Dictamen del Comité Económico y Social Europeo sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones — Una estrategia para una sociedad de la información segura — Diálogo, asociación y potenciación»

COM(2006) 251 final

(2007/C 97/09)

El 31 de mayo de 2006, de conformidad con el artículo 262 del Tratado constitutivo de la Comunidad Europea, la Comisión decidió consultar al Comité Económico y Social Europeo sobre la propuesta mencionada.

La Sección Especializada de Transporte, Energía, Infraestructuras y Sociedad de la Información, encargada de preparar los trabajos en este asunto, aprobó su dictamen el 11 de enero de 2007 (ponente: **Sr. PEZZINI).**

En su 433º Pleno de los días 15 y 16 de febrero de 2007 (sesión del 16 de febrero de 2007) el Comité Económico y Social Europeo ha aprobado por 132 votos a favor y 2 abstenciones el presente Dictamen.

1. **Conclusiones y recomendaciones**

1.1 El Comité está convencido de que el problema de la seguridad informática representa una preocupación creciente para las empresas, las administraciones, los organismos públicos y privados, y los propios ciudadanos.

1.2 El Comité comparte, en líneas generales, el análisis y los argumentos que llevan a adoptar una nueva estrategia para aumentar la seguridad de las redes y de la información frente a los ataques e intrusiones que no conocen límites geográficos.

1.3 El Comité considera que la Comisión debería realizar esfuerzos adicionales en aras de una estrategia innovadora y articulada, dada la dimensión del fenómeno y sus consecuencias en la economía y la vida privada.

1.3.1 El CESE subraya, además, que la Comisión ha publicado recientemente una nueva comunicación sobre la seguridad de la información y que en breve debería publicar un nuevo documento sobre el tema. El Comité se reserva el derecho a emitir en el futuro un dictamen más articulado que tenga en cuenta el conjunto de las comunicaciones.

1.4 El Comité subraya que el aspecto de la seguridad de la información no puede, de ningún modo, disociarse del refuerzo de la protección de los datos personales y de la salvaguardia de la libertad, derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

1.5 El CESE se pregunta cuál es, en el momento actual, el valor añadido de la propuesta sobre el enfoque integrado adoptado en 2001, cuyo objetivo coincidía con el indicado en la Comunicación sometida a examen ([1]).

1.5.1 El documento de evaluación de impacto ([2]), adjunto a la propuesta, contiene algunos cambios interesantes respecto de la posición de 2001, pero sólo se ha publicado en una lengua, por lo que resulta inaccesible para muchos ciudadanos europeos, que emitirían su juicio sobre el documento oficial escrito en las lenguas comunitarias.

1.6 El Comité recuerda las conclusiones extraídas en la Cumbre Mundial de Túnez de 2005 sobre la sociedad de la información, suscritas por la Asamblea de las Naciones Unidas el 27 de marzo de 2006:

— acceso no discriminatorio;

— promoción de las TIC como instrumento de paz;

— definición de instrumentos para reforzar la democracia, la cohesión y la buena *gobernanza;*

— prevención de abusos en el respeto de los derechos humanos ([3]).

1.7 El Comité subraya que una estrategia comunitaria dinámica e integrada debería poder abordar, aparte del diálogo, de la asociación y de la potenciación, los siguientes temas:

— acciones de prevención;

— el paso de la seguridad al aseguramiento de la información ([4]);

— la predisposición de un marco comunitario jurídico y de sanciones verdadero y reconocido;

— el refuerzo de la normalización técnica;

([1]) Véase el Dictamen del CESE 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», DO C 48 de 21.2.2002, p. 33.

([2]) Un documento de impacto no posee el mismo valor que un documento de estrategia.

([3]) Naciones Unidas 27.3.2006, Recomendaciones nº 57 y 58. Documento final de Túnez nº 15.

([4]) Véase: *Emerging technologies in the context of security (tecnologías emergentes en el contexto de la seguridad)* CCI, Instituto para la Protección y la Seguridad de los Ciudadanos, cuaderno de investigación estratégica, septiembre de 2005, Comisión Europea http://serac.jrc.it.

— la identificación digital de los usuarios;

— la realización de ejercicios europeos de análisis y prospectiva (*Foresight*) sobre la seguridad de la información, en condiciones de convergencia tecnológica multimodal;

— el refuerzo de los mecanismos europeos y nacionales de evaluación de riesgos;

— acciones dirigidas a evitar la emergencia de «monocultivos» informáticos;

— el refuerzo de la coordinación comunitaria a nivel europeo e internacional;

— la creación de un *Security Focal Point* de las TIC entre las direcciones generales;

— el establecimiento de una *European Network and Information Security Network (Red Europea y Red de Seguridad de la Información);*

— la optimización del papel de la investigación europea en la seguridad de la información;

— la celebración de un «Día europeo del ordenador seguro»;

— la organización de acciones piloto comunitarias en centros de enseñanza de diferentes tipos y niveles, sobre temas relativos a la seguridad de la información.

1.8 El CESE considera, por último, que para asegurar una estrategia comunitaria dinámica e integrada hay que prever recursos presupuestarios adecuados con iniciativas y acciones de coordinación reforzadas a nivel comunitario que puedan presentar unánimemente a Europa en el contexto internacional.

2. **Exposición de motivos**

2.1 Los retos que representa la seguridad de la sociedad de la información desempeñan un papel fundamental a la hora de asegurar la confianza y la fiabilidad de las redes y servicios de comunicación, que constituyen factores fundamentales para el desarrollo de la economía y de la sociedad.

2.2 Las redes y los sistemas de información requieren una protección permanente para mantener su capacidad competitiva y comercial, a fin de asegurar la integridad y continuidad de las comunicaciones electrónicas, prevenir los fraudes y garantizar la protección jurídica de la vida privada.

2.3 Las comunicaciones electrónicas y los servicios relacionados representan el segmento más amplio de todo el sector de las telecomunicaciones: en 2004 alrededor de un 90 % de las empresas europeas utilizó Internet de forma activa y un 65 % de éstas creó su propio sitio Web; mientras que se calcula que aproximadamente el 50 % de la población europea utiliza regularmente Internet y que el 25 % de las familias dispone de forma continua de servicios de banda ancha para el acceso a Internet ([5]).

([5]) *i2010 Una estrategia para una sociedad de la información segura,* DG Sociedad de la información y medios de comunicación «Factsheet 8» (junio de 2006) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

2.4 En comparación con el desarrollo acelerado de las inversiones, el volumen de los gastos en seguridad representa sólo entre el 5 y el 13 % del total de las inversiones en tecnologías de la información. Ahora bien, este porcentaje es, sin duda, demasiado limitado. Según estudios recientes, de una media de 30 protocolos que comparten las estructuras clave, 23 son vulnerables a los ataques multiprotocolo ([6]). Además, se calcula que diariamente se envía una media de 25 millones de mensajes electrónicos *spam* ([7]), por lo que el Comité celebra la propuesta al respecto recientemente presentada por la Comisión.

2.5 En el ámbito de los virus informáticos ([8]), se ha constatado la rápida evolución a gran escala de los gusanos informáticos ([9]) y los programas espía ([10]) paralelamente al creciente desarrollo de los sistemas de redes de comunicación electrónica. Éstos se han vuelto cada vez más complejos y vulnerables, también en función de la convergencia de los entornos multimedia y la telefonía móvil, así como de los sistemas *GRIS infoware* ([11]): los casos de extorsión, el Ddos (*Distributed denials of service*) o ataque de denegación de servicio distribuido, el robo de identidad en línea, el *phishing* ([12]), la piratería informática ([13]), etc. representan otros tantos retos para la seguridad de la sociedad de la información. La Unión Europea ya había abordado el problema en una Comunicación en 2001 ([14]), sobre la que el Comité pudo pronunciarse ([15]), y ahora propone una estrategia que gira en torno a tres líneas de intervención:

— medidas específicas de seguridad;

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security (Acta de la I Conferencia Internacional sobre disponibilidad, fiabilidad y seguridad)* (ARES'06) — volumen 00 ARES 2006; Editorial: IEEE Computer Society.

([7]) Spam = mensajes de correo electrónico indeseados de carácter comercial. El significado origial de *spam* es «*spiced pork and ham*», un tipo de carne de conserva en gelatina muy popular durante la Segunda Guerra Mundial (cuando se convierte en uno de los alimentos básicos) para las tropas estadounidenses y la población inglesa. Tras años con una dieta semejante, el término fue adquiriendo un significado peyorativo.

([8]) *Virus informático*: programa especial perteneciente a la categoría de programas maliciosos que puede, una vez ejecutado, infectar archivos para reproducirse haciendo copias de sí mismo, generalmente sin que el usuario lo note. Los virus pueden resultar más o menos dañinos para el sistema operativo que lo alberga, pero, incluso en el mejor de los casos, comportan una cierta pérdida de recursos en términos de RAM, UCP y espacio del disco duro (www.wikipedia.org/wiki/Virus_informatico).

([9]) «*Worm*» *o gusano informático*: programa dañino capaz de replicarse: un «*e-mail worm*» o gusano de correo electrónico constituye un ataque devastador contra una red, que consiste en la recopilación de todas las direcciones de correo electrónico contenidas en un programa local (por ejemplo, MS Outlook) para después enviarles centenares de mensajes electrónicos con el mismo gusano como adjunto invisible.

([10]) «*Spyware*» o *programas espía* = programas informáticos que conservan el rastro de la navegación en Internet efectuada por el usuario y que se autoinstalan sin notificárselo y sin que éste se de cuenta o lo haya autorizado y fuera de su control.

([11]) *GRIS infoware* = permite compartir, seleccionar y añadir una amplia gama de recursos electrónicos distribuidos geográficamente (por ejemplo, superordenador, torres de ordenadores, sistemas de memoria de datos, fuentes de datos, instrumentos y personas) presentándolos como recurso único independiente para resolver cálculos de extrema complejidad y tratamientos de datos de carácter especialmente intensivo.

([12]) *Phishing* = en el ámbito informático, es una técnica de *cracking* utilizada para obtener el acceso a información personal y reservada con la finalidad de robar la identidad mediante mensajes de correo electrónico falsos, creados para que parezcan auténticos.

([13]) Piratería informática = es un término empleado por los «piratas» de la informática para referirse a un programa al que se le ha quitado la protección anticopia y así se pueda bajar gratuitamente de la red.

([14]) COM(2001) 298 final.

([15]) Véase la nota 1.

— un marco jurídico, que incluye la protección de datos y de la vida privada;

— la lucha contra la ciberdelincuencia.

2.6 La detección de ataques informáticos, así como su identificación y prevención, en el contexto de un sistema de red, representan un reto para la búsqueda de soluciones adecuadas, dados los continuos cambios en la configuración, la variedad de los protocolos de red y de los servicios disponibles y desarrollados, además de la extrema complejidad de los procedimientos asíncronos de ataque ([16]).

2.7 Lamentablemente, la escasa visibilidad de la rentabilidad de las inversiones en seguridad y la insuficiente responsabilización por parte de los usuarios han conducido a una infravaloración de los riesgos y a una reducción de la atención prestada al desarrollo de una cultura de la seguridad.

3. **La propuesta de la Comisión**

3.1 Con la Comunicación sobre una estrategia para una sociedad de la información segura ([17]), la Comisión aspira a mejorar la seguridad de la información desarrollando una estrategia dinámica e integrada, basada en:

a) una mejora del diálogo entre las autoridades públicas y la Comisión, con una evaluación comparativa de las políticas nacionales y la determinación de las mejores prácticas de comunicación electrónica en sistemas seguros;

b) una mayor sensibilización de los ciudadanos y de las PYME sobre los sistemas eficaces de seguridad con un activo papel incentivador de la Comisión y una mayor intervención de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA);

c) un diálogo sobre instrumentos y normas a fin de hallar un equilibrio entre seguridad y derechos fundamentales, incluida la protección de la vida privada.

3.2 Por otro lado, la Comunicación ha previsto, con vistas al desarrollo de un marco adecuado de recopilación de datos sobre las violaciones de la seguridad, los niveles de confianza de los usuarios y la evolución de la industria de la seguridad, una asociación de confianza de la ENISA con:

a) los Estados miembros;

b) los consumidores y los usuarios;

c) la industria de la seguridad de la información;

d) el sector privado,

mediante la creación de un portal comunitario multilingüe de información y prevención de riesgos en aras de una asociación estratégica entre el sector privado, los Estados miembros y los investigadores.

3.2.1 Por otro lado, la Comunicación prevé una mayor responsabilización de las partes interesadas respecto a las necesidades y riesgos en materia de seguridad.

3.2.2 Por lo que se refiere a la cooperación internacional y con terceros países, «la dimensión mundial de la seguridad de las redes y de la información reta a la Comisión, tanto a nivel internacional como en coordinación con los Estados miembros, a redoblar sus esfuerzos de promoción de la cooperación mundial en materia de SRI» ([18]), pero tal indicación no se incluye entre las acciones de diálogo, asociación y potenciación.

4. **Observaciones**

4.1 El Comité coincide con el análisis y los argumentos que justifican una estrategia europea integrada y dinámica de la seguridad de las redes y de la información, ya que considera esencial la cuestión de la seguridad a fin de promover una actitud más favorable a la aplicación de las TI y aumentar la confianza en estas últimas. La posición del CESE al respecto ya se ha plasmado en numerosos dictámenes ([19]).

4.1.1 El Comité reitera que ([20]): «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».

([16]) Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* — 2005 Estados Unidos, Arizona Internet Technology Laboratory, ECE Department (Universidad de Arizona), http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, Estados Unidos — Trabajo realizado en colaboración con Intel Corporation IT R&D Council.

([17]) COM(2006) 251 final de 31.5.2006.

([18]) COM(2006) 251 final, penúltimo párrafo, apartado 3.

([19]) Véanse los siguientes documentos:
- Dictamen del CESE sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE» — DO C 69 de 21.3.2006, p. 16;
- Dictamen del CESE sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones — i2010 — Una sociedad de la información europea para el crecimiento y el empleo» — DO C 110 de 9.5.2006, p. 83;
- Dictamen del CESE 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» — DO C 157 de 28.6.2005, p. 136;
- Dictamen del CESE 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» — DO C 48 de 21.2.2002, p. 33.

([20]) Véase el tercer guión de la nota 19.

4.2 *En pro del refuerzo de las propuestas de la Comisión*

4.2.1 No obstante, el Comité considera que el enfoque propuesto por la Comisión — que consiste en basar dicha estrategia integrada y dinámica en un diálogo abierto e inclusivo, junto con una asociación y una potenciación reforzadas con todas las partes interesadas y, en particular, con los usuarios — podrá ampliarse.

4.2.2 Dicha postura ya se destacó en anteriores dictámenes: «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» ([21]).

4.2.3 A juicio del Comité, es indispensable que los usuarios y los ciudadanos, en general, se movilicen, de modo que se concilie la necesaria protección de la información y de las redes con las libertades civiles y el derecho de los usuarios a beneficiarse de accesos seguros y de bajo coste.

4.2.4 Cabe considerar que la búsqueda de la seguridad de la información representa también un coste para el consumidor en términos de tiempo perdido para eliminar o soslayar los obstáculos. El Comité opina que sería necesario imponer una obligación de instalación automática de sistemas de protección antivirus en cada ordenador, que el usuario pueda activar o no, pero que esté presente por defecto en el producto.

4.3 *En pro de una estrategia comunitaria más dinámica e innovadora*

4.3.1 Además, el Comité estima que la Unión debería fijarse objetivos más ambiciosos y adoptar una estrategia innovadora, integrada y dinámica, con el lanzamiento de nuevas iniciativas, como, por ejemplo:

— mecanismos que permitan la identificación digital de los usuarios, a quienes se les pide con demasiada frecuencia que faciliten sus datos personales;

— acciones a través de la ETSI ([22]) que sirvan de requisito para un uso seguro de las TIC y que puedan ofrecer soluciones específicas y rápidas, definidas con un umbral común de seguridad en toda la Unión;

— acciones de prevención mediante la inclusión de las exigencias mínimas de seguridad en los sistemas informáticos y de redes y el lanzamiento de acciones piloto con cursos de seguridad organizados en centros de enseñanza de cualquier tipo y nivel;

— creación de un marco jurídico verdadero y reconocido a nivel europeo. Dicho marco, aplicado a la informática y a las redes, consistiría en pasar de la seguridad al aseguramiento de la información;

— refuerzo de los mecanismos europeos y nacionales de evaluación de riesgos y mejora de la capacidad de aplicación de las disposiciones legislativas y reglamentos para combatir los delitos informáticos contra la privacidad y los archivos de datos;

— acciones dirigidas a evitar la aparición de «monocultivos informáticos» con productos y soluciones más eficaces. Apoyo a las innovaciones multiculturales diversificadas con vistas a la creación de un espacio único europeo de la información (SEIS — *Single European Information Space*).

4.3.2 A juicio del CESE, sería conveniente crear un *ICT-Security Focal Point, inter DG* ([23]). El *Focal Point* consistiría en actuar:

— a nivel de los servicios de la Comisión;

— a nivel de los Estados miembros, mediante soluciones horizontales para aspectos de interoperabilidad, gestión de la identidad, protección de la vida privada, libertad de acceso a la información y a los servicios, y requisitos mínimos de seguridad;

— a nivel internacional a fin de poder asegurar que la UE habla con una sola voz en los diversos contextos internacionales, como las Naciones Unidas, el G8, la OCDE y la ISO.

4.4 *En pro de acciones comunitarias de coordinación responsable reforzadas*

4.4.1 El CESE también atribuye mucha importancia a la creación de una *European Network and Information Security Network* (Red Europea y Red de Seguridad de la Información), mediante la que se puedan promover encuestas, estudios y talleres sobre los mecanismos de seguridad y su interoperabilidad, sobre criptografía avanzada y sobre la protección de la vida privada.

4.4.2 El CESE considera que para este sector tan delicado sería conveniente optimizar el papel de la investigación europea mediante una síntesis adecuada del contenido de:

— el programa europeo de investigación sobre seguridad (ESRP) ([24]), recogido en el Séptimo Programa Marco de IDT;

([21]) Véase el tercer guión de la nota 19.

([22]) ETSI, *European Telecommunications Standards Institute* (Instituto de Estándares de Telecomunicaciones Europeo); véase en particular el seminario de los días 16 y 17 de enero de 2006. El ETSI ha abordado, entre otros, los temas de las interceptaciones ilegales (TS 102 232; 102 233; 102 234), el acceso a Internet Lan Wireless (TR 102 519) y las firmas electrónicas, y ha desarrollado algoritmos de seguridad para GSM, GPRS y UMTS.

([23]) El *Focal Point inter DG* podría financiarse en el marco de la prioridad IST del Programa Específico de Cooperación del PQ7-RST o del programa europeo de investigación sobre seguridad (ESRP).

([24]) Véase el Séptimo Programa Marco de la CE de IDT+D, programa «cooperación»: Prioridad temática investigación sobre seguridad con un presupuesto de 1 350 millones de euros en el periodo 2007-2013.

— el Programa *Safer Internet Plus;*

— el programa europeo para la protección de infraestructuras críticas (EPCIP) ([25]).

4.4.3 A estas sugerencias se podría añadir el lanzamiento de un «Día europeo del ordenador seguro», apoyado con campañas nacionales de educación (en los centros de enseñanza) y de información a los consumidores acerca de los procedimientos de protección de la información a través del ordenador, aparte, evidentemente, de la información sobre los avances tecnológicos registrados en el vasto y cambiante ámbito de los ordenadores.

4.4.4 El Comité ha subrayado en diversas ocasiones que «la percepción de seguridad y confianza en las transacciones digitales determinan con toda probabilidad la velocidad con la que las empresas adoptan las TIC en sus actividades. En la disposición de los consumidores a proporcionar los datos de sus tarjetas de crédito en una página Web influye en gran medida la percepción de seguridad de este acto» ([26]).

4.4.5 El Comité está convencido de que, dado el enorme potencial de crecimiento del sector, por un lado, es necesario aplicar políticas específicas y, por otro, adecuar las políticas actuales a los nuevos avances. Es preciso vincular las iniciativas europeas en materia de seguridad de la información a una estrategia integrada, eliminando los límites sectoriales y garantizando una difusión homogénea y segura de las TIC en la sociedad.

4.4.6 A juicio del Comité, algunas estrategias importantes, como la que nos ocupa, funcionan con excesiva lentitud a causa de los obstáculos burocráticos y culturales que interponen los Estados miembros a las decisiones indispensables que han de adoptarse a nivel comunitario.

4.4.7 El Comité estima, asimismo, que los recursos comunitarios son insuficientes para realizar los numerosos proyectos urgentes que pueden aportar respuestas concretas a los nuevos problemas de la globalización, pero únicamente si se realizan a nivel comunitario

4.5 *En pro de una mayor seguridad comunitaria de protección del consumidor*

4.5.1 El Comité es consciente de que los Estados miembros han adoptado medidas tecnológicas de seguridad y procedimientos de gestión de la seguridad con arreglo a exigencias propias y con una tendencia a centrarse en diferentes aspectos. Por este motivo, también resulta difícil aportar una respuesta unánime y eficaz a los problemas de seguridad. Exceptuando algunas redes administrativas, no existe una cooperación transfronteriza sistemática entre los Estados miembros. No obstante, cabe señalar que los países no pueden afrontar las cuestiones de seguridad de forma aislada.

4.5.2 Por otra parte, el Comité subraya que, con su Decisión marco 2005/222/JAI, el Consejo ha adoptado un sistema de cooperación entre las autoridades judiciales y las otras autoridades competentes de los Estados miembros al objeto de garantizar un enfoque coherente por parte de estos últimos, mediante la aproximación de sus legislaciones penales en el sector de los ataques contra los sistemas de información en materia de:

— acceso ilícito a los sistemas de información;

— interferencia ilícita en lo que respecta a los sistemas, mediante acto intencionado dirigido a obstaculizar gravemente o a interrumpir el funcionamiento de un sistema de información;

— interferencia ilícita en lo que respecta a los datos, mediante acto intencionado de cancelar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles los datos informáticos en un sistema de información;

— instigación, encubrimiento y complicidad en los delitos mencionados supra.

4.5.3 Además, la Decisión indica los criterios para establecer la responsabilidad de las personas jurídicas y las posibles sanciones que pueden aplicárseles si se confirma tal responsabilidad.

4.5.4 En el ámbito del diálogo con las autoridades públicas de los Estados miembros, el Comité respalda la propuesta de la Comisión para que dichas autoridades emprendan un ejercicio de evaluación comparativa de las propias políticas nacionales en materia de seguridad de las redes y de los sistemas de información, incluidas las específicas del sector público. Dicha propuesta se recogía, asimismo, en un dictamen del CESE de 2001 ([27]).

4.6 *En pro de una cultura de la seguridad más generalizada*

4.6.1 Por lo que se refiere a la intervención de la industria de la seguridad de la información, a fin de proteger el derecho de los propios clientes a la vida privada y de asegurar la confidencialidad de los datos personales, dicha industria debe garantizar realmente el uso de los sistemas de vigilancia material de sus instalaciones y de la codificación de las comunicaciones, en función de la evolución de las técnicas ([28]).

([25]) COM(2005) 576 de 17.11.2005.
([26]) Véase el segundo guión de la nota 19.
([27]) Véase el cuarto guión de la nota 19.
([28]) Véase la Directiva 97/66/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DO L 24 de 30.1.1998).

4.6.2 En cuanto a la acción de sensibilización, el Comité considera fundamental que se cree una verdadera «cultura de la seguridad», concebida de modo que sea totalmente compatible con la libertad de información, de comunicación y de expresión. Por otro lado, recuerda que mientras numerosos usuarios no son conscientes de todos los riesgos que comporta la piratería informática, muchos operadores, vendedores o prestadores de servicios no se hacen una idea de la existencia y dimensión de los aspectos vulnerables.

4.6.3 Dado que la protección de la vida privada y de los datos personales constituye un objetivo prioritario, los consumidores también tienen el derecho a protegerse de forma verdaderamente eficaz contra el perfilado nominativo abusivo mediante programas espía (*spyware* y *web bugs* o escuchas web) o mediante otros métodos. También debería frenarse la práctica del *spamming* ([29]) (envíos masivos de mensajes no deseados) que a menudo se deriva de estos abusos. Estas intrusiones perjudican a las víctimas ([30]).

4.7 *En pro de una agencia comunitaria más fuerte y activa*

4.7.1 El Comité aboga por un papel más intenso y reforzado de la Agencia Europea de Seguridad de las Redes y de la Información en lo que se refiere a la sensibilización y, sobre todo, en acciones de información y formación de operarios y usuarios, como ya lo expresó en un Dictamen ([31]) reciente sobre la prestación de servicios públicos de comunicación electrónica.

4.7.2 Por último, con respecto a las acciones propuestas sobre la potenciación de cualquier grupo de interesados, éstas parecen ceñirse severamente al principio de subsidiariedad. Efectivamente, dichas acciones recaen en los Estados miembros y en el sector privado, según las responsabilidades específicas.

4.7.3 La Agencia Europea de Seguridad de las Redes y de la Información debería poder beneficiarse de la contribución de la Red Europea y Red de Seguridad de la Información (*European Network and Information Security Network*) para la organización de actividades conjuntas, así como del portal comunitario web multilingüe de prevención de seguridad informática para obtener información personalizada e interactiva con lenguajes facilitados, sobre todo, para los usuarios de diversas edades y para las PYME.

Bruselas, 16 de febrero de 2007.

El Presidente
del Comité Económico y Social Europeo
Dimitris DIMITRIADIS

([29]) «Pollu-postage», en francés.

([30]) Véanse los Dictámenes del CESE sobre: la «Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión» (DO C 123 de 25.4.2001, p. 50); la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior (DO C 169 de 16.6.1999, p. 36); y sobre el tema «Incidencia del comercio electrónico en el mercado interior (OMU)» (DO C 123 de 25.4.2001, p. 1).

([31]) Véase el primer guión de la nota 19.