INTERNET Y LOS DERECHOS FUNDAMENTALES

María Luisa Fernández Esteban
Profesora de Derecho Constitucional
Universidad Autónoma de Madrid

I. INTRODUCCION. TENDENCIAS EN LA REGULACION DE INTERNET.

La garantía de que Internet es un espacio seguro en el que comprar, aprender, divertirse o, simplemente comunicarse con otros se ha convertido en uno de los requisitos para el crecimiento de la Red. Tanto es así que ha sido objeto de consideración por los Consejos Europeos de Lisboa y Feira, en cuyas Conclusiones se establece que la confianza de los consumidores es un factor esencial en el crecimiento del comercio electrónico, principal motor de Internet. El factor más importante para el despegue del comercio electrónico en Europa es la confianza[1]. En su Comunicación sobre impacto y prioridades de Europa 2002, la Comisión señala que los

(1) E.Liikanen, E. "Is there a third way for the Internet in Europe?" *Global Internet Summit*, Barcelona, 22 de mayo de May 2000,
http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/00/189|0|RAPID&lg=EN>EU.

problemas de seguridad, tanto los reales como los percibidos como tales son un hecho que inhibe el comercio electrónico[2]. Una encuesta realizada por el Eurobarómetro en otoño del 2000 dio como resultado que entorno al 17 % de los usuarios de Internet ha experimentado algún tipo de problemas. Varias son las razones que ponen a prueba la seguridad de los intercambios en Internet: la utilización de Internet para la comisión de delitos tales como la propagación de virus informáticos, el ataque de los piratas informáticos, la violación de los derechos de propiedad intelectual y la usurpación de marca, y la ocupación de direcciones de Internet a expensas de sus legítimos propietarios o *cibersquatting*. Algunos de estos obstáculos a la seguridad inciden directamente en los derechos fundamentales: la proliferación de contenido ilícito en Internet, o la interceptación ilegal de las comunicaciones; la amenaza a la intimidad que supone la recolección y proceso oculto de datos en Internet, etc.

Un aspecto esencial en la creación de un entorno seguro es que cada vez es más indispensable solucionar los problemas jurídicos a escala mundial, en la medida en que las incertidumbres que acompañan a las distintas respuestas nacionales y regionales a estos desafíos constituyen obstáculos al desarrollo de un mercado electrónico mundial. La Comisión Europea es consciente de la creciente necesidad de reforzar la coordinación internacional para hacer frente a los problemas jurídicos que plantea Internet[3]. En opinión de la Comisión no se trata de establecer una nueva autoridad internacional de vigilancia o una serie de normas vinculantes. Se deberá, más bien, tratar de lograr un acuerdo orientado hacia el futuro sobre el mejor medio de elaborar enfoques comunes frente a los problemas y a sus soluciones, es decir, desarrollar un procedimiento constante de coordinación en que los intereses del sector público y privado estén representados de manera adecuada.

Un segundo aspecto importante a la hora de hacer frente a los retos que presenta Internet es la creciente importancia de la autorregulación y la corregulación. Frente a la regulación, la autorregulación, esto es, la capacidad de los actores del mercado para organizarse y crear normas propias de adhesión voluntaria en un sector,

(2) Comunicación de la Comisión de 13 de marzo de 2001, Impacto y prioridades de Europa 2002, COM(2001) 140 final. Comunicación para el Consejo Europeo de primavera de Estocolmo de 23 y 24 de marzo de 2001.
http://europa.eu.int/eur-lex/es/com/cnc/2001/com2001_0140es01.pdf

(3) Comisión Europea, Comunicación "La mundialización y la sociedad de la información: necesidad de reforzar la coordinación internacional donde se analiza la creciente necesidad de cooperación internacional" COM (98) 50 final.
http://www.ispo.cec.be/eif/policy/com9850en.html

presenta ciertas ventajas que la hacen especialmente apropiada para algunos de los aspectos jurídicos de Internet: es una alternativa flexible, eficaz y rentable a la regulación, ya que consigue los mismos efectos que la regulación sin la lentitud que conllevan los procesos regulatorios. La autorregulación debe, desde luego, cumplir algunos requisitos. Debe, en primer lugar, respetar y reforzar la legislación en vigor. También debe ser de factible y de comprobable aplicación. Hasta hace poco, regulación y autorregulación eran percibidas como opuestas. En la economía de Internet y de las nuevas tecnologías se impone el pragmatismo. La corregulación significa el reparto de responsabilidad entre el operador público y los actores privados[4]. Pero el procedimiento legislativo se ve también afectado por el vertiginoso mundo de internet. En la Comunicación "Puesta al Día sobre eEurope[5]" la Comisión Europea destaca que una de las áreas en las que el impacto de internet es más perceptible es la del proceso legislativo. Los gobiernos y administraciones, incluida la Comisión, se han dado cuenta de que la "nueva economía", y en particular Internet, plantea nuevos retos al marco legislativo. Internet es un medio transfronterizo en el que están apareciendo nuevas maneras de ejercer la actividad comercial. Al transformar rápidamente el contexto del mercado y las "reglas del juego" *de facto*, plantea problemas, en ámbitos tales como la protección de datos, la seguridad de la información, la fiscalidad y la protección de los consumidores, que exigen soluciones inmediatas. Es preciso acelerar el proceso de elaboración de la legislación. La Comisión entiende que debe favorecer una mayor flexibilidad en la regulación del comercio electrónico basándose más en la autorregulación, entre otras cosas, mediante la cooperación con los organismos comerciales pertinentes, como el Global Business Dialogue (GBDe).

En tercer lugar, es preciso tener en cuenta que uno de los objetivos principales es potenciar el crecimiento de la economía digital, para lo cual resulta imprescindible mantener una visión integral de

(4) E.Liikanen, E. "Is there a third way for the Internet in Europe?" *Global Internet Summit*, Barcelona, 22 de mayo de May 2000,
http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/00/189|0|RAPID&lg=EN>EU

(5) Comisión Europea, Comunicación de la Comisión al Consejo y al Parlamento Europeo. Puesta al día sobre eEurope 2002. Preparada por la Comisión Europea para el Consejo Europeo de Niza, 7 y 8 de diciembre de 2000
http://europa.eu.int/comm/information_society/eeurope/documentation/update/index_es.htm

la regulación que permita, al mismo tiempo, proteger intereses constitucionales prioritarios y derechos fundamentales, sin desdeñar el respeto a la libre competencia y sin dañar el crecimiento en los nuevos mercados. La imposición de obligaciones jurídicas demasiado estrictas a los operadores del sector de Internet puede determinar que se impida el crecimiento de este sector, tanto frente a otros sectores relacionados como frente a sus competidores de países que permiten un crecimiento más libre de las empresas de Internet. La Comunicación de la Comisión sobre convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sus consecuencias para la reglamentación[6] subrayó el creciente acercamiento de los sectores audiovisual, de telecomunicaciones, e informático, cuyo paradigma es Internet y la creciente competencia que se está produciendo entre los actores de estos mercados.

1. El Plan de Acción EEuropa 2002.

La Unión Europea ha respondido a estos retos planteados por Internet a través de varias iniciativas. La iniciativa eEuropa fue lanzada el 8 de diciembre de 1999 con la adopción por parte de la Comisión de la Comunicación "eEuropa - Una Sociedad de la Información para todos[7]". El Consejo Europeo ha respaldado el Plan de Acción global "eEurope 2002" y ha solicitado a las Instituciones Comunitarias, a los Estados miembros y a todos los demás agentes que garanticen su plena aplicación a su debido tiempo, antes de 2002[8]. El objetivo de la iniciativa es acelerar la implantación de las tecnologías digitales en toda Europa y garantizar que todos los europeos tengan los conocimientos necesarios para utilizarlas. El Consejo Europeo se fijó como objetivo el convertir a Europa en la economía más competitiva y dinámica del mundo y ha convertido las cuestiones relativas a la sociedad de la información y a la nueva

(6) Comunicación "La convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sus consecuencias para la reglamentación" de 10 marzo 1999, COM(1999) 108 final

http://europa.eu.int/ISPO/convergencegp/com%2899%29108/com%2899%29108esfinal.html

(7) Comunicación "eEuropa - Una Sociedad de la Información para todos", 8 de diciembre de 1999, *http://europa.eu.int/comm/information_society/eeurope/index_en.htm*

(8) Consejo Europeo, Conclusiones de la Presidencia del Consejo Europeo de Lisboa, de 23 y 24 de marzo de 2000,

http://ue.eu.int/Newsroom/related.cfm?NOREFRESH=1&MAX=1&BID=76&GRP=2379&LANG=1

Conclusiones de la Presidencia del Consejo Europeo de Santa María da Feira de 19 y 20 de junio de 2000.

http://ue.eu.int/Newsroom/LoadDoc.cfm?MAX=1&DOC=!!!&BID=76&DID=62071&GRP=2587&LANG=7

economía en una de las prioridades de las instituciones comunitarias. En el Plan de Acción "Europa 2002, Una Sociedad de la Información para todos[9]" la Comisión y el Consejo dan cuenta de una serie de acciones para impulsar la sociedad de la información en Europa. El Plan de Acción introduce tres objetivos principales: una Internet rápida, barata y segura, inversión en capital humano y en su formación, y el estímulo del uso de Internet.

Uno de los medios de la iniciativa eEuropa para incrementar la confianza en Internet es completar el marco regulatorio de Internet. Componen este marco regulatorio numerosas iniciativas de la Comisión que afectan a distintos aspectos de la vida de Internet tales como decisiones sobre la liberalización definitiva de las telecomunicaciones, la introducción de un dominio general de alto nivel .eu, el estímulo de contenidos multimedios europeos y de la educación a través de las nuevas tecnologías, la protección de los derechos de propiedad intelectual en la Red, la lucha contra la delincuencia en el ciberespacio, la regulación de contenidos en Internet, la regulación del comercio electrónico, la protección de datos personales y de la intimidad en las comunicaciones electrónicas, la nueva regulación de la encriptación y la firma electrónica. Estas iniciativas son muy variadas, y van desde planes de acción a directivas y reglamentos comunitarios, pasando por las famosas comunicaciones y libros verdes de la Comisión. El Plan de Acción eEuropa 2002 pretende recopilar todas las iniciativas de regulación de Internet por parte de la Unión Europea. Por lo que a derechos fundamentales se refiere, estas acciones incluyen las propuestas para la lucha contra el cibercrimen, en particular contra la delincuencia en Internet, la regulación de contenidos en Internet, la medidas para la protección de datos en la Red, la lucha contra el racismo y la xenofobia en Internet o la simplificación del uso de tecnologías de doble uso que tutelan la intimidad en internet.

En este trabajo se analizarán los aspectos concretos del Plan eEurope que inciden en los derechos fundamentales[10]. El siguiente

(9) Consejo de la Unión y Comisión Europea, Plan de Acción, Una sociedad de la información para todos. preparado por el Consejo y la Comisión Europea para el Consejo Europeo de Feira 19-20 de junio de 2000, de 14 de junio de 2000.
http://europa.eu.int/eur-lex/es/com/cnc/2000/com2000_0330es01.pdf

(10) Sobre estos temas, véase M.L. Fernández Esteban : *Nuevas tecnologías, internet y Derechos Fundamentales* (Mc Graw Hill, 1998), y más recientemente "Incidencia de Internet en los derechos fundamentales" *Derecho sobre Internet* (BSCH,2000)
http://www.derechosobreinternet.com/textos/capitulo1.html

apartado está dedicado a la lucha contra el cibercrimen a través del proyecto de tratado del Consejo de Europa contra el cibercrimen. La lucha contra la pornografía infantil en Internet es uno de los ámbitos donde existe más consenso para su erradicación. El segundo apartado analiza la regulación de contenidos en Internet. En este caso se parte del análisis comparado de la situación en Estados unidos y en la Unión Europea con el Plan de Acción para el fomento del uso seguro de Internet. En relación con la regulación del contenido en internet es preciso mencionar la creciente presencia de material xenófobo o racista en internet. En el tercer apartado se analizan las causas de este crecimiento y las dificultades para encontrar un punto de acuerdo para la lucha contra este contenido de internet. El último apartado está dedicado a uno de los retos más importantes que supone internet para la protección de la intimidad: la protección de datos en internet.

II. LA LUCHA CONTRA EL CIBERCRIMEN.

El cibercrimen es una de las actividades delictivas de mayor crecimiento en el mundo. Existen un gran número de actividades criminales realizadas a través de la Red como delitos financieros, entrada ilegal en los sistemas informáticos *(hacking)*, circulación de pornografía infantil, virus informáticos, y delitos de genocidio y apología del racismo y la xenofobia a través de páginas web. La reunión del G-8 en París del 15 al 17 de mayo de 2000 trató sobre la coordinación internacional para hacer frente a la creciente criminalidad en La Red. El Consejo de Ministros trata de aproximar las penas por el tráfico de personas y la pornografía infantil.

Debe mencionarse la existencia de un proyecto de Convenio sobre cibercrimen auspiciado por el Consejo de Europa[11]. Se trata del Proyecto de Convenio sobre delincuencia en el ciberespacio que ha sido hecho público para su discusión pública por el Consejo de Europa el 27 de abril de 2000. Es el primer tratado internacional en regular aspectos penales y procesales de varios delitos contra sistemas informáticos y otros abusos. De entrar en vigor, el Proyecto de Tratado armonizaría la legislación de los Estados miembros sobre

(11)Proyecto de Convenio sobre delincuencia en el ciberespacio, PC-CY (2000) proyecto n° 19, *http://conventions.coe.int/treaty/en/projets/cybercrime.htm*

estas cuestiones, facilitando las investigaciones y permitiendo una cooperación eficaz entre las autoridades de los 41 miembros del Consejo de Europa y otros, como Estados Unidos y Canadá. La versión final debería estar preparada para diciembre de 2000 y el texto podría ser aprobado por el Comité de Ministros del Consejo de Europa durante el otoño de 2001.

El Proyecto de Tratado introduce, entre otras cosas, la armonización en cuanto a la definición de ataques a sistemas informáticos, interceptación ilegal de comunicaciones electrónicas, fraude y falsificación. También prohíbe la pornografía infantil en Internet, incluyendo la posesión y la reproducción y distribución de material sujeto a derechos de propiedad intelectual. El Proyecto de Tratado no sólo define los delitos, sino que introduce disposiciones sobre responsabilidad y determina unos niveles mínimos para las penas. También se incluyen medidas para su aplicación: los países miembros del tratado deberán otorgar competencias a sus autoridades competentes para permitir el registro y secuestro de ordenadores y datos, y obligar a terceros a entregar datos referentes a la comisión de delitos. La interceptación legal de las comunicaciones electrónicas es objeto de discusión en estos momentos, y ello porque este tipo de medidas requiere la cooperación de los operadores de telecomunicaciones. En este sentido, la redacción del Proyecto de tratado ha recibido las críticas del Grupo de Trabajo sobre protección de datos personales de la Unión Europea, que ha expresado su preocupación sobre las obligaciones que se establecen para los operadores de cooperar con las fuerzas del orden, que les llevan a tener que almacenar los datos de tráfico hasta 60 días, lo que puede suponer una violación tanto del derecho fundamental a la protección de datos como un notable coste económico para estos operadores de Internet. Además, el proyecto, que tendrá un importante impacto en los derechos fundamentales, incorpora definiciones vagas de orden público y no presenta ninguna disposición sobre protección de datos personales. La participación en el proyecto de tratado de países que no son miembros del Consejo de Europa puede generar conflictos sobre la aplicación del tratado en relación a la protección de derechos fundamentales, ya que países como los Estados Unidos o Canadá no están vinculados por los estándares mínimos establecidos en el Convenio de Roma de 1950[12].

(12)Grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, Dictamen 4/2001, de 22 de marzo, sobre el proyecto de Tratado del Consejo de Europa sobre Cibercrimen
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp41en.hm

Como el cibercrimen es, a menudo, de naturaleza internacional, las medidas nacionales necesitan ser completadas con la cooperación internacional. El Proyecto de Tratado requerirá a los países miembros una cooperación activa entre ellos, conservando las pruebas o indicios del delito y localizando a los sospechosos. Las formas tradicionales de cooperación internacional, asistencia y extradición se verán completadas por una red de puntos nacionales de contacto, en contacto permanente, con el fin de agilizar las investigaciones internacionales. La cooperación internacional entre países miembros del Consejo de Europa y países no miembros puede suponer riesgos para la intimidad de las personas, ya que no queda en absoluto claro que las autoridades de los primeros puedan oponerse a la transferencia de datos sensibles a países que no garanticen la protección de datos, en franca contradicción con los principios del Convenio de Roma y las Directivas comunitarias de protección de datos.

El Plan de Acción eEuropa ha incluido entre sus objetivos el establecimiento de un enfoque europeo coordinado y coherente frente a la delincuencia informática. En un Consejo informal celebrado en febrero de 2001 en Estocolmo, los ministros de interior decidieron adoptar un marco legal común que permita armonizar la definición y las penas de estos delitos.

En este contexto se inscribe la Comunicación de la Comisión sobre ciberdelincuencia y ciberseguridad de febrero de 2001[13]. La Comunicación constituye la primera declaración política global sobre ciberdelincuencia efectuada por la Comisión. Esta Comunicación pone en perspectiva las diversas cuestiones, anunciará medidas legislativas y no legislativas y delinea la manera en que la Comisión va a tratar de alcanzar un equilibrio entre los distintos intereses sociales en la preparación de nuevas propuestas de medidas. Combatir el cibercrimen para crear un entorno más seguro en Internet es uno de los objetivos del Plan de Acción de eEurope 2002, que es vital para el desarrollo del comercio electrónico en Europa y de la Sociedad de la Información en general.

(13) Comunicación de la Comisión. Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.
http://europa.eu.int/ISPO/ecommerce/legal/documents/crimecom/CrimeComES.pdf

La nueva infraestructura ofrecida por Internet ofrece nuevas oportunidades de actividades delictivas. Éstas constituyen una amenaza para la inversión y pueden causar daños considerables. Es precisa, por tanto la acción para prevenir la actividad delictiva como para asegurar a las fuerzas del orden que cuentan con los medios de acción necesarios. La Comunicación anuncia medias legislativas y no legislativas. Las medidas legislativas previstas incluyen la aproximación de la legislación de los Estados miembros, en particular de las medidas contra la pornografía infantil. Esto último forma parte de un paquete de medidas contra la explotación infantil y el tráfico de seres humanos que la Comisión aprobó recientemente[14]. En el futuro la Comisión introducirá propuestas para la aproximación del derecho penal sustantivo en materia de criminalidad de alta tecnología, incluyendo medidas contra la denegación de servicio y los ataques informáticos *(hacking)*. La Comisión también examinará la posibilidad de una acción contra el racismo y la xenofobia en Internet.

En segundo lugar, la Comunicación sugiere también una serie de medidas no legislativas para impulsar el conocimiento de este tipo de acciones por los actores de la seguridad de la Información. Esta propuesta insiste en la necesidad de una formación adecuada de las fuerzas de seguridad del Derecho y del resto de operadores jurídicos en temas relacionados con la criminalidad de alta tecnología a través de los programas de la Comisión.

En materia de lucha contra la pornografía infantil el Consejo adoptó una Decisión para combatir la pornografía infantil en Internet en mayo de 2000[15] Esta Decisión se refiere a la necesidad de estimular la colaboración de los ciudadanos indicando los modos de ponerse en contacto con las autoridades policiales y al establecimiento de una cooperación más estrecha entre puntos de contacto especializados de las policías de los Estados miembros. La Decisión menciona la necesaria cooperación de los proveedores de acceso a Internet para acabar contra esta lacra.

(14) Propuesta de una decisión marco del Consejo para combatir el tráfico de seres humanos. Comunicación de la Comisión de 21 de diciembre de 2000, COM(2000) 854 final. Combatir el tráfico del seres humanos y combatir la explotación sexual de los niños y la pornografía infantil.

http://europa.eu.int/eur-lex/es/com/pdf/2000/com2000_0854es01.pdf

(15) Decisión del Consejo 2000/375/JAI, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet DOCE L 138/1 de 9.6.2000

http://europa.eu.int/ISPO/docs/policy/docs/42000X0375/es.pdf

En diciembre de 2000, la Comisión hizo pública una Propuesta de Decisión Marco del Consejo para combatir el tráfico de seres humanos, en el ámbito del tercer pilar del Tratado de la Unión Europea[16]. El actual artículo 29 del Tratado de la Unión Europea, contiene una referencia explícita a los delitos contra los niños. El Consejo Europeo de Tampere expresó el acuerdo en definiciones comunes de los tipos penales y las penas en delitos cometidos con el uso de nuevas tecnologías. La Propuesta se refiere a la cada vez más preocupante cuestión de la pornografía infantil en Internet, con el fin de dejar patente la determinación de la Unión Europea de incorporar medidas comunes de derecho penal y contribuir a crear un entorno más seguro para los usuarios de Internet. La propuesta de la Comisión se ha inspirado en el trabajo realizado en el ámbito internacional por el Protocolo de Naciones Unidas sobre tráfico de seres humanos y la futura convención sobre cibercrimen antes mencionada.

En su Propuesta de decisión marco del Consejo para combatir la explotación sexual de los niños y la pornografía infantil, la Comisión introduce importantes elementos para combatir la pornografía infantil que serán tratados también en la futura Convención sobre cibercrimen. La propuesta de Decisión marco prevé la aproximación de las legislaciones penales de los estados miembros relacionadas con la explotación sexual de los niños y la pornografía infantil. La propuesta incluye cuestiones judiciales horizontales y cooperación judicial entre los países.

El artículo 6 de la Propuesta se refiere a la responsabilidad civil y penal de las personas jurídicas, y es relevante por lo que se refiere a la comisión de estos delitos en las redes informáticas. El artículo 6 no afecta a las disposiciones de la Directiva 2000/31/EC sobre comercio electrónico[17], que establece las normas sobre responsabilidad de los proveedores de servicios intermediarios sus artículos 12, 13 y 14 y el artículo 15, que especifica que los estados

(16) Propuesta de una decisión marco del Consejo para combatir el tráfico de seres humanos. Comunicación de la Comisión de 21 de diciembre de 2000, COM(2000) 854 final. Combatir el tráfico del seres humanos y combatir la explotación sexual de los niños y la pornografía infantil.

http://europa.eu.int/eur-lex/es/com/pdf/2000/com2000_0854es01.pdf

(17) Directiva 2000/31/CE del Parlamento y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular el comercio electrónico, en el Mercado Interior (Directiva sobre el comercio electrónico), DOCE L 178 de 17 de julio de 2000

http://europa.eu.int/comm/internal_market/en/media/eleccomm/com31es.pdf

miembros no impondrán a los intermediarios una obligación general de supervisión, ni una obligación de buscar indicios de actividad ilegal. La Directiva 2000/31/CE sobre el comercio electrónico prohíbe a los Estados miembros que impongan a los prestadores de servicios una obligación general de supervisar los datos que transmiten, ni de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, sin perjuicio de cualquier actividad de supervisión, selectiva y transitoria establecida por mandamiento judicial, aunque sí que podrán establecer un deber de cooperación una vez que conozcan de la existencia del material ilícito. Existe actualmente una segunda versión del Anteproyecto de Ley para incorporar la Directiva del comercio electrónico, de 30 de abril de 2001. En el artículo 11 del Anteproyecto se establecen algunas obligaciones de cooperación de los prestadores de servicios con la autoridad policial y judicial:

a) Comunicar a las autoridades judiciales o administrativas competentes, tan pronto como tengan conocimiento de su existencia, la actividad presuntamente ilícita, realizada por el destinatario del servicio.

b) Comunicar a las autoridades judiciales o administrativas competentes, a solicitud de éstas, la información que les permita identificar a los destinatarios de servicios.

c) Suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio de la sociedad de la información, para poner fin a una infracción o impedirla, cuando así les sea solicitado por una autoridad judicial o administrativa competente.

d) Supervisar o conservar todos los datos relativos a un determinado sitio de Internet durante un período máximo de seis meses y ponerlos a disposición de la autoridad judicial competente, cuando ésta así lo requiera.

III. LA REGULACION DE CONTENIDOS EN INTERNET.

La preocupación por la regulación de la libertad de expresión en Internet se ha intensificado desde la incorporación masiva de cientos de millones de usuarios en todo el mundo. La inquietud por la necesidad de crear un entorno seguro que favorezca el crecimiento de la Red es compartida por muchos países.

Aunque la preocupación por la presencia de material ilícito y nocivo en la Red es la misma en Europa y en Estados Unidos, las soluciones que se han adoptado son distintas. Mientras que en Estados Unidos ha existido un intento de regulación y limitación de la libertad de expresión en Internet con la Ley de Decencia en las Telecomunicaciones (*Congress Decency Act*, en adelante CDA)[18], desde la Unión Europea auspician otras soluciones menos restrictivas de la libertad de expresión, como el Plan de Acción.

1. La Ley de Decencia en las Telecomunicaciones de Estados Unidos y la polémica en torno a los filtros obligatorios.

Reflejando preocupaciones análogas de otros lugares del mundo, en febrero de 1996 el Congreso de Estados Unidos estableció la CDA. Esta Ley declaraba ilegal el uso de ordenadores y de las líneas telefónicas para transmitir material "indecente", y preveía severas penas de privación de libertad y multas para los nuevos tipos penales. La CDA establecía penas de prisión de hasta dos años y multas de hasta 250.000 dólares para cualquiera que usase un tipo de discurso "indecente" *(indecent)* o "claramente ofensivo" *(patently offensive)* en una red de ordenadores en los que ese tipo de discurso pudieran ser visto por menores.

Al prohibir de hecho la presencia de material "indecente" en Internet, La CDA introducía una severa restricción de la libertad de expresión en aras de la protección de la juventud y la infancia que, debido a la gravedad de las penas, hubiese provocado la "autocensura" *(chilling effect)* de los que introducen contenidos en Internet. Por este y otros motivos, la CDA fue declarada inconstitucional por el Tribunal Supremo Norteamericano por ser contraria a la Primera Enmienda a la Constitución Norteamericana[19]. El objeto fundamental de la sentencia del Tribunal Supremo norteamericano consistía en decidir si Internet es similar a la radiodifusión, en cuyo caso, el Congreso podía lícitamente prohibir el contenido "indecente", o bien se asemeja más a la prensa escrita, lo que impediría al Congreso establecer esa limitación.

(18) *United States Congress Communications Decency Act,*
http://www.gseis.ucla.edu/iclp/cda.dispute.html

(19) Sentencia del Tribunal Supremo de Estados Unidos de 26 de junio de 1997. Tribunal Supremo de Estados Unidos, caso No. 96-511. Janet reno v. ACLU, de 27 de junio de 1997

http://www.ciec.org/SC_appeal/opinion.shtml

Comentarios a esta sentencia, M.L , Fernández Esteban: "Limitaciones Constitucionales e inconstitucionales a la Libertad de Expresión en Internet", *Revista Española de Derecho Constitucional*, núm. 53, 1998, pág.283; Volokh, E.: "Freedom of Speech, Shielding Children, and Transcending Balancing" *Supreme Court Review*, 1997,

http://www.law.ucla.edu/faculty/volokh/shield.htm

Basándose en la equiparación de Internet a la prensa escrita, el Tribunal Supremo norteamericano declaró la inconstitucionalidad de la CDA, inclinándose a favor de una mayor libertad de expresión en el ciberespacio. En este sentido, el Tribunal Supremo considera que Internet se asemeja más a la prensa escrita y al teléfono que a la radiodifusión, y, por ello, Internet carece de las características que tradicionalmente han justificado la mayor limitación del ejercicio de la libertad de expresión en la radiodifusión.

Durante el segundo semestre de 1998 fueron aprobadas en Estados Unidos otras dos leyes federales: la Ley de Internet Seguro para las Escuelas *(Safe Schools Internet Act)*[20] y la Ley de Protección de los Menores Conectados a Internet, *(Child Online Protection Act)*[21], que ha sido denominada por sus detractores la *Congress Decency Act II*. La Ley del Internet Seguro para las escuelas requiere que toda escuela, instituto o biblioteca que reciba fondos públicos debe instalar programas-filtro para restringir el acceso a Internet. En estos momentos existen ya varios procesos judiciales abiertos contra la Ley[22]. La nueva Ley bordea los límites de la declaración de inconstitucionalidad CDA, ya que permite a los titulares de páginas web distribuir pornografía, pero exige que aquellos sitios que distribuyen material que es nocivo para los menores comprueben que el usuario es un adulto a través del uso de cartas de crédito, códigos de acceso para adultos u otras tecnologías que puedan desarrollarse en el futuro. La Ley de Protección de los Menores Conectados a Internet ya ha sido declarada inconstitucional, y por ello inaplicable, por un juez de Filadelfia el 1 de febrero de 1999[23].

(20) *United States Congress Safe Schools Internet Act, http://www.techlawjournal.com/congress/blocking/s1619.htm*

(21) *United States CongressChild Online Protection Act http://www.techlawjournal.com/congress/s1482coats/s1482.htm*

(22) Sentencia del Tribunal del Distrito Este de Virginia, caso No. 97-2049-A. *Mainstream Loudoun v. Board Of Trustees Of Loudoun County Library*, de 23 de noviembre de 1998, *http://www.techlawjournal.com/courts/loudon/81123op.htm*

(23) Tribunal del Distrito Este de Virginia, caso NO. 98-5591. *ACLU V. Reno*, decisión de 1 de febrero de 1999.

http://www.aclu.org/court/acluvrenoII_pi_order.html

2. El Plan de Acción comunitario para promover el uso seguro de Internet.

La Comisión Europea hizo público el 23 de octubre de 1996 el Libro Verde sobre la Protección de los menores y de la Dignidad Humana en los Nuevos Servicios Audiovisuales y de Información[24] en el que distingue entre dos tipos de contenido en Internet que pueden afectar a la creación de un entorno seguro: contenido ilegal y contenido perjudicial. "Contenido ilegal" se refiere a una amplia variedad de problemas: seguridad nacional; protección de los menores; protección de la dignidad humana; seguridad económica; protección de la información; protección de la vida privada; protección de la reputación; y propiedad intelectual. "Contenido perjudicial" es un contenido autorizado pero de distribución limitada (reservada a los adultos, por ejemplo) y un contenido que puede ofender a algunos usuarios, aunque no se limite su publicación debido al derecho fundamental a la libertad de expresión.

La distinción entre contenido ilegal y perjudicial es importante puesto que reciben un tratamiento diferente: del contenido ilegal deben ocuparse desde su origen las autoridades policiales y judiciales, cuyas actividades quedan cubiertas por las normas legales nacionales y por los acuerdos de cooperación judicial. La industria puede, sin embargo, aportar una ayuda importante para limitar la circulación del contenido ilegal (en particular en los casos de pornografía infantil, racismo y antisemitismo) mediante mecanismos de autorreglamentación eficaces (como códigos de conducta y establecimiento de líneas directas) regulados y apoyados por disposiciones jurídicas y que se beneficien del apoyo de los consumidores; para tratar el contenido perjudicial, las acciones deben dar a los usuarios la posibilidad de rechazarlo, preferentemente mediante el desarrollo de soluciones tecnológicas (sistemas de filtrado y de clasificación), reforzar la sensibilización de los padres y desarrollar una autorreglamentación que pueda proporcionar un marco adecuado, en particular para la protección de los menores. Comparando los distintos medios audiovisuales, se hace patente el desarrollo de actividades con una intensidad variable; la mayor parte de los esfuerzos

(24) Libro Verde sobre la Protección de los menores y de la Dignidad Humana en los Nuevos Servicios Audiovisuales y de Información.
COM (96) 483, *http://www2.echo.lu/legal/en/internet/content/gpen-toc.html*

están dedicados a la protección de los menores y de la dignidad humana con relación a internet, y la menor parte se refieren a los Videojuegos. En lo relativo a la comparación de las actuaciones llevadas a cabo por los Estados miembros, se observa una gran variación, desde los países en los que apenas se ha intervenido, especialmente por lo que se refiere a internet, como es el caso de España a los Estados en que se han realizado esfuerzos notables por establecer una política común a los distintos medios audiovisuales, como Países Bajos o Reino Unido.

El 25 de enero de 1999 se aprobó el Plan plurianual de Acción para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales[25]. La Comisión Europea, el Parlamento Europeo y el Consejo de la Unión son los promotores de esta iniciativa cuya finalidad es contribuir de manera eficaz a promover el uso seguro de Internet, completando y en cierta medida coordinando las acciones de los estados miembros. El Plan de Acción comunitario se basa en tres pilares fundamentales: (1) fomento de un uso responsable de Internet a través de la educación y de la promoción de métodos de control por el usuario, como filtros y sistemas de clasificación (2) impulso de la autorregulación del sector y establecimiento de líneas de denuncia y (3) sensibilización. El plan de acción, de una duración de cuatro años (del 1 de enero de 1999 al 31 de diciembre de 2002) tiene como objetivo: incentivar el desarrollo de los actores (industria, usuarios) y la aplicación de sistemas adecuados de autorreglamentación; el impulso inicial favoreciendo las demostraciones y promoviendo la aplicación de soluciones técnicas; alertar e informar a padres y profesores, en particular por medio de las asociaciones correspondientes; fomentar la cooperación y el intercambio de experiencias y mejores prácticas; promover la coordinación a escala europea y entre los actores interesados; garantizar la compatibilidad entre los enfoques adoptados en Europa y en otros lugares.

Para realizar estos objetivo, se emprenderán bajo la responsabilidad de la Comisión las acciones siguientes (art.3): promoción de la autorreglamentación de la industria y de los sistemas de seguimiento de contenidos (especialmente relacionados con contenidos

(25) Decisión 276/1999/EC del Consejo y del Parlamento Europeo, DOCE L 33 de 6 de febrero de 1999
ftp://ftp.echo.lu/pub/iap/decision/no276es.pdf

como la pornografía infantil, el racismo y el antisemitismo); incentivos a la industria para que se dote de instrumentos de filtrado y mecanismos de clasificación que permitan a padres o profesores seleccionar contenidos convenientes para los niños a su cuidado y que permitan al mismo tiempo a los adultos elegir el contenido legal al que desean acceder y que tengan en cuenta la diversidad cultural y lingüística; aumento de la sensibilización de los usuarios, en particular padres y profesores, hacia los servicios ofrecidos por la industria; evaluación de las implicaciones jurídicas; actividades que favorezcan la cooperación internacional etc.

2.1 Fomento de la autorregulación a través de códigos de conducta.

La reglamentación tradicional de por sí, que era útil en un entorno analógico, ya no constituye el enfoque adecuado en la era digital. El desarrollo de los medios digitales, particularmente de internet, la radiodifusión digital y los videojuegos, representa un reto fundamental para la política audiovisual de la Unión Europea, especialmente por lo que se refiere a la protección de menores. El desarrollo de internet ha complicado en mayor medida la situación de proteger a los menores. Mientras que en la radiodifusión tradicional –ya sea por vía analógica o digital– es fácil identificar al organismo de radiodifusión de que se trate, es difícil y a veces imposible determinar la fuente de las informaciones de internet. Por tanto, es fácil acceder, incluso de manera involuntaria, a contenidos nocivos e ilícitos.

Para responder a este reto, el Consejo adoptó la Recomendación 98/560 sobre la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana[26], por la que se pedía el establecimiento de marcos autorreguladores nacionales que complementen a los marcos reguladores europeos, a fin de mejorar la protección de los menores y de la dignidad humana en los sectores de la radiodifusión e internet. La recomendación incluía un anexo, con unas directrices

(26) Recomendación 98/560/CE 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.
http://europa.eu.int/eur-lex/es/lif/dat/1998/es_398X0560.html

para la aplicación de los marcos de autorregulación. El objetivo perseguido era elaborar, en el marco nacional de autorregulación, normas básicas estrictamente proporcionadas a los objetivos perseguidos. Estas normas debían integrarse en un código o códigos de conducta adoptados y aplicados voluntariamente por los operadores (esto es, principalmente las empresas). A la hora de elaborar estas normas, la Recomendación mencionaba que debían tenerse en cuenta tanto los principios de libertad de expresión y de protección de la vida privada así como el principio de libre circulación de servicios como el principio de viabilidad técnica y económica, dado que el objetivo global es el desarrollo de la sociedad de la información en Europa.

En cuanto al contenido, la Recomendación mencionaba en primer lugar, la protección de menores, con el objetivo de permitir que los menores utilicen de forma responsable los servicios en línea y evitar que accedan sin permiso de sus padres o educadores a contenidos legales que puedan perjudicar su desarrollo físico, mental o moral; la protección de la dignidad humana, a través de la lucha contra el contenido ilícito y el establecimiento de medidas de control de las infracciones de los propios código de conducta.

Para proteger a los menores la Recomendación establece que los códigos de conducta deben incluir disposiciones sobre información a los usuarios por los proveedores de acceso de los peligros y riesgos que genera internet, las condiciones a las que la oferta y difusión de contenidos que puedan perjudicar a los menores deban quedar sometidas, y el apoyo al ejercicio del control parental. En cuanto a las condiciones de oferta de material nocivo, la Recomendación señala que los códigos de conducta pueden hacer referencia a medidas tales como una portada de advertencia o una señal sonora o visual, marcado descriptivo o clasificación del contenido o sistemas de comprobación de la edad de los usuarios. El apoyo al ejercicio del control parental implica que, siempre que sea posible, debería proporcionarse a los padres, educadores y demás personas que ejerzan este tipo de control, herramientas de ayuda fáciles de usar y suficientemente flexibles que, sin comprometer sus opciones educativas, permitan que los menores de los que son responsables accedan a los servicios, incluso sin supervisión. Se trata de los programas de filtrado que serán analizados en el siguiente apartado. También se menciona en la Recomendación que debe hacerse mención en los códigos de conducta a una gestión de reclamaciones sencilla, a través líneas directas.

En cuanto a la lucha contra el contenido ilícito a través de los códigos de conducta, merece ser destacada la mención a la cooperación de los operadores con las autoridades judiciales y policiales. Los códigos de conducta deberían abordar, por ejemplo, la cuestión de las normas básicas sobre los procedimientos de cooperación entre los operadores y las autoridades públicas competentes.

El 27 de febrero de 2001, la Comisión ha hecho público un Informe[27] de evaluación de la aplicación de la Recomendación en los Estados miembros dos años después de su adopción. En la mayoría de los Estados miembros, entre ellos España, ya se han creado asociaciones de operadores de Internet. Cuatro Estados miembros, entre ellos España, tienen más de una representación de Operadores. En el ámbito europeo se ha creado la Asociación Europea de Proveedores de Servicios de Internet (EuroIspa)[28], como federación paneuropea de asociaciones de proveedores de servicios de internet procedentes de distintos países de la Unión Europea. Entre sus objetivos, se encuentran la promoción de internet, la contribución al desarrollo de un mercado de telecomunicaciones libre y abierto, la elaboración de normas profesionales para el sector, la influencia en el desarrollo de normas técnicas, la promoción de la autorregulación y la influencia en el proceso normativo en representación de la industria de internet. Se han establecido códigos deontológicos por los proveedores de acceso en los que se tratan cuestiones como la responsabilidad de los proveedores respecto a las informaciones que ofrecen, la protección de los menores y los procedimientos que deben seguirse con relación a las reclamaciones. Este tipo de códigos existen en todos los Estados miembros.

2.2 Fomento del uso responsable a través del filtrado.

Otra línea de actuación del Plan de Acción tiene por objeto fomentar el establecimiento de sistemas europeos de filtrado y de clasificación, así como familiarizar a los usuarios con su utilización y demostrar los beneficios que reportan estos recursos. Sólo en

(27) Comisión Europea, Informe de la evaluación de la Comisión al Consejo y al Parlamento europeo sobre la aplicación de la recomendación del Consejo de 24 de septiembre de 1998 sobre la protección de los menores y la dignidad humana 27.02.2001,COM(2001) 106 final
http://europa.eu.int/eur-lex/es/com/cnc/2001/com2001_0106es01.pdf
(28) *http://www.euroispa.org*

Francia los operadores están obligados a informar a los usuarios sobre los sistemas de filtrado y clasificación y los programas informáticos de que disponen para determinar la edad del usuario, mientras que en España esto forma parte del código deontológico de los operadores. La Comisión Europea ha impulsado cinco proyectos y está preparando otra convocatoria de propuestas. Las medidas incluyen, en particular, los aspectos siguientes:

(i) espacios protegidos; éstos consisten en portales especiales en los que los operadores garantizan la calidad de los sitios a los que dan acceso.

(ii) la adaptación de programas informáticos existentes para abarcar nuevas lenguas;

(iii) métodos de busca de fácil manejo para la familia;

(iv) suministro por parte de organizaciones comerciales o no comerciales, pero orientadas a la defensa de determinados valores, de plantillas *(templates)* y listas que puedan utilizarse en combinación con opciones de filtrado integradas en navegadores; y evaluación de los programas informáticos y los servicios de filtrado.

Un estudio encargado por la Comisión europea[29], publicado en diciembre de 1999, analiza la situación de estos dispositivos. La creciente difusión de Internet y de sus servicios ha sensibilizado a los usuarios frente a la necesidad de hallar nuevas formas de proteger a los menores del contenido ilícito y nocivo presente en Internet. Aunque los programas existentes en el mercado permiten controlar el acceso a este tipo de contenido por parte del usuario, es precisa una supervisión por parte de los organismos públicos sobre este tipo de dispositivos por los problemas que pueden generar. La definición de lo que es ilegal o nocivo varía de un país a otro. La noción de contenido nocivo tiene un componente cultural muy fuerte que da lugar a una nueva problemática y que requiere soluciones específicas.

(29) Mathonet, Ph. y otros "Review of European third-party filtering and rating software & services" (1999), *www.idate.org, http://europa.eu.int/ISPO/iap/index.html*

Todas las diferencias entre los estándares de gusto, decencia u obscenidad entre países deben ser tenidos en consideración a la hora de decidir el etiquetado de páginas. Aparte de las ventajas y oportunidades que los programas de filtrado ofrecen para un uso seguro de internet, otras dimensiones culturales, lingüísticas o éticas deben ser también consideradas, con el fin de apreciar la eficacia de los sistemas de filtrado y valoración y su adopción por los usuarios.

El objetivo del estudio era analizar la eficacia y aceptación de cinco programas en seis países europeos. Con otras palabras, se trataba de apreciar si los programas pueden funcionar teniendo en cuenta la diversidad cultural y lingüística de los usuarios europeos. Los resultados demostraron que los usuarios sólo están parcialmente satisfechos con estos programas, y demuestran una gran desconfianza hacia la eficacia de estos dispositivos para bloquear el contenido considerado peligroso o inapropiado para los niños. La insatisfacción de los consumidores procede, en gran parte de las dificultades de instalación, de la incapacidad de los programas para discernir cuando el material es apropiado o inapropiado para los niños según su contexto, sucediendo un exceso o defecto en el bloqueo del material presente en Internet. Además, los usuarios analizados en países de habla no inglesa declararon su insatisfacción con la capacidad de estos productos para bloquear material nocivo en otros idiomas distintos del inglés. Como conclusión, los autores del análisis entienden que es preciso aún realizar notables mejoras para extender el uso del filtrado entre los consumidores europeos.

La mejora de estos productos es esencial si se quieren convertir en productos de uso masivo para la protección de menores en Internet. En general, los productos deben mejorar para garantizar una mayor compatibilidad con los sistemas operativos, incluir instrucciones de instalación y uso más claras y mejorar su eficacia y el uso de estos dispositivos no debería ralentizar el uso del ordenador. Por lo que se refiere al contenido, los programas de filtrado deberían ser capaces de bloquear imágenes pornográficas, cosa que algunos programas no hacen. Además, deberían evitar que los usuarios pudieran manipular fácilmente por sus destinatarios los niños. El aviso de que se va a entrar en una página pornográfica no es suficiente. Los creadores de este tipo de programas deben mejorar el proceso de indexado de palabras para integrar mejor el significado de palabras asociadas con el contexto y crear un sistema de filtrado más inteligente. En general, deberían darse a los consumidores una

mejor explicación sobre los criterios de filtrado y clasificación usados por las compañías.

Finalmente el estudio propone como medida suplementaria la creación de listados negros de páginas con contenido ilícito o nocivo con el fin de informar a los usuarios y la creación de mecanismos de clasificación de páginas que sean respetuosos con la tradición europea y la diversidad lingüística. El problema, naturalmente, es el de definir criterios comunes de clasificación del contenido. Se recomienda también la creación de una línea de información, independiente de las compañías que comercialicen estos productos, que permitiera informar a los usuarios sobre este tipo de dispositivos y a ayudarles en su configuración o instalación.

La Comisión ha publicado un reciente informe[30] sobre INCORE. El objetivo del proyecto INCORE es analizar la posibilidad de un sistema de autoetiquetado y sistema de filtrado para el contenido de Internet desde una perspectiva europea. Este sistema debe respetar los principios de libre competencia y el derecho a la libertad de expresión, tener en cuenta las diferencias culturales y lingüísticas de los Estados miembros, ser aceptado por la comunidad de Internet y asegurar unos niveles de calidad suficientes frente al etiquetado incorrecto.

El informe, como el elaborado sobre el sistema de filtrado, parte de la constatación de que existe una gran diferencia entre lo que los consumidores quieren y lo que el mercado ofrece hoy en día. La mayor parte de los consumidores aprecian las ventajas y beneficios potenciales del autoetiquetado de páginas y del filtrado. Estos sistemas pueden permitir a cada usuario aplicar sus propios valores, aunque existen notables diferencias entre sus valores como grupo lingüístico, como país y como individuos. Sin embargo, los sistemas existentes no cumplen con las expectativas creadas por estos productos. El principal problema es que el material etiquetado es insuficiente, ya que el número de páginas etiquetadas es insuficiente. Los consumidores europeos buscan páginas en su propio idioma y sólo pocas páginas escritas en idiomas distintos del inglés han sido etiquetadas, aunque los usuarios de habla inglesa se

(30) Kerr, D. "INCORE, Final Report", Abril 2000, *http://www.incore.org/full.pdf*

encuentran con la misma situación. El número de páginas etiquetadas es inferior a lo requerido para generar confianza en los consumidores en los sistemas existentes. En segundo lugar, los consumidores requieren que el etiquetado incorpore más elementos que los que actualmente se catalogan, lo que requerirá unos programas más complejos, que tengan en cuenta esta demanda.

La complejidad de estos sistemas hace necesario que se establezcan sistemas de ayuda a los usuarios para manejar la complejidad de las clasificaciones a través de perfiles ya elaborados por terceros independientes. Esto implica que exista una posibilidad de elegir de un grupo de fuentes dentro de cada grupo nacional o lingüístico. Además, el estudio sugiere también la necesidad de que se de a los usuarios la posibilidad de bajarse de Internet listas verdes de páginas aceptables para sus navegadores.

Los actuales sistemas de etiquetado y filtrado no son una herramienta práctica para el mercado europeo. El establecimiento de sistemas viables depende de que se incremente la cantidad de material catalogado a través de un sistema basado en el autoetiquetado o en el etiquetado por terceros. Además, es particularmente importante estimular el etiquetado de páginas en idiomas distintos del inglés. A través de una buena campaña de información puede persuadirse a los proveedores de contenidos a que etiqueten sus contenidos. La expansión de este mercado depende también de la posibilidad de que los navegadores puedan usar perfiles predefinidos para la navegación y las listas verdes definidas por terceros.

El estudio sugiere que los productos sean diseñados de manera que no supongan un coste adicional para el usuario y mantengan el control sobre los juicios de valor en manos del cliente y asocien estos sistemas con mecanismo para bajar listas verdes o blancas de sitios de internet de confianza para los consumidores y de su elección. El sistema que reciba el apoyo de la Comisión debería permitir a los usuarios bajarse de internet e instalar fácilmente perfiles que se ajusten a sus preferencias o tener la posibilidad de completar la información recibida del autoetiquetado a través de información recibida de terceros. Finalmente, es preciso que exista un organismo de estandarización internacional que garantice la interoperabilidad.

En la primavera de 1999, un grupo de empresas y asociacio-

nes internacionales presentes en internet crearon la Asociación para la clasificación de informaciones de internet (*Internet Content Rating Association – ICRA*[31]) como una organización independiente sin ánimo de lucro. La misión de ICRA es desarrollar, aplicar y gestionar un sistema de autoclasificación voluntario, de aplicación internacional, que proporcione a los usuarios de internet en todo el mundo la posibilidad de limitar el acceso a contenidos que consideran nocivos, especialmente para los menores.

Finalmente merece una reflexión el sistema de filtrado concebido para Internet en relación a otros medios de control parental de la información en otros sectores cercanos a Internet. Tanto las instituciones comunitarias como Estados Unidos estudian la oportunidad de introducir sistemas de control parental en la televisión digital (*tecnología v-chip*). Lo cierto es que debería estudiarse el impacto que una regulación en tal sentido tendría respecto a la competencia entre la televisión digital y el sector de las empresas de contenidos en internet. Si el sistema de filtrado en Internet se sigue considerando como un sistema voluntario, mientras que se introducen sistemas obligatorios de control parental en la televisión digital, esto podría introducir distorsiones de competencia entre los dos sectores, que cada vez más compiten entre sí. La Asociación Europea de radiodifusión digital (DVB) considera que tratar de introducir un nuevo sistema técnico para ayudar a los padres a ejercer un control que sólo sea aplicable a la radiodifusión digital distorsionaría sin necesidad el mercado de las tecnologías de transmisión, ya que supondría para los organismos de radiodifusión tradicionales y los distribuidores de radiodifusión una situación de competitividad en desventaja frente a internet. En su opinión, cualquier sistema nuevo que contribuya al control de los padres debe aplicarse proporcionalmente a todos los canales de recepción de informaciones en el hogar. Deben superarse los retos respecto a la protección de los menores y de la dignidad humana en todos los medios, ya sea internet, la radiodifusión, los videojuegos o los soportes como cintas de vídeo y DVD. Es necesario realizar nuevos esfuerzos por conseguir un enfoque coherente, especialmente debido a que la convergencia continuará aumentando con la televisión por internet, la radiodifusión interactiva o la descarga de videojuegos de internet.

(31) *www.icra.org*

2.3 El establecimiento de líneas directas.

Una tercera línea de actuación del Plan de Acción se refiere a la creación de un entorno más seguro mediante el establecimiento de una red europea de líneas directas (INHOPE) y de vínculos entre esta red y las líneas directas de terceros países.

En casi todos los Estados miembros se han creado o se están estableciendo líneas directas para tramitar las reclamaciones sobre contenidos ilícitos o nocivos, y en España, según el informe de la Comisión[33] se prevé el establecimiento de una línea de estas características. Ya existen líneas directas asociadas a la Red europea de líneas directas INHOPE[34] –financiada por la Comisión y que forma parte del Plan de acción-en seis Estados miembros (Austria (ISPA), Alemania (FSM, Newswatch, jugendschutz.net), Francia (AFA-France), Irlanda (Hotline), Países Bajos (Meldpunt) y Reino Unido (IWF). España está en proceso de incorporarse a esta red. En Suecia, los grandes operadores disponen de departamentos de detección de abusos y se está facilitando a la policía la información disponible sobre contenidos ilícitos; además, el defensor del pueblo proporciona ayuda y apoyo a los usuarios de internet en lo referente tanto a problemas técnicos como a informaciones, y se ha creado una línea directa especial denominada «Salven a los niños».

IV. LA CRECIENTE PRESENCIA DE MATERIAL RACISTA Y XENOFOBO EN INTERNET.

Se está produciendo un aumento dramático de toda la clase de propaganda racista y xenófoba en internet. Las disposiciones de la Unión Europea sobre cibercrimen que han sido analizadas hacen todas mención a este preocupante fenómeno. Algunos expertos incluso hablan de una “comunidad electrónica del odio”. En 1997 La Asamblea General de los Naciones Unidas adoptó la resolución 51/81 que estableció un seminario sobre el papel del Internet en la perpetuación o la eliminación del racismo y de la discriminación racial. Esta conferencia exploró las características de este tipo de propaganda en la red y qué se está haciendo para oponerla.

(33) Comisión Europea, Informe de la evaluación de la Comisión al Consejo y al Parlamento europeo sobre la aplicación de la recomendación del Consejo de 24 de septiembre de 1998 sobre la protección de los menores y la dignidad humana 27.02.2001,COM(2001) 106 final

http://europa.eu.int/eur-lex/es/com/cnc/2001/com2001_0106es01.pdf

(34) *http://www.inhope.org*

La aplicación de las leyes nacionales contra el racismo y la xenofobia se enfrenta a problemas derivados de la naturaleza global de Internet y a la distinta estrategia seguida por los países para combatir el racismo y la xenofobia[35]. Así, si para la mayoría de los países que han ratificado la Convención Internacional sobre la Eliminación de todas formas de Discriminación Racial, el discurso racista y xenófobo y el revisionismo está perseguido, en países como Estados Unidos o Australia se trata de un contenido protegido por la Constitución, por lo que no puede prohibirse su publicación. Si en la época previa a Internet la regulación de esta materia de un determinado país tenía relevancia tan sólo para ese país, la accesibilidad inmediata a todo tipo de material en la Red en cualquier parte del mundo y desde cualquier punto del planeta supone una dura prueba para aquellos países como España que han optado por ilegalizar este tipo de material. La existencia de normas penales muy estrictas en la Europa comunitaria poco puede hacer contra la proliferación de páginas de Internet de grupos racistas, neonazis, revisionistas o xenófobos en servidores de Estados Unidos o Australia, como *stormfront*, contra la venta de libros cuya distribución y venta está prohibida en Europa como *Mein Kampf*, en librerías electrónicas como Amazon.com o contra la venta de recuerdos y parafernalia nazi en páginas de subasta como ebay.com[36].

Internet se ha convertido en un lugar perfecto para toda clase de grupos organizados que fomentan el odio racial. Estos grupos crean sitios internet en nombres de dominio genéricos como .org, cuya política de registro de nombres de dominio de segundo nivel es muy permisiva, situadas en Estados Unidos y creando centenares de conexiones internacionales a otras fuentes de la información racista y xenófoba. En este tipo de páginas se utiliza todo tipo de estrategias para seducir a futuros miembros de estos grupos, tales como publicación de música con contenido racista, videojuegos de duro contenido antisemita y comercialización de libros, ropa, y

(35) Sobre estas cuestiones, M.L. Fernández, "The Internet, a new horizon for race hatred?" *Collected Courses of the Academy of European Law 2000* (Oxford University Press, en prensa)

(36) El 4 de mayo de 2001, ebay ha anunciado que desde el 17 de mayo no subastará material ligado a crímenes en los últimos 100 años. El sitio ya había bloqueado el acceso a este tipo de materiales en Alemania y Francia. "eBay retira la subasta de material

criminal" *El País*, jueves 10 de mayo de 2001.
parafernalia nazi. En páginas como la de *stormfront*, auténtico portal de entrada al mundo racista, pueden encontrarse páginas dedicadas a niños, con peligrosos videojuegos y captación de datos personales de menores. La comunicación barata, instantánea y mundial sin exposición física que permite internet contribuye al éxito de este tipo de páginas

V. LA PROTECCION DE DATOS EN INTERNET.

Internet se está convirtiendo en un canal importantísimo para el suministro de bienes o servicios. Los datos ofrecidos por los interesados para obtener determinados servicios son tales, por cantidad y calidad, que permiten toda una serie de empleos secundarios, particularmente remunerativos, para los gestores de sistemas interactivos. Estos pueden elaborar perfiles de consumo individual o familiar y análisis de preferencias, informaciones estadísticas a partir de las informaciones obtenidas gracias a la oferta de servicios[37]. La dependencia cada vez más estrecha entre la provisión de datos personales y el disfrute de servicios en Internet compromete la intimidad y secreto de los datos referentes a la vida privada. Además, el usuario se encuentra en una situación de evidente desigualdad de poder respecto al proveedor de servicios, por lo que no puede hablarse en rigor de un consentimiento libre para las transacciones que se refieren a sus datos personales. Algunos programas de Internet permiten la creación de "rastros de cliqueo" del usuario de Internet. Los "rastros de cliqueo" consisten en información sobre el comportamiento, la identidad, el recorrido efectuado o las elecciones expresadas por la persona al visitar el sitio web y contienen los vínculos por los que ha pasado un usuario y que están registrados en el servidor web. La riqueza, fiabilidad y tempestividad de los datos recogidos a través de Internet agravan este problema, que se centra en la creación de una nueva mercancía: perfiles individuales y colectivos de usuarios. Cuanto mayor extensión tiene la red de servicios, más crecen las posibilidades de interconexión entre ficheros, o bancos de datos y la diseminación internacional de la información recogida. A dondequiera que se accede en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada.

(37) Rodotà, S.: *Tecnologia e Diritti* Ed. Il Mulino, 1994, p. 47.

Actualmente una ingente cantidad de datos personales de los usuarios de Internet está siendo recogida sin el consentimiento o conocimiento previo del dueño de los datos gracias al proceso invisible de los datos. Las compañías de publicidad a través de internet procesan estos datos que se van acumulando a través de distintos procedimientos como las *cookies* o los enlaces invisibles y generan publicidad individualizada según el perfil previamente elaborado. Una sola de estas compañías puede generar hasta un billón de *banners* de publicidad personalizados al día. A través del enlace invisible a una de estas compañías en una página de internet como un buscador, esta página abrirá una conexión http independiente con la compañía de publicidad. El navegador que esté usando el usuario de internet transmitirá automáticamente un flujo de datos que le son solicitados a través del diálogo http, tales como la dirección del ordenador desde el que está navegando el usuario, las palabras que el usuario está buscando en el buscador, la marca, versión e idioma del navegador(por ejemplo Internet explorer 4.02, español, sistema operativo windows 98). La *cookie* de identificación, que puede haber sido colocada por la compañía previamente a través del enlace invisible, es capaz de transmitir instantáneamente todo tipo de información sobre el usuario tal como nombre, dirección de correo electrónico, páginas visitadas, noticias consultadas en internet, teclas que han sido presionadas, palabras clave utilizadas en la búsqueda... El usuario medio de internet desconoce la existencia de esta maquinaria que acumula sus datos y el hecho de que al acudir a una página de Internet con el navegador, es decir, al teclear una dirección http, gran parte de la publicidad de la página, de los banners, no se origina en la página que está visitando, sino en la compañía de publicidad, que va elaborando un perfil sobre su persona cada vez más preciso, gracias a los datos que el usuario, sin saberlo, va incorporando a las *cookies* que han sido instaladas de forma invisible en su disco duro y que transmitirán lealmente la información que "espían" y acumulan. Un ejemplo reciente y potencialmente más dañino para la intimidad son los llamados "programas E.T", por que una vez instalados en el disco duro del usuario y encontrada y recopilada la información que se les ha pedido hacen lo que hacía el simpático personaje de Steven Speilberg: llamar a casa. Se trata de unos instrumentos que recogen y procesan de forma invisible los datos del usuario de internet, enviándolos a la empresa que recolecta esos datos. Se trata del instrumento más poderoso de ela-

boración de perfiles individuales existente, de tal forma que la compañía Amazon.com pagó 250 millones de dólares por una base de datos generada con este sistema[38].

La acumulación de datos personales en internet y la elaboración de perfiles por las compañías de ciberpublicidad tiene un valor estratégico en el crecimiento de las empresas de comercio electrónico. Es preciso mencionar que la recogida de datos se produce sin coste para las empresas, ya que los usuarios suelen proveer estos datos ellos mismos al rellenar formularios para acceder a servicios. En este sentido, y dejando al margen el proceso invisible de datos que ha sido mencionado, es también observada con preocupación el empleo secundario que se está dando a los datos recabados con consentimiento del usuario o bien aportados por él mismo a través de formularios. Los nuevos mecanismo llamados de minería de datos *(datamining)* son capaces de extraer perfiles de comportamiento del usuario de internet de una lista de páginas de internet visitada por el usuario. La combinación del proceso invisible de datos y el uso secundario dado a los datos recogidos con el consentimiento del usuario dan como resultado perfiles de usuario sumamente detallados, que permiten el envío de mensajes de publicidad *(banners)* que son lo más cercanos posibles a los intereses de los usuarios de Internet.

Los bancos de datos de clientes de estas compañías se han convertido también en una fuente de ingresos adicional cuando la compañía suspende pagos. Estos perfiles incluyen nombres, direcciones, información sobre facturas, perfiles de consumo y fechas de cumpleaños de parientes. La compañía puede ahorrarse hasta 100 dólares por la captación de cada cliente, si utiliza los útiles servicios de las compañías de *telemarketing*.

(38) Grupo de trabajo sobre Protección de las personas en lo que respecta al tratamiento de datos personales, Documento de trabajo: "Intimidad en internet- Una visión integrada de la protección de datos en línea" de 21 de noviembre de 2000
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.pdf
Véase también del mismo grupo, "Documento de trabajo: Tratamiento de datos personales en Internet" de 23 de febrero de 1999, *http://europa.eu.int/comm/internal_mar-*

ket/en/media/dataprot/wpdocs/wp27es.pdf

La Directiva 95/46/CE, de 24 de octubre, relativa a la protección de la personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos[39] armoniza las condiciones de protección del derecho a la intimidad en relación con la protección de datos personales, consagrado en las constituciones o sistemas jurídicos de los Estados miembros. Esta Directiva otorga contenido y amplía los principios incluidos en el Convenio Europeo para la Protección de los Derechos Humanos de 4 de noviembre de 1950 y en el Convenio 108 del Consejo de Europa, de 28 de enero de 1981 para la protección de las personas en relación con el tratamiento automático de datos personales. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal realiza la incorporación a nuestro ordenamiento interno de la Directiva 95/46/.

Además, la Directiva 97/66/CE del Parlamento y del Consejo, de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[40] adapta las disposiciones de la Directiva 95/46 al sector de telecomunicaciones. Ambas Directivas se aplican al tratamiento de los datos personales en Internet, incluidos los datos sobre tráfico relacionados con abonados y usuarios.

El tratamiento de los datos personales en Internet debe respetar los principios de protección de datos al igual que en el mundo no conectado o fuera de línea. Esto no constituye una limitación de la utilización de Internet, sino que, por el contrario, forma parte de los requisitos fundamentales destinados a garantizar la confianza de los usuarios en el funcionamiento de Internet y los servicios que se facilitan mediante esa red. La protección de datos en Internet es, por tanto, una condición indispensable para el desarrollo del comercio electrónico[41].

(39) Directiva 95/46/CE, de 24 de octubre, relativa a la protección de la personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

DOCE n° L 281 de 23 de noviembre de 1995, *http://www2.echo.lu/legal/es/protedat/directiv/directiv.html*

(40) Directiva 97/66/CE del Parlamento y del Consejo, de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, DOCE n° L 024 de 30 de enero de 1998, *http://europa.eu.int/eur-lex/es/lif/dat/1997/es_397L0066.html*

(41) Grupo de trabajo sobre Protección de las personas en lo que respecta al tratamiento de datos personales, "Documento de trabajo: Tratamiento de datos personales en Internet" de 23 de febrero de 1999,

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp27es.pdf

En el marco de la tendencia a la autorregulación que caracteriza a Internet, la Directiva 95/46/ establece en su artículo 27 que los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas. En nuestro país puede destacarse la iniciativa de la Asociación Española de Comercio Electrónico[42], para la creación del Código Ético de protección de Datos Personales en que ha recibido el respaldo y la aprobación de la Agencia de Protección de datos. Al Código pueden adherirse todas las empresas que lo deseen, que de este modo están vinculadas por él. Como contrapartida, las empresas pueden utilizar el sello de garantía de protección de datos. El Código establece la obligación de todas aquellas empresas que capten datos personales de informar sobre el uso que hacen de esos datos. Antes de cualquier transferencia de datos deberán advertir a los dueños de esos datos para darles la oportunidad de prohibir la cesión. Uno de los principios del Código Ético es permitir las mayores facilidades para negarse a la recogida o cesión de datos. También se establecen medidas específicas para garantizar que la publicidad sólo se va a enviar a clientes que no hayan manifestado su oposición. Las ofertas en línea deben identificarse claramente como tales, revelando asimismo la identidad del anunciante. Donde sea posible, los consumidores deberán disponer de la opción a negarse a recibir ofertas y publicidad través del correo electrónico. El Código incluye también disposiciones sobre la captación de datos de menores. El control del cumplimiento de las normas del código ético se encomienda al Comité de protección de datos de la AECE, creado por el propio Código.

Se ha establecido un grupo de coordinación con la industria para profundizar en el estudio de las cuestiones relativas a la información sobre localización de quienes efectúan llamadas desde móviles y para formular propuestas a la Comisión. Sobre la base de estas consultas, en el primer semestre 2001 la Comisión podría proponer cualquier otra medida necesaria para completar el marco regulador.

(42) Asociación Española de Comercio Electrónico, Código Ético de protección de

Datos Personales en Internet, *http://www.aece.org/corporativo/codigoetico.doc*

1. La protección de datos por las empresas de la Red en los Estados Unidos y en la Unión Europea. El principio de "puerto seguro" y el acuerdo entre el Gobierno norteamericano y la Comisión Europea.

La Directiva 95/46 establece reglas para garantizar que los datos personales sólo van a ser transferidos a terceros países que garantizan una protección a los datos personales similar a la que se garantiza en la Unión Europea, salvo que la transferencia se recoja en una excepción del artículo 26. Si un país no garantiza un nivel adecuado de protección, los Estados miembros de la Unión Europea y la Comisión deben informarse recíprocamente. Cuando la Comisión compruebe que un tercer país no garantiza un nivel de protección adecuado los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

Debido a las enormes implicaciones que estas normas tienen para las empresas, el artículo 26 permite a las compañías establecer ellas mismas mecanismos que garanticen que el flujo de datos respeta los principios de la Directiva, para las que se puede autorizar la transmisión de datos fuera de la Unión Europea. Las soluciones técnicas, como los mecanismos que informan a los consumidores y obtienen su consentimiento para el procesamiento de datos, serán especialmente útiles para evitar la prohibición de exportación de datos[43]. En Estados Unidos la protección de datos tiene lugar a través de normas de autorregulación del sector, y no a través de una norma del Estado. Ello llevó a la Comisión Europea a declarar que Estados Unidos no era una nación segura a efectos de la Directiva, con lo que se imposibilitaba la transmisión de datos personales desde Europa a Estados Unidos[44].

(43) Comisión europea, Documento informativo "Data Protection: Background Information",
http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm

(44) Grupo de Trabajo sobre Protección de las Personas en lo que respecta al tratamiento de datos personales. Dictamen 7/99, de 3 de diciembre de 1999, relativo al nivel de protección de datos previsto por los principios de «puerto seguro» hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EE.UU. *http://www.europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp27es.pdf*

2000.

Tras más de dos años de negociaciones, la Comisión ha llegado a un acuerdo provisional con el Gobierno de Estados Unidos el 14 de marzo de 2000 sobre el mecanismo de "puerto seguro" propuesto por Estados Unidos para garantizar la protección de datos de las empresas norteamericanas en Internet[45]. El acuerdo provisional permite a las empresas norteamericanas continuar recibiendo datos personales desde Europa si respetan el principio de puerto seguro. El acuerdo provisional no cubre los servicios financieros que aún está en fase de negociación. Se espera poder formalizar el acuerdo en los meses de junio o julio. El grupo de trabajo ha dado su visto bueno a un Proyecto de Decisión de la Comisión, de 27 de marzo de 2001 sobre cláusulas contractuales estándar en Internet para la transferencia de datos personales a terceros países[46]. Con esta futura decisión se pretenden aligerar los trámites necesarios para la transmisión de datos a terceros países acogidos a la doctrina del puerto seguro, diferenciando los datos más comprometedores de aquellos que representan un escaso riesgo para la intimidad de las personas, a través de cláusulas contractuales estándar que se detallan en le anexo a esta futura Decisión. De este modo, las compañías de comercio electrónico podrán transmitir los datos de sus clientes europeos a esos terceros países recabando su consentimiento a través de este tipo de cláusulas estándar.

2. La protección de datos en las comunicaciones eléctricas.

Otra importante Directiva es la 97/66/CE del Parlamento y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Esta acción de la Comunidad pretende dar un primer paso armonizador frente a las necesidades específicas en materia de protección de datos personales e intimidad que generan los nuevos servicios interactivos que se prestan a través de la Red Digital de Servicios integrados y los teléfonos móviles. Como se ha dicho, los riesgos más importantes que presentan los servicios interactivos tienen que ver con el almacenamiento y el tratamiento

(45) Grupo de Trabajo sobre Protección de las Personas en lo que respecta al tratamiento de datos personales. Dictámen 4/2000, de 16 de mayo, sobre el nivel de protección que proporcionan los "principios de puerto seguro", *http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp32es.pdf*

-Dictamen 3/2000, de 16 de mayo, sobre las negociaciones entre la Unión Europea y Estados Unidos sobre los principios de "puerto seguro",

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp31en.pdf

(46) Proyecto de Decisión de la Comisión, de 27 de marzo sobre cláusulas contractuales estándar en Internet para la transferencia de datos personales a terceros países

http://europa.eu.int/comm/internal_market/en/media/dataprot/news/clausesdeci-

sion.htm
informático de datos relativos a abonados y usuarios. La Directiva contiene disposiciones que conciernen a varios temas: seguridad de la información transmitida a través de las redes públicas de comunicación; confidencialidad de las comunicaciones; limitaciones a la capacidad de proceso de datos sobre el tráfico y los recibos por los proveedores de los servicios; opciones del usuario sobre la identificación de la línea llamante y la línea conectada; protección de los consumidores frente a llamadas automáticas o llamadas no solicitadas; y derecho de los abonados de no aparecer en listados públicos.

La Directiva establece que los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de los servicios e informar a los abonados al servicio de todo riesgo concreto de violación de la seguridad de la red. En el caso concreto de violación de la seguridad de la red, el proveedor de un servicio de telecomunicaciones deberá informar a los abonados sobre ese riesgo (art. 4).

Por lo que se refiere a la confidencialidad de las comunicaciones, se establece que los Estados miembros destinatarios de la Directiva deberán garantizar la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicación. En particular, deberán prohibir la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, salvo que estén autorizadas legalmente (artículo 5). Los datos de tráfico relacionados con los usuarios y abonados para establecer comunicaciones y almacenados por el proveedor de la red deberán destruirse o hacerse anónimos al acabar la comunicación. Además, el tratamiento de los datos de tráfico y facturación deberá limitarse a las personas que actúen bajo las órdenes del proveedor de la red, que se ocupe de la gestión de la facturación o tráfico, solicitudes de información de los clientes, detección de fraudes y promoción comercial de los propios servicios del proveedor (artículo 6). Las garantías que establece la directiva frente al proceso de los datos de tráfico pueden pronto verse afectas con el actual proyecto de ciberdelito auspiciado por le Consejo de Europea, ya que, como se ha visto, el actual proyecto prevé que pueda imponerse a los proveedores de servicios de comunicaciones electrónicas el almacenamiento de los datos de tráfico hasta 60 días. En opinión del Grupo para la protección de datos personales, la mejor manera de reducir los ataques a la intimidad de las personas en las comunicaciones electrónicas es que los datos de tráfico no deberían ser almacenados por los operadores de telecomunicaciones y los proveedores de servicios de internet para sus super-

visión por las fuerzas de seguridad y, tan sólo, deberían almacenarse para elaborar las facturas[47].

Esta Directiva ha sido incorporada a nuestro ordenamiento a través de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, en particular en el Título III, capítulo III "Secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculados con las redes y servicios de telecomunicaciones". Actualmente existe una Propuesta de Directiva para la protección de la intimidad en las comunicaciones electrónicas, de 12 de julio de 2000[48], que debería modificar la Directiva 97/66 con el fin de considerar incluidos los prestadores de servicios en Internet. La propuesta ya no se refiere a los servicios de telecomunicaciones, sino a los servicios de comunicación electrónicos.

Una respuesta a la creciente demanda de seguridad en las comunicaciones es la encriptación. La encriptación es el arte de crear y usar métodos para disfrazar mensajes usando códigos, algoritmos y otros métodos de tal modo que sólo las personas que conocen esos códigos pueden acceder a la información.

Los principales aspectos que garantiza la encriptación son la confidencialidad, la integridad y la autenticidad de la información. El servicio que se asocia más frecuentemente con la encriptación es la transformación de la información de manera que resulta ininteligible para todo aquel que no sea el destinatario de la misma. La encriptación otorga una total seguridad a estas transacciones. No sólo evita que los mensajes, de cualquier tipo que sean, puedan ser conocidos por personas ajenas a la comunicación, sino que otorgan una fiabilidad absoluta sobre la veracidad de esos datos. Por lo que se refiere a la integridad de la información transmitida, se trata de un servicio garantizado por la encriptación, que permite al usuario detectar si la información ha sido alterada durante su transmisión o almacenaje. Relacionada íntimamente con la integridad, se halla la garantía de la autenticidad de la información. La autenticación permite identificar al emisor de la información. La autenticación pasa frecuentemente a través de la asociación de una clave de encriptación con un usuario, lo que a veces se conoce como firma digital.

(47) Grupo de trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, Dictamen 4/2001, de 22 de marzo, sobre el proyecto de Tratado del Consejo de Europa sobre Cibercrimen

(48) Propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, COM(2000) 385, 12 de julio de 2000.

En el marco de eEuropa se ha adoptado un nuevo Reglamento comunitario que regula este tipo de productos[49]. El Reglamento sobre productos de doble uso acaba con la mayor parte de los controles a la exportación intracomunitaria de este tipo de productos, al igual que establecer un sistema general de licencias que permitan la exportación fuera de la Unión Europea.

3. La recepción de correo no solicitado.

Un estudio preparado por la Comisión asegura que el *spamming*, es decir, la recepción de correo no solicitado cuesta a los usuarios de Internet del mundo 10 billones de euros al año[50]. Según este estudio, que se concentra en el mercado más desarrollado, el de Estados Unidos, la industria de la publicidad a través de Internet trabaja en sistemas de acumulación e intercambio de datos personales a través del permiso expreso del usuario. La protección otorgada contra los mensajes no solicitados en la Unión Europea en las directivas comunitarias es aplicada de diferentes maneras en los distintos países comunitarios. La protección consiste en sistemas de inscripción voluntaria, es decir, en solicitudes formales para recibir los mensajes (*opt ins*), o en exclusión voluntaria, por ejemplo, una casilla indicando que no se desea recibir este tipo de mensajes (*opt outs*). La Directiva 2000/31/CE de Comercio electrónico permite a los Estados optar por cualquiera de los dos sistemas. El Anteproyecto de ley de incorporación de esta Directiva, en una primera versión de 18 de enero de 2001 había optado por el sistema de exclusión voluntaria en el artículo 22.

La rapidez con la que evoluciona la tecnología ha propiciado que la Comisión propusiera en julio de 2000 la revisión de la actual Directiva (97/66) de protección de datos y de la intimidad en el sector de las telecomunicaciones. La propuesta se inclina a favor de la primera opción, es decir, de un sistema de opt-in o de adscripción voluntaria. La nueva posición de la Comisión es reforzada por el

(49) Reglamento (CE) nº 1334/2000 del Consejo, de 22 de junio de 2000, por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnología de doble uso

http://europa.eu.int/eur-lex/es/lif/dat/2000/es_300R1334.html

(50) Gauthronet S. y otros "Comunicaciones comerciales no solicitadas y protección de datos" enero de 2001

http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamsumes.pdf

estudio en el que se aprecia que, desde el punto de vista de la industria, el envío de correo basado en el consentimiento, constituye un método más eficaz y viable de recolección de datos. Según el estudio, los sistemas de adscripción voluntaria u opt-ins estimulan la confianza de los consumidores. Las diferencias existentes, debidas a la incorporación de las directivas pueden convertirse en barreras a la libre circulación de datos en el Mercado único. La última versión del Anteproyecto de Ley de Servicios de la Sociedad de la Información y de comercio electrónico[51], de 30 de abril de 2001 ha acogido este sistema, ya que prohíbe la remisión de publicidad por correo electrónico u otras vías de comunicación electrónica equivalentes, salvo que el destinatario haya dado su consentimiento en el artículo 21. Con ello, se persigue erradicar la práctica del envío indiscriminado de mensajes publicitarios por medios electrónicos a destinatarios de correo electrónico o de otros dispositivos electrónicos equivalentes.

(51) *http://www.setsi.mcyt.es/novedad/antepr_elect_300401.doc*