5.8 El CESE considera que el Reglamento 4056/86 debería ser derogado y sustituido por un nuevo Reglamento de la Comisión sobre conferencias marítimas que garantice una exención por categorías. El nuevo régimen debería respetar estrictamente los criterios establecidos por el Tribunal Europeo de Primera Instancia y la Comisión (por ejemplo, el caso TACA). El sistema de conferencias debería también mantenerse para defender la competitividad de los navieros comunitarios por todo el mundo. Al tiempo que para los transportadores grandes pueden resultar apropiadas las «alianzas» y otros tipos de acuerdos de cooperación, los transportadores pequeños y medianos aún necesitan conferencias para mantener sus cuotas de mercado, especialmente en el comercio con países en vías de desarrollo. La abolición de la exención puede tener efectos anticompetitivos para estos pequeños transportadores, consolidando así la posición dominante de los más grandes.

5.9 Convendría que la Comisión utilizara este periodo transitorio provisional para supervisar la evolución del sector del transporte marítimo regular, incluida la tendencia a la consolidación. Además, la Comisión debería realizar consultas con otros países (OCDE) con vistas a hallar un sistema alternativo adecuado que sea compatible a escala mundial.

5.10 El CESE aprueba las propuestas del Libro Blanco relativas al tratamiento de los servicios de cabotaje y de *tramp* dado que en la gran mayoría de los casos en estos sectores no causaría problemas de competencia. Sin embargo, en aras de la seguridad jurídica, se pide a la Comisión que provea una orientación jurídica relativa a la autoevaluación de grupos y de transportes especializados en lo que se refiere a su compatibilidad con el artículo 81 del Tratado CE.

5.11 El CESE espera aportar su contribución al seguimiento del ejercicio de reflexión lanzado por el Libro Blanco.

Bruselas, 16 de diciembre de 2004.

La Presidenta
del Comité Económico y Social Europeo
Anne-Marie SIGMUND

Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Decisión del Parlamento Europeo y del Consejo por la que se crea un programa comunitario plurianual para el fomento de un uso más seguro de Internet y las nuevas tecnologías en línea»

(COM(2004) 91 final — 2004/0023 (COD))

(2005/C 157/24)

El 26 de marzo de 2004, de conformidad con el artículo 153 del Tratado constitutivo de la Comunidad Europea, el Consejo decidió consultar al Comité Económico y Social Europeo sobre la propuesta mencionada.

La Sección Especializada de Transportes, Energía, Infraestructuras y Sociedad de la Información, encargada de preparar los trabajos en este asunto, aprobó su dictamen el 5 de octubre de 2004 (Ponente: Sr. RETUREAU, Coponente: Sra. DAVISON).

En su 413º Pleno de los días 15 y 16 de diciembre de 2004 (sesión del 16 de diciembre de 2004), el Comité Económico y Social Europeo ha aprobado por 147 votos a favor y 1 abstención el presente Dictamen.

1. **Resumen del proyecto de dictamen**

1.1. La Comisión propone el lanzamiento de un nuevo proyecto del plan de acción «Safer Internet» (Internet más segura), pero reforzándolo habida cuenta de los rápidos cambios de la sociedad de la información en lo que se refiere a las redes de comunicaciones. De esta manera, el proyecto se ha bautizado «Safer Internet plus» (2005-2008).

1.2. Además de la propuesta de Decisión del Parlamento y el Consejo presentada por la Comisión, el Comité ha examinado la evaluación *ex ante* de Safer Internet plus (2005-2008) contenida en el documento de trabajo de la Comisión *(«Commission Staff working paper»)* SEC(2004) 148 y COM(2004) 91 final. Apoya la ampliación del ámbito de aplicación del nuevo plan de acción y sus objetivos, que tienen en cuenta la rápida evolución y la diversificación de los medios de acceso en línea y el muy rápido crecimiento del número de accesos de alta velocidad y de conexiones permanentes. En sus observaciones generales y particulares formula sugerencias complementarias de acciones políticas y normativas, en particular:

— normas técnicas y jurídicas (obligatorias y de carácter voluntario);

— la educación-formación de los usuarios;

— las obligaciones de los proveedores de espacios y de acceso y de otros agentes (compañías de tarjetas de crédito, motores de búsqueda...);

— la responsabilidad de los autores de programas informáticos y proveedores de medios de seguridad;

— la protección de las personas vulnerables contra el fraude o las informaciones dudosas (estafas diversas, venta «libre» de medicamentos activos, consejos o curaciones ofrecidos por personas sin autoridad médica...)

2. **Propuestas de la Comisión (resumen)**

2.1. El programa propuesto tiene por objeto promover una utilización segura de Internet y de las tecnologías en línea para el usuario final, en particular, para los niños y los jóvenes, tanto en el hogar como en la escuela. A este fin, está previsto cofinanciar proyectos concebidos por asociaciones y otros grupos (equipos de investigadores, diseñadores de programas informáticos, centros de enseñanza...) que permitan desarrollar medios de protección: por ejemplo, *hot lines,* mecanismos contra la publicidad no solicitada, contra los virus informáticos, filtros de navegación inteligentes....)

2.2. El plan anterior para una Internet segura (1999-2002) fue prolongado hasta el período 2003-2004.

2.3. El sitio Internet de la Comisión indica los proyectos ya realizados en el marco del proyecto *Safer Internet* hasta finales de 2003 ([1]).

2.4. La propuesta actual (2005-2008) se extiende también a los nuevos medios de comunicación en línea, para los cuales pretende reforzar la lucha contra contenidos ilícitos y perjudiciales, incluidos los virus y otros contenidos nocivos o no solicitados (*spam*).

2.5. Para las instituciones comunitarias, este refuerzo de la lucha se justifica por varias razones entre las que cabe destacar:

— el rápido desarrollo de las conexiones de alta velocidad de larga duración o permanentes de particulares, empresas, administraciones e instituciones privadas (ONG);

— la diversificación de los medios y métodos de acceso a Internet y a nuevos contenidos en línea, muchos de ellos no solicitados (*correo electrónico, SMS*), y el mayor poder atractivo de los contenidos (multimedia);

— la dramática expansión de contenidos no solicitados y potencialmente peligrosos o inadecuados crea nuevos peligros para el público en general (virus: invasión de los espacios de almacenamiento, uso indebido o destrucción de datos, utilización no autorizada de los medios de comunicación de la víctima; contenidos no solicitados (*spam*): uso abusivo de la banda pasante y de los espacios de almacenamiento, invasión de los buzones electrónicos, lo que bloquea u obstruye la utilización útil de Internet y las comunicaciones y acarrea costes importantes no sufragados por los «contaminadores» sino por el usuario final) y para algunas categorías importantes de usuarios, como los niños (*spam* de contenido explícitamente sexual, mensajes inadecuados y propuestas de citas formuladas por pederastas en los espacios de debate directo (*chat rooms*);

— contenidos inadecuados fácilmente accesibles para los niños debido a la muy relativa eficacia de los medios actuales de filtrado de que disponen en general las personas responsables de los niños.

2.6. El objetivo principal del programa es la protección de los niños y el respaldo a quienes son responsables de ellos (padres, profesores, educadores, etc.) o defienden sus intereses morales y su bienestar. El programa atañe pues a las ONG del sector social, de los derechos del niño, de la lucha contra el racismo, la xenofobia ([2]) y cualquier otra forma de discriminación, de defensa de los consumidores y de defensa de las libertades civiles, etc.

2.7. Interesa también a los Gobiernos, a sus autoridades legislativas, judiciales y policiales y a los órganos de regulación. La legislación propiamente dicha y sus procedimientos deben adaptarse en consecuencia, y el personal correspondiente, en número suficiente, debe ser formado y equipado debidamente.

2.8. Interesa también a la industria, que necesita un entorno seguro para reforzar la confianza de los consumidores.

2.9. Las universidades y la investigación pueden orientar sobre el uso de los nuevos medios de comunicación por parte de los niños. La mejor manera de transmitir los mensajes relativos a la seguridad es dar a conocer los métodos que utilizan los transgresores en estos medios de comunicación, buscar nuevas soluciones técnicas y proporcionar un punto de vista independiente sobre la conciliación de los intereses afectados por los procedimientos de regulación y de autorregulación.

2.10. El programa tiene una doble dimensión. A nivel social, se centra en ámbitos donde la regulación y el mercado no estarían en condiciones, por sí solos, de garantizar la seguridad de los usuarios. A nivel económico, se trata de promover la utilización segura de Internet y de las tecnologías en línea creando un clima de confianza.

2.11. Se prevé una financiación de aproximadamente 50 millones de euros para desarrollar los medios técnicos y jurídicos, los programas informáticos y la información para luchar más eficazmente contra las invasiones de redes y terminales o su utilización fraudulenta por medio de contenidos no solicitados que pueden ser nocivos moral, social o económicamente.

([1]) http://www.europa.eu.int/information_society/programmes/iap/index_en.htm.

([2]) Estos temas corresponden a una petición previa del Comité.

3. **Observaciones generales del Comité**

3.1. El Comité recuerda sus posiciones previas sobre la protección de los niños en Internet y sobre el primer plan de acción ([1]). Acoge positivamente la propuesta de un nuevo plan de lucha contra contenidos ilícitos o nocivos en las comunicaciones en línea (véase más arriba el punto 1: «Resumen del proyecto de dictamen»). Apoya los objetivos y las prioridades del programa *Safer Internet plus* como uno de los mecanismos destinados a mejorar la seguridad en Internet. No obstante, el Comité destaca la extensa dimensión del problema y la necesidad de acciones internacionales y de regulación para afrontarlo.

3.2. Internet y las nuevas tecnologías de comunicación en línea (por ejemplo, los teléfonos móviles o las agendas de bolsillo conectables a funciones multimedia, en plena expansión), constituyen en opinión del Comité instrumentos fundamentales para el desarrollo de la economía del conocimiento y la economía y administración con soporte informático. Son instrumentos proteicos de comunicación de cultura, de trabajo y de ocio. Es, pues, primordial garantizar la seguridad y la continuidad del funcionamiento de las redes de comunicación, ya que se trata de un servicio público esencial que debe seguir siendo abierto, accesible y en el cual todos los usuarios deben tener confianza para que pueda desempeñar sus múltiples funciones en condiciones óptimas. La inclusión de información sobre la protección de Internet en los distintos programas *e-Europe*, en particular en la formación, constituiría un medio realmente prometedor, en términos de coste-eficacia, para llegar a un gran número de personas.

3.3. La libertad de expresión y de comunicación que caracteriza Internet viene facilitada por los costes relativamente poco elevados de las conexiones, incluida la de alta velocidad, que dan acceso a contenidos multimedia, cada vez más fácilmente. Sólo algunos países con marcado déficit democrático pretenden controlar las comunicaciones y los contenidos disponibles para sus nacionales, a base de una restricción permanente de las libertades. El Comité considera que es necesario garantizar una mayor seguridad conservando y promoviendo al mismo tiempo las libertades de información, comunicación y expresión.

3.4. Sin embargo, este espacio de libertad de expresión e información que es Internet también se utiliza –incluso más que los otros medios de comunicación– para actividades ilegales como la pederastia o la difusión de contenidos racistas y xenófobos; algunos contenidos pueden también resultar nocivos para determinados públicos, los menores de edad en particular, como la pornografía o los juegos de dinero (estos últimos están incluso prohibidos en algunos países) y distintas actividades delictivas (apropiación indebida de la banda pasante o utilización fraudulenta de datos y servidores). El Comité aprueba pues la extensión del plan de acción al conjunto de los medios de comunicación electrónicos que pueden ser objeto de accesos exteriores no solicitados u hostiles.

3.5. La regulación de este nuevo espacio en pleno crecimiento se ha vuelto compleja por su carácter de red internacional abierta y accesible por todos a partir de cualquier servidor o terminal de cliente libremente conectado desde prácticamente todos los países del mundo. Sin embargo, son numerosos los países que tienen aún una legislación ineficaz o insuficiente, que permite que sitios prohibidos en la Europa comunitaria prosigan sus actividades. Parece muy importante que la Unión Europea se pronuncie y actúe en favor de una acción internacional, en particular con los principales países donde está muy extendida la Internet de banda ancha –Norteamérica y Asia– con el fin de proteger a los más vulnerables y para luchar más eficazmente contra los contenidos no solicitados (*spam*), que amenazan el desarrollo de las comunicaciones por correo electrónico, y contra la propagación de virus, que debilitan el comercio electrónico. Aunque necesarios en el espacio comunitario, los medios que deben utilizarse han de insertarse también en un enfoque global.

3.6. Dado que no existen acuerdos internacionales, la prohibición de ciertos contenidos en algunos países puede ser incluso objeto de denuncia ante la OMC, en el marco de los TBT ([2]), por lo que esta cuestión debería tratarse en las negociaciones en curso ([3]).

3.7. La territorialidad del Derecho y la diversidad de las legislaciones nacionales constituyen un problema difícil de superar. El estado de la tecnología permite también los intercambios directos entre personas de ficheros de toda clase (P2P, *peer to peer*), incluidos ficheros criptográficos cuyo contenido es incontrolable: toda máquina o red en línea puede utilizarse para el almacenamiento y envío de contenidos cada vez más sofisticados, y es posible conectarse a cualquier servidor de manera anónima y sin dejar rastro alguno y utilizar medios de cifrado muy robustos e incluso «irrompibles».

3.8. La moda de las páginas personales y bitácoras (*weblogs*), el desarrollo de sitios comerciales o servicios financieros electrónicos, la multitud de sitios informativos, educativos, científicos o técnicos, pero también pornográficos o de juegos de dinero, etc., hacen que existan cientos de millones de sitios en todo el mundo. Con todo, puede ejercerse un cierto control en la elaboración del índice de las palabras clave por los motores de búsqueda. La creación de conexiones directas y de sitios de envíos automáticos de contenidos, como los *spam* es también controlable por los proveedores de acceso a Internet (FAI): la publicidad y otros contenidos no solicitados así enviados pueden tener un carácter nocivo de carácter general (uso indebido de la banda pasante, virus), o particular para algunos destinatarios, como los niños (daños morales o psicológicos).

([1]) Dictamen del CESE sobre un «Programa para la protección de la infancia en Internet», Ponente: Sra. DAVISON, DO C 48 de 21.2.2002 y sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones – Seguridad de las redes y de la información: Propuesta para un enfoque político europeo», Ponente: Sr. RETUREAU, DO C 48 de 21.2.2002, así como sobre el «Libro verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información», Ponente: Sra. BARROW, DO C 287 de 22.9.1997.

([2]) «Technical Barriers to Trade». Acuerdos sobre obstáculos técnicos a los intercambios y prestaciones de servicios. Véase por ejemplo el caso planteado por Estados Unidos contra Antigua y Barbuda «Medidas que afectan al suministro transfronterizo de servicios de juegos de azar y apuestas» Decisión del Grupo Especial de la Organización Mundial de Comercio (http://www.wto.org/french/tratop_f/dispu_f/distabase_wto_members1_f.htm) documento 03-4429, WT/DS285/3 del 26 de agosto de 2003. Asunto en curso.

([3]) Acuerdos sobre los obstáculos técnicos a los intercambios y prestaciones de servicios. Véase por ejemplo el caso .....

3.9. Internet es utilizada por grupos mafiosos, defraudadores, autores de virus, piratas, espías industriales y demás delincuentes para llevar a cabo sus actividades. Reprimirlas resulta difícil, aunque en muchos países hay servicios especializados de policía que se afanan en identificar y localizar a los transgresores para demandarlos y poner fin a las actividades criminales constatadas; ello requiere en general una cooperación internacional que convendría promover aún más.

3.10. ¿Cómo luchar contra actividades criminales como las de los sitios de pederastia? Su prohibición no debería plantear dificultades jurídicas, pero conviene establecer los medios necesarios para detectar tales redes; ahora bien ¿cómo proteger también a los niños de los pederastas que actúen en espacios de debate en directo, especialmente apreciados por los jóvenes, para intentar obtener citas? El debate no se refiere a la legitimidad de la prohibición y la represión en estos casos particulares, sino a los medios que deben utilizarse para realizarlas.

3.11. Los proveedores de espacios y de acceso a Internet (FAI) no pueden supervisar y controlar todos los sitios albergados ni todas las comunicaciones (que constituyen correspondencia privada). Sin embargo, si son requeridos por un magistrado o un servicio de policía o de protección de menores habilitado, los FAI deben responder inmediatamente a las peticiones o decisiones relativas al cierre de tales lugares y a la identificación de las personas que los utilizan; esto implica conservar durante un determinado tiempo las informaciones sobre los enlaces y conexiones en red.

3.12. No obstante, las compañías de tarjetas de crédito, los motores de búsqueda y los FAI deberían llevar a cabo controles –por ejemplo, mediante sondeos– para detectar en Internet sitios de pederastia o que ofrecen otros contenidos delictivos; para ello, podrían utilizar como indicios palabras clave o zonas geográficas informando posteriormente de ello a la policía. Se deberían utilizar las mismas técnicas para localizar a «clientes» que hagan pedidos con tarjetas de crédito de pornografía infantil o *snuff movies* ([1]). Si fuera necesario, la legislación debería exigir tales investigaciones. Los motores de búsqueda de Internet deberían también reducir las posibilidades de que un internauta pueda encontrar pornografía infantil u otros contenidos delictivos mediante el uso de determinadas palabras y frases clave.

3.13. Ello requiere además, por parte de los poderes públicos, medios de lucha adaptados, personal cualificado, cooperaciones transfronterizas generalizadas y normas equilibradas a nivel nacional, europeo e internacional, que no afecten a las libertades de los internautas, pero permitan neutralizar las actividades de los individuos y grupos que utilizan estas redes para transmitir contenidos ilegales, y bloquear voluntariamente la recepción de contenidos inadecuados o nocivos.

3.14. Igualmente, para que esta lucha sea eficaz, debe incumbir directamente a todos los usuarios de Internet, que deben formarse e informarse de las precauciones que se han de tomar y de los medios que deben utilizarse para asegurarse contra la recepción de tales contenidos peligrosos o no deseables al objeto de no ser utilizados como enlaces de los mismos. La parte de información y formación del plan de acción debe, según el Comité, dar una alta prioridad a la movilización de los usuarios para responsabilizarles de sí mismos y de quienes dependen de ellos. Así, por ejemplo, los sitios sobre la salud no regulados representan un problema. Para protegerse, las empresas deben interesarse también en la formación de su personal y en la protección de sus redes y sitios de comercio en línea; y también las administraciones y las instituciones públicas y privadas deben recurrir a las mismas políticas de seguridad y garantizar la confidencialidad absoluta de los datos tratados, en particular los datos de carácter personal. La mayor sensibilización debería ir acompañada de incentivos para mejorar la calidad de los contenidos en línea, así como de estímulos para realizar actividades sanas al margen de Internet como alternativas a una «navegación» prolongada o a juegos de rol que pueden afectar a la larga a algunas personalidades inmaduras.

3.15. Los usuarios deben poder disponer de los medios para denunciar fácilmente los contenidos ilegales que encuentren en las redes ante centros de llamadas de urgencia especializados o ante organismos reconocidos o servicios especializados de las fuerzas de policía, con el fin de alertar a las autoridades públicas para que adopten, cuando sea necesario, medidas adecuadas. Se deberían formular advertencias a los padres en los países donde es frecuente el maltrato de niños para la pornografía en línea y en otros soportes, por ejemplo en las fronteras exteriores de la Unión; esto podría incluirse en determinados programas de cooperación RELEX.

3.16. Al tiempo que aprueba los objetivos específicos del programa, a saber, permitir que los usuarios denuncien los contenidos ilícitos (por medio de *hot lines*), desarrollar las tecnologías de filtrado de contenidos no deseados, la clasificación de los contenidos, la lucha contra el *spam*, la autorregulación de la industria y el conocimiento de la utilización segura de las tecnologías, el Comité sugiere, en sus observaciones particulares, algunos objetivos suplementarios que le parece útil tomar en consideración.

4. **Observaciones particulares del Comité**

4.1. El Comité ya ha pedido anteriormente a la Comisión que se reduzca la excesiva burocracia de los programas financiados por la UE, en concreto, para facilitar el acceso a la financiación de los microproyectos o de las ONG locales. El Comité considera que los controles deben centrarse en los resultados tangibles alcanzados en el marco del programa y en la eficacia de las soluciones propuestas. La difusión de las soluciones debería ser menos confidencial.

4.2. En opinión del Comité, debería examinarse la oportunidad de adoptar medidas normativas en apoyo de la protección de los usuarios finales, en el marco de este programa cuando ello sea posible y, si no, a través de una nueva iniciativa de la Comisión.

([1]) Películas en las que se muestran escenas reales de extremada violencia, torturas y asesinatos.

4.3. Los autores de programas informáticos de acceso a Internet y de sistemas de explotación de los servidores o de lucha contra las intrusiones deberían asumir plenamente la responsabilidad de sus actos; los usuarios deberían tener la garantía de que los autores de estos programas informáticos utilizan las mejores técnicas disponibles y ponen al día regularmente sus productos. La autorregulación o, en su defecto, una normativa comunitaria, deberían reforzar las garantías de los clientes.

4.4. Los proveedores de acceso a Internet deberían proponer (ya lo hacen muchos de ellos) medios fáciles de lucha antivirus a partir del propio sitio antes de transmitir un correo o ficheros adjuntos, y proponer medios de filtrado previo del correo para evitar los *spam*. Esto puede ofrecer una ventaja comercial a los proveedores que hagan esfuerzos serios de protección de sus clientes. Debido a que los niños se desenvuelven con frecuencia mejor que sus padres en lo que se refiere a la utilización de Internet, los sistemas de filtrado del correo, eliminación de virus, protección contra las intrusiones y control parental deben estar instalados previamente y ser fáciles de utilizar y de administrar por parte de personas que no tengan conocimientos técnicos particulares.

4.5. El programa debería también promover la investigación sobre programas informáticos especializados y otros medios de comprobación de la «estanqueidad» del código de los distintos programas informáticos de seguridad y de protección, incitar o eventualmente obligar a los proveedores a suministrar rápidamente los correctivos *(patches)* para todas las deficiencias observadas o señaladas que permitan intrusiones, y desarrollar la eficacia de los cortafuegos materiales y en forma de programas informáticos así como de los métodos de filtrado y de identificación del origen real de los contenidos.

4.6. El Comité habría deseado una mayor difusión de la evaluación de la eficacia y de los resultados obtenidos en el marco del plan *Safer Internet* anterior, con una clasificación por categorías de los problemas tratados por los diferentes proyectos. Convendría garantizar que todos los enlaces con las realizaciones que han sido objeto de financiación siguen estando activos y sean mejor conocidos por los destinatarios. El sitio de la Comisión debería asimismo informar sobre las iniciativas y experiencias adquiridas en los países miembros o en terceros países para difundir los conocimientos y los intercambios o cooperaciones útiles.

4.7. Es perfectamente posible adoptar acciones legales. Los FAI, las compañías de tarjetas de crédito y los motores de búsqueda son susceptibles de regulación y algunos ya practican una autorregulación. Las sanciones penales para los sitios que promueven el terrorismo, el racismo, el suicidio o la pornografía infantil deberían ser estrictas y disuasivas; se deberían realizar esfuerzos internacionales más importantes para identificar y localizar tales sitios con el fin de hacerlos cerrar en la medida de lo posible y si a este fin no se pueden entablar negociaciones con el país que las alberga.

5. **Conclusiones**

Al tiempo que apoya la continuación y extensión del programa *«Safer Internet plus»* el Comité (que hizo un llamamiento a favor de su creación) considera que la gravedad y el alcance de la amenaza de abusos, sobre todo de niños, requieren acciones legislativas urgentes y complementarias y medidas prácticas en función de cada caso en los ámbitos siguientes:

— deberes generales para todos los operadores interesados en lo que se refiere a la protección de los niños, en general a los usuarios y en particular a los más vulnerables,

— instalación por defecto de sistemas de filtrado,

— mensajes de seguridad claros en todas las páginas de presentación y portales de acceso a los espacios de debate en línea (*chat rooms*),

— apoyo a las asociaciones que crean líneas directas (*hot lines*) para señalar los sitios y actividades en línea que pueden perjudicar gravemente a los niños,

— impedimento de la utilización de tarjetas de crédito para pedidos de pornografía infantil y otros contenidos delictivos en Internet así como para las operaciones de blanqueo de dinero,

— advertencias y actividades específicas destinadas a los padres y a los educadores, así como a las autoridades de los países donde el maltrato de niños con fines pornográficos constituye un problema preocupante,

— más acción en lo que se refiere a los vínculos entre la explotación de niños con fines pornográficos y la delincuencia organizada,

— sistemas de identificación e información sobre contenidos nocivos y retirada de contenidos racistas, difusión de información sobre los intentos de estafa o la venta de sustancias que pueden afectar a la salud a través de Internet con el fin de proteger a las personas más vulnerables o mal informadas,

— búsqueda de cooperación y de normativas comunes a nivel internacional para luchar más eficazmente contra el *spam*,

— cooperación internacional (mejora del sistema de alerta precoz) y sanciones penales disuasivas para los difusores de virus informáticos y para la utilización ilegal de las redes privadas y públicas con fines criminales (intrusión al objeto de utilizar la red para actividades de espionaje industrial, apropiación indebida de la banda pasante y otros usos abusivos).

Bruselas, 16 de diciembre de 2004.

La Presidenta
del Comité Económico y Social Europeo
Anne-Marie SIGMUND