laberintos y las encriptaciones de sus mensajes electrónicos.

b) *Los filtros*, consistentes en programas informáticos selectivos que bloquean el acceso a determinados documentos pero no a otros. La Unión Europea apoya la denominada PICS (*Platform for Internet Content Selection*). Se trata de un servicio para seleccionar contenidos en Internet que lanzó oficialmente el *World Wide Web Consortium*. Estos filtros pueden programarse en un triple sentido: 1) "*Lista blanca*", dejando pasar solamente aquellos servicios o informaciones que previamente han sido registrados; 2) "*Lista negra*" bloqueando aquellos servicios o programas a los que no se desea tener acceso. Se ha hecho famosa la lista *CyberNot*; que abarca unos siete mil programas clasificados como nocivos por sus contenidos de violencia, obscenidad, racismo, cultos satánicos, drogas... Gracias a este sistema los padres pueden bloquear de forma selectiva el acceso a aquellos servicios que consideran nocivos o peligrosos para sus hijos; 3) "*Etiquetado neutro*", permitiendo construir un menú de servicios personalizados para cada usuario. Este sistema ofrece un alto grado de flexibilidad y seguridad, al facilitar que cada usuario realice personalmente la criba de aquellos contenidos de Internet que juzgue apropiados a su sensibilidad, cultura y sistema de valores.

c) *Los cortafuegos*, que operan facilitando o impidiendo la transferencia de imágenes o datos desde Internet a un ordenador o viceversa. Estos sistemas de seguridad permiten el acceso a aquellos servicios previamente establecidos, cortando la entrada o salida a los demás.

d) *Los certificados digitales*, que permiten identificar o relacionar a todas las partes que intervienen en transacciones comerciales realizadas a través de Internet, dotándolas de la máxima rapidez y seguridad. Así, por ejemplo, el sistema *SET (Secure Electronic Transaction)*.

e) *Los Ciberpolicías*, se trata de entidades, como por ejemplo *FIRST (Forum of Incident Response and Security Teams)* y *CERT (Computer Emergency Response Team)*, las cuales ofrecen equipos de expertos en la localización de piratas informáticos, y suministran programas de defensa frente a sabotajes y proporcionan ayuda en caso de siniestros informáticos. Algunas policías de países técnicamente desarrollados han organizado unidades especiales en la investigación de actividades criminales realizadas a través de Internet. En España existe un Grupo de Delitos Informáticos perteneciente a la Unidad Central de Policía Judicial.

Estos sistemas de seguridad representan un principio de esperanza frente a los riesgos y peligros que, sin resquicio a dudas, comportan las actividades abusivas o ilícitas realizadas a través de Internet. Su eficacia es diversa y, todavía, difícilmente evaluable, pero esos sistemas demuestran frente a pesimistas y escépticos que Internet no es un paraíso para el ejercicio de la delincuencia, ni un espacio inexorablemente condenado a la zozobra y la inseguridad (Bensoussan, 1996; Bustos, 1996; Ribas, 1996).

4. El ciberespacio: ¿anarquía libertaria o libertad garantizada?.

Como la mayoría de las grandes conquistas científicas y tecnológicas que registra la historia, Internet es una realidad ambivalente. Renunciar a sus logros sería hoy una pretensión imposible, porque se trata de un avance irrenunciable y un signo del progreso de nuestro tiempo. Pero ello no debe conducir a aceptar pasivamente o a claudicar ante los riesgos de "*abordaje*" criminal que amenazan la navegación por el ciberespacio.

Como he indicado, en sus inicios, uno de las mayores alicientes de Internet residía en su carácter *ácrata*; se trataba de un espacio absolutamente libre, sin ningún tipo de autoridad o poder que lo regulara o acotara. Como elocuente ejemplo de esa concepción anárquica y libertaria de Internet puede citarse la *Declaración de Independencia del Ciberespacio* "promulgada" por John Perry Barlow en Davos, Suiza, el 8 de Febrero de 1996. Dicha Declaración ha adquirido notable celebridad en estos meses entre los usuarios de Internet. Consiste en un texto que, en mi opinión, se articula en torno a tres ideas-guía:

1ª) La afirmación de la total *autonomía* de los cibernautas respecto a cualquier tipo de autoridad estatal: "Gobiernos del Mundo Industrial...No son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos juntamos...El Ciberespacio está fuera de sus fronteras".

2ª) Negación de los *conceptos y categorías jurídicas tradicionales*: "Vuestros conceptos legales de propiedad, expresión, identidad, movimiento y contenido no se aplican a nosotros. Aquellos se basan en la materia, pero en nuestro mundo la materia no existe".

3ª) Confianza *utópica* en un ciberespacio ideal: "Crearemos una civilización de la Mente en el Ciberespacio. Que sea más humana y justa que el mundo creado anteriormente por sus gobiernos".

Como contrapunto a esa visión idílica de Internet señala el profesor de Teoría de la Comunicación en la Universidad París-VII y Director de *Le Monde Diplomatique*, Ignacio Ramonet, que el ciberespacio está siendo colonizado despiadadamente por todos los gigantes de las telecomunicaciones. Internet está creando nuevas formas de desigualdad entre "inforricos" e

"infopobres", al establecer discriminaciones graves en el acceso y utilización de informaciones entre el Norte y el Sur, donde la falta de equipos va a condenar a la marginación a millones de personas. Recuerda, por ejemplo, que hay más líneas telefónicas sólo en la isla de Manhattan (Nueva York), que en toda África negra, y sin esas líneas no se puede acceder a Internet. Según Ramonet resulta ingenuo pensar que necesariamente el aumento de comunicación debe traducirse en mayor equilibrio y armonía social. La comunicación, en sí, no es progreso social "y mucho menos cuando la controla, como es el caso de Internet, las grandes firmas comerciales y cuando, por otra parte, contribuye a acrecentar las diferencias y desigualdades entre ciudadanos de un mismo país, y habitantes de un mismo planeta. Internet -concluye Ramonet- era una esperanza; nos la han robado"(1997; vid. también, Fernández Calvo, 1996).

Internet ha abierto nuevas y preocupantes posibilidades operativas a los sistemas de control social y político. Se ha hecho célebre una imagen expuesta por Philip Zimmermann en su informe ante el Subcomité de Política Económica, Comercio y Medio Ambiente del Congreso Norteamericano. Indicaba allí Zimmermann que en el pasado cuando el Estado pretendía violar la intimidad de los ciudadanos debía esforzarse en interceptar, abrir al vapor y leer el correo, o escuchar, grabar y transcribir conversaciones telefónicas. Eso era como pescar con caña, de pieza en pieza. Por el contrario, los mensajes del correo electrónico son más fáciles de interceptar y se pueden scanear a gran escala, y ordenar en función de palabras claves. Esto es como pescar con red; y supone una diferencia orwelliana cuantitativa y cualitativa para la garantía de la democracia.

El utopismo ácrata se opone a cualquier regulación del Ciberespacio por entender que con ello se reprime la libertad de los cibernautas, a la vez, que se refuerza el poder estatal. Pero la realidad no es tan simple. Paradójicamente los grandes beneficiarios de la anarquía de Internet no son los cibernautas particulares, sino las grandes multinacionales e, incluso los aparatos de control social de los gobiernos. No huelga advertir que, en los últimos meses, se están transmitiendo por Internet, sin ningún tipo de garantías y con evidente menoscabo del derecho a la intimidad, datos personales (incluso voz e imagen) en investigaciones policiales; a través de un medio que por su naturaleza y características es accesible a millones de usuarios de todo el mundo. Tampoco está de más, recordar que algunos Colegios de Abogados norteamericanos han denunciado las prácticas de determinadas oficinas fiscales tendentes a interceptar las comunicaciones por Internet entre distintos bufetes de sus colegiados, especialmente en casos referentes a narcotráfico (Cavazos y Morin, 1994).

Los peligros de una utilización abusiva, incontrolada o criminal de ese espacio plantean ahora, de forma apremiante, la necesidad de su ordenación. Han sostenido historiadores muy autorizados que la historia es cíclica y retorna siempre; quizás por ello los actuales debates sobre Internet recuerdan a aquellos mantenidos hace siglos por los filósofos contractualistas en relación con el estado naturaleza. En la tradición contractualista se explica el origen de las instituciones políticas y jurídicas a partir de la exigencia -empírica o racional, utilitaria o ética, a tenor de las diversas interpretaciones del estado de naturaleza y el pacto social- de abandonar una situación (el estado de naturaleza) en la que el hombre posee una ilimitada (aunque insegura) libertad, a otra de libertad limitada pero protegida y garantizada por la autoridad y las leyes (Pérez Luño, 1997).

5. Algunas respuestas jurídicas.

Una vez perdida la inocencia del idílico "estado de naturaleza" de libertad sin restricciones de

Internet, las circunstancias aconsejan remediar los peligros del desorden mediante soluciones jurídicas. Esa necesidad de apelar al Derecho para poner coto a los abusos perpetrados desde Internet ha llevado a algunos juristas a invocar en art.301 del nuevo Código Penal español, que pena a quien "convierta o transmita bienes, sabiendo que éstos tienen su origen en un delito grave...". Cabría asimismo aducir que, en la medida en que Internet es hoy, entre otras muchas cosas, un espacio lúdico utilizado para su esparcimiento de forma habitual por un creciente número de niños, sería posible incriminar, al amparo del art. 186 del Código Penal español, a quien "por cualquier medio directo, difundiere, vendiere o exhibiere material pornográfico entre menores de edad o incapaces...".

Pero el recurso a esas normas suscita la inquietud de si se está escanciando el vino nuevo de las más recientes formas de criminalidad informática en los odres viejos de tipos penales pensados para castigar conductas delictivas ajenas al universo tecnológico. Porque a diferencia de los más graves atentados informáticos contra la intimidad, la utilización ilícita de tarjetas electromagnéticas y la estafa o fraude informáticos, que se hallan expresamente previstos en el nuevo Código Penal español (en los arts. 197, 239 y 248.2, respectivamente), parece evidente que nuestro legislador penal no pensaba en Internet al tipificar el delito de receptación o de exhibicionismo y provocación sexual. Por ello, la aplicación de estos tipos puede suscitar serias dudas en orden al respeto del principio de legalidad penal, pero no hacerlo puede provocar situaciones de profunda alarma en la sociedad.

En los últimos meses se han producido algunas iniciativas dirigidas a establecer un marco jurídico regulador de los contenidos criminales de Internet. La más importante ha sido la Ley para la Decencia en las Comunicaciones (*Communications Decency Act*) (CDA), aprobada por el Congreso de los Estados Unidos en febrero de 1996. Dicha ley prevé sanciones para quienes almacenen o distribuyan por la red informaciones, imágenes o sonidos que puedan considerarse obscenos o indecentes por agredir a la media de los valores morales de la comunidad.

Esta norma ha suscitado una viva polémica entre los juristas y ha sido objeto de diversos recursos. Como resultado de uno de ellos, un Tribunal de Pennsylvania ha declarado la inconstitucionalidad de dicha ley, el 11 de Junio de 1996, por decisión unánime de sus tres jueces. Se considera que la CDA limita injustificadamente el derecho a la libertad de expresión garantizado en la Primera Enmienda de la Constitución norteamericana, ya que al no considerar las informaciones transmitidas por Internet como prensa escrita se las somete a la censura previa por parte de la influyente Comisión Federal de Comunicaciones. Se denuncia también que esta ley lesiona las debidas garantías procesales (*due process of law*) reconocidas por la Quinta Enmienda y, en definitiva, la seguridad jurídica de los ciudadanos por la forma excesivamente vaga e imprecisa con la que se tipifican los supuestos que pueden entrañar atentados contra la decencia. Asimismo se considera que, la legítima protección de los menores, no debiera limitar la libre difusión de informaciones o imágenes normales para adultos, ya que los suministradores de servicios no pueden determinar la edad de los usuarios.

Uno de los jueces del Tribunal que declaró la inconstitucionalidad de la CDA, Stewart R. Dalzell, entendió que Internet implica una garantía para el desarrollo libre y autónomo de las comunicaciones entre los ciudadanos normales frente a la prepotencia de los grandes magnates poseedores de los medios de información. Internet puede considerarse, según este juez, como una "conversación mundial sin fin". Por ello, el Gobierno no puede arbitrariamente interrumpir esta conversación cívica por medio de normas como la CDA. Internet, según el juez Dalzell, por ser la forma más utilizada para un diálogo participativo de masas desarrollada hasta el presente, merece la más eficaz protección jurídica frente a intervenciones restrictivas gubernamentales que no se hallen debidamente justificadas.

Esta sentencia del Tribunal de Distrito de Pennsylvania fue recurrida ante la Supreme Court norteamericana, en el proceso de Janet Reno, Attorney General of the United States, et al., *versus* American Civil Liberties Union et al., que ha sido resuelto por la sentencia de 26 de Junio de 1997 (nº 96-511), que ha confirmado con el voto unánime del Tribunal la inconstitucionalidad de la CDA. El juez John Paul Stevens, al expresar la opinión mayoritaria del Tribunal, indica que la CDA es

abiertamente contraria a la Primera Enmienda y, de forma expresa, considera: "como un aspecto de la tradición constitucional que, en ausencia de evidencia en contrario, se presume que la regulación gubernamental del contenido de las comunicaciones tiende más a interferir el libre intercambio de ideas que a promoverlo. El interés por fomentar la libertad de expresión en una sociedad democrática sobrepasa cualquier teórico e improbable beneficio de la censura". Los jueces Sandra Day O'Connor y William Rhenquist, en un voto particular, mantienen también el carácter inconstitucional de la CDA, excepto en su estricta aplicación a cuanto hace referencia a la comunicación a los menores de informaciones o imágenes indecentes u obscenas (sobre todo ello vid., The Electronic Frontier Foundation, 1997)

6. Iniciativas de la Unión Europea.

En el seno de la Unión Europea se ha elaborado, en octubre de 1996, una Comunicación de la Comisión sobre *Contenidos ilícitos y nocivos en Internet*. Constituye el fin principal de dicho documento el logro de "un correcto equilibrio entre la garantía de la libre circulación de la información y la protección del interés público" entre los Estados miembros de la Unión Europea. Se parte para ello del principio básico de que lo que es ilegal fuera de la red también lo es en ella, por lo que los Estados miembros deben aplicar la legislación existente que pueda sancionar esas conductas ilícitas. No obstante, dada la descentralización y el carácter planetario de Internet, parece necesario establecer medidas en el ámbito de Justicia e Interior para intensificar la cooperación y la respuesta jurídica unitaria frente al reto que representa la criminalidad en Internet. Para ello, la Comisión, en el documento de referencia, insta a incrementar el intercambio de información entre los Estados miembros sobre los suministradores de contenidos delictivos; al tiempo que exhorta a los Estados miembros para que establezcan "criterios europeos mínimos" sobre contenidos criminales en Internet. La comisión reitera su propósito de fomentar los proyectos de autorregulación elaborados por las asociaciones de suministradores de acceso a Internet, por considerar que el papel de las mismas es de primordial eficacia para limitar la distribución de contenidos ilícitos en la red.

Complementaria, en cuanto a su cronología y alcance, de esa iniciativa se puede considerar el *Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información*, debida también a la Comisión respondiendo a una petición previa del Parlamento Europeo y del Consejo. Si se coteja el *Libro Verde* con la Comunicación se advierte que se trata de un documento, paradójicamente, más genérico y más específico. Más genérico en cuanto a su *ámbito*, ya que no se limita a la regulación de Internet, sino que se ocupa de todos los servicios audiovisuales y de información. Pero, al propio tiempo, se trata de un texto más específico en cuanto a su *objeto*, ya que se circunscribe a la protección de los menores y de la dignidad humana.

El *Libro Verde* recuerda que la protección jurídica de los menores y la dignidad en las normas constitucionales y legislativas de los Estados miembros de la Unión Europea tienen como soporte básico el Convenio Europeo de Derechos Humanos. Dicho Convenio ha sido integrado en el ordenamiento jurídico comunitario por el art. F2 del Tratado de la Unión Europea.

En el Convenio Europeo se reconoce el derecho al respeto de la vida privada y familiar (art.8) y, asimismo, el derecho a la libertad de expresión (art.10). No obstante, ambos derechos no son considerados como absolutos e ilimitados, al estar previsto que pueda condicionarse su ejercicio por medidas necesarias, en una sociedad democrática, para garantizar la seguridad, la salud, la moral o los derechos y libertades de los demás (arts.8.2 y 10.2).

La libertad de expresión a través de los servicios audiovisuales y, en consecuencia, de Internet no es ilimitada en el seno de la Unión Europea, si bien, sus limitaciones deben ser admitidas restrictivamente. No en vano la libertad de prestar servicios, también en la esfera de la información y la comunicación, es una de las libertades básicas reconocidas en el Tratado de la Unión. El *Libro Verde* se remite a la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) de Estrasburgo para advertir que la libertad de expresión defiende no sólo las ideas e informaciones que

no suponen intromisión u ofensa en los valores o derechos ajenos, sino también las susceptibles de ofender, contradecir o perturbar (STEDH, Handyside/Reino Unido, 1976).

El Libro Verde, acogiendo la jurisprudencia del TEDH (SS, Handyside/Reino Unido, 1976; The Sunday Times/Reino Unido, 1979; Autronic, 1990; Groppera Radio, 1990; Informationsverein Lentia, 1993), propugna que las restricciones a la libertad de expresión fundadas en la defensa de derechos ajenos, en concreto de los de los menores y la dignidad, se halle condicionada a tres exigencias acumulativas:

- 1) *Prohibición de arbitrariedad*, lo que implica que cada restricción deba estar prevista por la ley;
- 2) *Necesidad social* imperiosa de garantizar valores y derechos de las sociedades democráticas;
- 3) *Legitimidad de objetivos*, enumerados de forma limitada y entre los que la defensa de la moralidad y la salud públicas se estiman particularmente adecuados para proteger a los menores y la dignidad humana.

Es fácil inferir los problemas que pueden derivarse de la precisión de lo que, en cada caso, deba considerarse como "necesario" para legitimar una medida legal restrictiva y que persiga un "objetivo legítimo". No basta para ello que tal medida resulte "útil" o "razonable". El carácter legítimo de la medida sólo puede probarse tras un profundo examen de su eficacia en relación con el grado de injerencia que implica. Este análisis constituye una *prueba de proporcionalidad* de las medidas restrictivas. De ello se desprende que no deben imponerse restricciones a la libertad de expresión audiovisual que no estén justificadas en virtud de dicha prueba de proporcionalidad.

El Libro Verde, en definitiva, auspicia una regulación de las redes audiovisuales que tienda a armonizar la libertad de expresión con la defensa de los menores y de la dignidad. Para ello, aboga por el establecimiento de sistemas (por ejemplo, filtros de clasificación de contenidos) que garanticen que los menores no accedan a programas perjudiciales, permitiendo no obstante el acceso de los adultos. Se trata de soluciones procedentes de la base (*bottom up*) más que procedentes desde arriba (*top down*), que permiten obviar la necesidad de censura previa y aumentan la potencial eficacia de la autorregulación

7. Hacia una ética jurídica ciberespacial.

No es este el lugar para una consideración detenida en pormenores sobre las múltiples implicaciones económicas, culturales, sociales y políticas que se derivan de ese ciberespacio cuya navegación y conquista ha hecho posible Internet. Las consecuencias que pueden derivarse de esa forma de comunicación humana en soporte informático son imprevisibles y, a veces, paradójicas. Puede darse la circunstancia de que el máximo desarrollo de la comunicación tecnológica implique simultáneamente un empobrecimiento de las formas de comunicación tradicionales. Suele aducirse, para corroborar esos riesgos, la anécdota de un foro de "cibernautas" que concertaron un encuentro personal para reforzar sus contactos iniciados a través de Internet. La reunión fue un completo fracaso por las dificultades para establecer un diálogo interpersonal; la comunicación sólo se hizo de nuevo fluida cuando cada uno de los cibernautas la reemprendió desde su pantalla de ordenador.

No obstante, esta reflexión pecaría de un exceso de pesimismo si no reconociese las posibilidades de una renovación de los valores cívicos que puede promover Internet. En el área francófona se ha utilizado la expresión "*Netiquette*", es decir, "ética de la *Net* (red)", para aludir a las reglas deontológicas que deben presidir la utilización de Internet. Se trata de normas o programas éticos dirigidos a evitar las conductas perturbadoras realizadas por los cibernautas y para prevenir cualquier actividad que perjudique el normal funcionamiento de la red (Piette-Coudol y Bertrand, 1997).

Las redes de telecomunicaciones pueden conducir a una nueva ética "ciberespacial", que genere y

estímule actitudes de conciencia colectiva sobre el respeto de las libertades y de los bienes amenazados por una utilización indebida del ciberespacio, y contribuir a la formación de vínculos solidarios para la prevención de los crímenes informáticos y la ayuda a su descubrimiento. La difusión capilar de las redes comunicativas puede conducir a la producción de reglas jurídicas consuetudinarias sobre su uso, en las que la dimensión coactiva de las normas basada en la autoridad de un poder centralizado, deje paso a códigos de conducta cuya eficacia se base en la convicción de los usuarios y en su responsabilidad solidaria (Colom y Van Bolhuis, 1995; Forester, y Morrison, 1990).

8. Bibliografía.

Barlow, J. P., (1996): *Declaración de Independencia del Ciberespacio*, en "Cibernautas por la Tolerancia", <http://www.ctv.es/USERS/mrb/tolerancia/>.

Bensoussan, A., (ed.) (1996): *Internet: aspects juridiques*, Hermes, Paris.

Branscomb, A.W., (1995): *Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspace*, en "Yale Law Journal", n.104, pp. 1639 ss.

Bustos, M., (1996): *Detectives en el Ciberespacio*, en "Especial Simo", "El País", 5, noviembre.

Byassee, W.S., (1995): *Jurisdiction of Cyberspace*, en "Wake Forest Law Review", n. 30, pp. 197 ss.

Cavazos, E.A. y Morin, G., (1994): *Cyberspace and the Law*, MIT Press, Cambridge (Mass.).

Ciampi, C., (1995), *Una guida per giuristi nel ciber spazio di Internet: strumenti per la navigazione e prospettive di sviluppo*, en Atti del Congresso Annuale AICA, Chia-Cagliari, vol.I, pp. 543-550.

Ciampi, C., (1996): *Guida all'informazione giuridica nel ciber spazio*, http://www.idg.fi.cnr.it/ita/informazione/guida/cs_guide.htm.

Colom, V. y Van Bolhuis, H. E., (1995): *Cyberspace Reflections*, European Commission, Brussels.

Contenidos ilícitos y nocivos en Internet, (1996), Comunicación de la Comisión de las Comunidades Europeas, en "Documentos COM (96)" 487 final.

Cutrerá, T., (1991): *The Constitution in Cyberspace: the Fundamental Rights of Computers Users*, en "University of Missouri Law Review", n. 60, pp. 139 ss.

Fernández Calvo, R., (1996): *El Ciberespacio y sus dilemas* en "Especial Simo", "El País", 5, noviembre.

Forester, T. y Morrison, P. (1990): *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, MIT Press, Cambridge (Mass.).

Frosini, V. (1995): *Law and Liberty in the Computer Age*, Tano, Oslo.

Frosini, V. (1997): *la democrazia nel XXI secolo*, Ideazione, Roma.

Hance, O., (1996): *Leyes y negocios en Internet*, trad. cast. de Y. Juárez, MacGraw-Hill, México.

Internet desde la perspectiva jurídica, (1997): en *Manual práctico de Internet*, nº 13, en "Cuadernos de Cinco Días", 19, Febrero.

Iteanu, O., (1996): *Internet et le Droit*, Eyrolles, Paris.

La explosión Internet, (1997): Dossier de "Muy Especial", nº 28.

Libro Verde sobre la protección de los menores y de la dignidad humana en los nuevos servicios audiovisuales y de información, (1996), Comisión de las Comunidades Europeas, en "Documentos COM (96)" 483 final.

Moreno, M. A., (1995): *¿Es segura la Internet?* en "Base Informática", n. 27, pp.60-65.

Pascuzzi, G. (1995): *Cyberdiritto*, Zanichelli, Bologna.

Pérez Luño, A.E., (1996): *Manual de Informática y Derecho*, Ariel, Barcelona.

Pérez Luño, A.E., (1997), *Internet navegaciones y abordajes*, en "La Ley" (Revista Jurídica Española de Doctrina, Jurisprudencia y Bibliografía), nº 4258, pp. 1 y 14-15.

Piette-Coudol T. y Bertrand A., (1997): *Internet et la loi*, Dalloz, Paris.

Ramonet, I., (1997): *¿Nos han robado una esperanza !*, en *Internet, ¿un bien o una maldición?* en "El País Digital-Debates", 25, Febrero.

Rheinhold, H., (1996): *La comunidad virtual*, trad. cast. de J.A. Alvarez, Gedisa, Barcelona.

Ribas, J., *Aspectos legislativos de las autopistas de la información: Delitos en Internet*, (1996): en "Jornadas Profesionales Informat- 96", Barcelona, Octubre.

Rico, I., (1995): *Navegar por Internet* en, "Ideas-IBM" n. 15.

Rocha, M.L. y Macedo, M., (1996): *Direito no ciberespaco*, Cosmos, Lisboa.

Sánchez Bravo., *La regulación de los contenidos ilícitos y nocivos en Internet: una propuesta desde la Unión Europea*, en curso de publicación en "Informática y Derecho".

Sartor, G. (1996): *Intelligenza artificiale e diritto*, Giuffrè, Milano.

Sciuto, P. (1997): *Internet e diritto romano*, en "Informatica e diritto", n.1.

Stuckey, K., (1995): *Business and Legal Aspects of the Internet and online Services: Rights and Responsibilities of Information Service Providerr*, en "The Data Law Report", vol, 2, n. 4 y 5.

Terceiro, J.B., (1996): *Socied@d digit@l. Del homo sapiens al homo digitalis*, Alianza Editorial, Madrid.

The Electronic Frontier Foundation, (1997): *Free Speech On-Line Blue Ribbon Campaign*, <http://www.eff.org/>

