Parere del Comitato economico e sociale europeo in merito alla Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni — Una strategia per una società dell'informazione sicura — Dialogo, partenariato e responsabilizzazione

COM(2006) 251 def.

(2007/C 97/09)

La Commissione, in data 31 maggio 2006, ha deciso, conformemente al disposto dell'articolo 262 del Trattato che istituisce la Comunità europea, di consultare il Comitato economico e sociale europeo in merito alla proposta di cui sopra.

La sezione specializzata Trasporti, energia, infrastrutture, società dell'informazione, incaricata di preparare i lavori del Comitato in materia, ha formulato il proprio parere in data 11 gennaio 2007, sulla base del progetto predisposto dal relatore PEZZINI.

Il Comitato economico e sociale europeo, in data 16 febbraio 2007, nel corso della 433ª sessione plenaria, ha adottato il seguente parere con 132 voti favorevoli e 2 astensioni.

1. **Conclusioni e raccomandazioni**

1.1 Il Comitato è convinto che il problema della sicurezza informatica rappresenti una preoccupazione crescente per le aziende, per le amministrazioni, per gli organismi pubblici e privati nonché per i singoli cittadini.

1.2 Il Comitato condivide, in linea generale, le analisi e gli argomenti che impongono una nuova strategia per aumentare la sicurezza delle reti e dell'informazione contro gli attacchi e le intrusioni che si manifestano senza confini geografici.

1.3 Il Comitato ritiene che la Commissione dovrebbe fare ulteriori sforzi per realizzare una strategia innovativa e articolata, vista l'ampiezza del fenomeno e le sue conseguenze sul piano economico e su quello della vita privata.

1.3.1 Il CESE sottolinea altresì che la Commissione ha recentemente pubblicato una nuova comunicazione sulla sicurezza informatica e che, entro breve termine, dovrebbe uscire un altro nuovo documento sull'argomento. Il Comitato si riserva quindi di esprimere in futuro un parere più articolato, che tenga conto dell'insieme delle comunicazioni.

1.4 Il Comitato sottolinea che l'aspetto della sicurezza informatica non può in alcun modo essere disgiunto dal rafforzamento della protezione dei dati personali e dalla tutela delle libertà, che sono diritti garantiti dalla Convenzione europea dei diritti dell'uomo.

1.5 Il CESE si domanda quale sia, allo stato attuale, il valore aggiunto della proposta rispetto all'approccio integrato adottato nel 2001, il cui scopo coincideva con quello indicato nella presente comunicazione ([1]).

1.5.1 La valutazione di impatto (*Impact Assessment*) ([2]), allegata alla proposta, contiene alcuni interessanti aggiornamenti rispetto alla posizione del 2001 ma è disponibile in una sola lingua; essa non è quindi accessibile a molti cittadini europei, che formulano il loro giudizio sul documento ufficiale, pubblicato in tutte le lingue comunitarie.

1.6 Il Comitato richiama le conclusioni adottate dal vertice mondiale di Tunisi del 2005 sulla società dell'informazione e sottoscritte dall'Assemblea dell'ONU del 27 marzo 2006:

— accesso non discriminatorio,

— promozione delle TIC come strumento di pace,

— definizione di strumenti per rafforzare la democrazia, la coesione e la buona *governance*,

— prevenzione degli abusi, nel rispetto dei diritti umani ([3]).

1.7 Il Comitato sottolinea che una strategia comunitaria dinamica e integrata dovrebbe poter affrontare, oltre al dialogo, al partenariato e alla responsabilizzazione, anche i temi seguenti:

— azioni di prevenzione,

— il passaggio dalla sicurezza all'assicurazione informatica ([4]),

— la predisposizione di un quadro UE certo e riconosciuto per quanto concerne le norme giuridiche e regolamentari e le sanzioni previste,

— il rafforzamento della standardizzazione tecnica,

([1]) Cfr. parere del CESE in merito alla *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni — Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, GU C 48 del 21.2.2002, pag. 33.

([2]) La «valutazione di impatto» non ha lo stesso valore che ha un «documento di strategia».

([3]) ONU 27.3.2006, Raccomandazioni n. 57 e 58. Documento finale di Tunisi n. 15.

([4]) Cfr. *Emerging technologies in the context of security* CCR — Istituto per la protezione e la sicurezza del cittadino, quaderno di ricerca strategica, settembre 2005, Commissione europea, http://serac.jrc.it.

— l'identificazione digitale degli utenti,

— il lancio di esercizi europei di analisi e di prospettiva (*Foresight*) sulla sicurezza informatica, in condizioni di convergenze tecnologiche multimodali,

— il rafforzamento dei meccanismi europei e nazionali di valutazione dei rischi,

— azioni volte ad evitare l'emergere di monoculture informatiche,

— il rafforzamento del coordinamento comunitario a livello europeo e internazionale,

— l'istituzione tra le direzioni generali di un TIC *Security Focal Point*,

— la creazione di una rete europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Network*),

— l'ottimizzazione del ruolo della ricerca europea sulla sicurezza informatica,

— il lancio di una «Giornata europea del computer sicuro»,

— l'organizzazione di azioni pilota comunitarie, nelle scuole di vario ordine e grado, sui temi della sicurezza informatica.

1.8 Il CESE ritiene infine che per assicurare una strategia comunitaria dinamica e integrata si debbano prevedere dotazioni di bilancio adeguate, con iniziative e azioni di coordinamento rafforzate a livello comunitario che siano in grado di rappresentare l'Europa con una voce unica nel contesto globale.

2. **Motivazioni**

2.1 Le risposte date alle sfide in materia di sicurezza della società dell'informazione svolgono un ruolo fondamentale nell'assicurare fiducia e affidabilità alle reti e ai servizi di comunicazione, che costituiscono fattori critici per lo sviluppo dell'economia e della società.

2.2 Le reti e i sistemi informatici hanno bisogno di essere protetti per mantenere le loro capacità competitive e commerciali, assicurare l'integrità e la continuità delle comunicazioni elettroniche, prevenire le frodi e garantire la tutela giuridica della vita privata.

2.3 Le comunicazioni elettroniche e i servizi ad esse correlati rappresentano il segmento più ampio dell'intero settore delle telecomunicazioni: nel 2004 circa il 90 % delle imprese europee ha usato Internet attivamente e il 65 % ha sviluppato un proprio sito web, mentre si calcola che circa la metà della popolazione europea fa uso regolare di Internet e che il 25 % delle famiglie utilizza in modo continuativo l'accesso a banda larga ([5]).

2.4 Di fronte allo sviluppo accelerato degli investimenti, il volume della spesa per la sicurezza rappresenta solo una percentuale compresa tra il 5 e il 13 % del totale degli investimenti nelle tecnologie dell'informazione. Orbene, questa percentuale è decisamente troppo limitata. Recenti studi hanno evidenziato che «su una media di 30 protocolli che condividono le strutture chiave, 23 sono vulnerabili ad attacchi multiprotocollo» ([6]) mentre si valutano in 25 milioni i messaggi elettronici *spam* ([7]) trasmessi mediamente ogni giorno: il Comitato si rallegra dunque della proposta recentemente presentata dalla Commissione in proposito.

2.5 Nell'ambito dei virus informatici ([8]), la rapida evoluzione su larga scala di «vermi informatici» (*worms*) ([9]) e di software «spia» (*spyware*) ([10]) si è mossa parallelamente al crescente sviluppo dei sistemi e delle reti di comunicazione elettronica. Questi sono diventati sempre più complessi e al tempo stesso vulnerabili, anche in funzione della convergenza di multimedia, telefonia mobile e dei sistemi *GRID infoware* ([11]): i casi di estorsione, di DdoS (*Distributed denials of service*, ossia un'interruzione del servizio con origine da più fonti), di furto di identità in linea, di *phishing* ([12]), di *piracy* ([13]) e via dicendo rappresentano altrettante sfide alla sicurezza della società dell'informazione. La Comunità europea aveva già affrontato il problema in una sua comunicazione del 2001 ([14]), su cui il Comitato ha avuto modo di pronunciarsi ([15]). In essa la Commissione proponeva una strategia secondo tre linee d'intervento:

— misure specifiche di sicurezza,

([5]) *i2010*: *Una strategia per una società dell'informazione sicura*. DG Società dell'informazione e media, «Factsheet 8» (giugno 2006) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

([6]) Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) — volume 00 ARES 2006 Editore: IEEE Computer Society.

([7]) *Spam* = messaggi indesiderati di posta elettronica a carattere commerciale. Il significato originale di *spam* è «*spiced pork and ham*», una specie di conserva di carne in gelatina molto popolare ai tempi della seconda guerra mondiale quando divenne una delle principali risorse alimentari, non essendo per di più razionata, per le truppe statunitensi e per la popolazione inglese. Anni e anni di una tale dieta fecero sì che il termine acquistasse un significato negativo.

([8]) *Virus informatico*: particolare software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere più o meno dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano sempre un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso (www.wikipedia.org/wiki/Virus_informatico).

([9]) *Worm* = software maligno capace di replicarsi: un «*e-mail worm*» è un attacco devastante contro un network, che consiste nel raccogliere tutti gli indirizzi e-mail contenuti in un programma locale (ad esempio MS Outlook) per poi inviare loro centinaia di e-mail che contengono il *worm* medesimo come allegato invisibile.

([10]) *Spyware* = programmi che conservano traccia della navigazione in Internet effettuata dall'utilizzatore e che si autoinstallano senza alcuna notifica all'utente, né sua consapevolezza, autorizzazione e controllo.

([11]) *GRID infoware* = permette di condividere, selezionare ed aggregare un'ampia gamma di risorse di elaborazione elettronica distribuite geograficamente (ad esempio supercomputer, blocchi di computer, sistemi di memorizzazione dei dati, fonti di dati, strumenti e persone) presentandole come una risorsa unica e a sé stante per risolvere calcoli di estrema complessità ed elaborazioni di dati a carattere particolarmente intensivo.

([12]) *Phishing* =in ambito informatico si definisce *phishing* una tecnica di *cracking* utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici.

([13]) *Piracy* = è un termine utilizzato dai «pirati» dell'informatica per descrivere un software al quale è stata tolta la protezione anticopia e che viene reso disponibile a essere scaricato via Internet.

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

([15]) Cfr. nota 1.

— quadro normativo, inclusivo della protezione dei dati e della vita privata,

— lotta contro la cibercriminalità.

2.6 Il rilevamento degli attacchi informatici e la loro identificazione e prevenzione, nell'ambito di un sistema a rete, rappresentano una sfida per la ricerca di soluzioni adeguate, dati i continui cambiamenti di configurazione, la varietà dei protocolli di rete e dei servizi offerti e sviluppati nonché l'estrema complessità dei comportamenti asincroni di attacco ([16]).

2.7 Purtroppo, però, la scarsa visibilità del ritorno degli investimenti in sicurezza e l'insufficiente assunzione di responsabilità da parte dei cittadini utilizzatori hanno portato ad una sottovalutazione dei rischi e ad un calo dell'attenzione per quanto concerne la cultura della sicurezza.

3. **La proposta della Commissione**

3.1 Con la comunicazione sulla strategia per una società dell'informazione sicura ([17]), la Commissione ha inteso migliorare la sicurezza informatica mettendo a punto una strategia dinamica e integrata, basata su:

a) un miglioramento del dialogo tra autorità pubbliche e Commissione, con analisi comparativa (*benchmarking*) delle politiche nazionali e individuazione delle migliori pratiche di comunicazione elettronica in regime sicuro;

b) una più intensa sensibilizzazione dei cittadini e delle PMI verso i regimi efficaci di sicurezza, con un ruolo attivo di stimolo della Commissione e un coinvolgimento maggiore dell'Agenzia europea per la sicurezza delle reti e dell'informazione (AESRI/ENISA);

c) un dialogo su strumenti e norme atti a garantire un rapporto equilibrato tra sicurezza e diritti fondamentali, compresa la protezione della vita privata.

3.2 Inoltre la comunicazione ha previsto, nella prospettiva di sviluppo di un quadro adeguato di raccolta dati sulle violazioni della sicurezza, sui livelli di fiducia degli utenti e sugli sviluppi dell'industria della sicurezza, un partenariato di fiducia dell'AESRI/ENISA:

a) con gli Stati membri;

b) con i consumatori e gli utenti;

c) con l'industria della sicurezza informatica;

d) con il settore privato;

mediante la creazione di un portale comunitario plurilingue di informazione e di allerta rischi, ai fini di un partenariato strategico tra il settore privato, gli Stati membri e i ricercatori.

3.2.1 La comunicazione prevede, inoltre, una maggiore responsabilizzazione dei soggetti interessati sui bisogni e sui rischi in materia di sicurezza.

3.2.2 Per quanto attiene alla cooperazione internazionale e con i paesi terzi, «la dimensione globale delle reti e dell'informazione impone alla Commissione di moltiplicare i suoi sforzi, sia a livello internazionale che in coordinamento con gli Stati membri, per promuovere una collaborazione globale sulla sicurezza delle reti e dell'informazione» ([18]): tale indicazione non viene però ripresa nelle azioni di dialogo, partenariato e responsabilizzazione.

4. **Osservazioni**

4.1 Il Comitato condivide le analisi e gli argomenti che giustificano una strategia europea integrata e dinamica per la sicurezza delle reti e dell'informazione, in quanto ritiene che la questione della sicurezza sia essenziale per incoraggiare un atteggiamento più favorevole all'applicazione delle TI e accrescere la fiducia in queste ultime. Le posizioni del CESE sono d'altronde già state illustrate in numerosi pareri ([19]).

4.1.1 Il Comitato ribadisce ancora una volta ([20]) che «la rete Internet e le nuove tecnologie di comunicazione on-line (ad esempio, la telefonia mobile o i PDA con funzioni multimediali e in grado di connettersi in rete, che sono in piena espansione) costituiscono strumenti fondamentali per lo sviluppo dell'economia della conoscenza, della *e-economy* e dell'amministrazione on-line».

([16]) *Multivariate Statistical Analysis for Network Attacks Detection*. Guangzhi Qu, Salim Hariri* — 2005 USA, Arizona
Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, USA — Lavoro finanziato in parte dalla Intel Corporation IT R&D Council.

([17]) COM(2006) 251 def. del 31.5.2006.

([18]) Cfr. COM(2006) 251 def., penultimo paragrafo cap. 3.

([19]) Cfr. i seguenti documenti:
— parere del CESE in merito alla *Proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE*, GU C 69 del 21.3.2006, pag. 16,
— parere del CESE in merito alla *Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni «i2010 — Una società europea dell'informazione per la crescita e l'occupazione»*, GU C 110 del 9.5.2006, pag. 83,
— parere del CESE in merito alla *Proposta di decisione del Parlamento europeo e del Consiglio che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie on-line*, GU C 157 del 28.6.2005, pag. 136,
— parere del CESE in merito alla *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni — Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, GU C 48 del 21.2.2002, pag. 33.

([20]) Cfr. nota 19, terzo trattino.

4.2 *Per un maggior vigore delle proposte della Commissione*

4.2.1 Il Comitato ritiene tuttavia possibile ampliare ulteriormente l'approccio proposto dalla Commissione, che consiste nel basare la sua strategia integrata e dinamica su un dialogo aperto e inclusivo e su un partenariato rafforzato con tutte le parti interessate e, in particolare, con gli utenti, nonché su una loro maggiore responsabilizzazione.

4.2.2 Tale posizione è stata già sottolineata in precedenti pareri: «Per essere efficace, questa azione di contrasto deve coinvolgere direttamente tutti gli utenti di Internet, i quali devono essere formati e informati sulle precauzioni da adottare e sui mezzi da impiegare per premunirsi contro la ricezione di contenuti nocivi o indesiderati, o per evitare di essere utilizzati come intermediari di tali contenuti. A giudizio del Comitato, la parte del programma relativa alla formazione e all'informazione deve quindi accordare assoluta priorità al coinvolgimento degli utenti» ([21]).

4.2.3 Il coinvolgimento degli utenti e dei cittadini deve però avvenire, a giudizio del Comitato, in modo da conciliare la necessaria protezione dell'informazione e delle reti con le libertà civili e il diritto degli utenti a beneficiare di accessi sicuri e a costi contenuti.

4.2.4 Occorre considerare che la ricerca di sicurezza informatica rappresenta un costo per il consumatore anche in termini di tempo perduto per rimuovere o aggirare gli ostacoli. Secondo il Comitato, sarebbe necessario stabilire l'obbligo di inserire automaticamente in ogni computer dei sistemi di protezione antivirus, che l'utente potrà attivare o meno ma che saranno comunque presenti «ab origine» nel prodotto.

4.3 *Per una strategia comunitaria più dinamica e innovativa*

4.3.1 Oltre a questo, secondo il Comitato, l'Unione dovrebbe porsi obiettivi più ambiziosi e varare una strategia innovativa, integrata e dinamica, con il lancio di nuove iniziative come, ad esempio le seguenti:

— l'introduzione di meccanismi che permettano una identificazione digitale dei singoli utenti, troppo spesso sollecitati a fornire i propri dati anagrafici,

— azioni, messe in atto tramite l'ETSI ([22]), che fungano da requisito per un uso sicuro delle TIC e che possano offrire soluzioni puntuali e veloci, definite secondo una soglia comune di sicurezza in tutta l'Unione,

— azioni di prevenzione, attraverso l'integrazione dei requisiti minimi di sicurezza nei sistemi informatici e di rete e il lancio di azioni pilota mediante corsi di sicurezza organizzati nelle scuole di ogni ordine e grado,

— creazione, a livello europeo, di un quadro giuridico-normativo certo e riconosciuto. Tale quadro, applicato all'informatica e alle reti, consentirebbe di passare dalla sicurezza informatica all'assicurazione informatica,

— rafforzamento dei meccanismi europei e nazionali di valutazione dei rischi e miglioramento della capacità di applicazione delle disposizioni legislative e regolamentari per colpire i crimini informatici compiuti sulla privacy e sugli archivi di dati,

— azioni volte ad evitare l'emergere di monoculture informatiche che utilizzano prodotti e soluzioni particolarmente vulnerabili. Appoggio a innovazioni pluriculturali diversificate volte alla realizzazione di uno Spazio unico europeo dell'informazione (SEIS — *Single European Information Space*).

4.3.2 Secondo il CESE sarebbe opportuna la creazione di un *ICT-Security Focal Point inter DG* ([23]). Il *Focal Point* consentirebbe di agire:

— a livello dei servizi della Commissione,

— a livello dei singoli Stati, attraverso soluzioni orizzontali per gli aspetti di interoperatività, gestione dell'identità, protezione della vita privata, libertà d'accesso all'informazione e ai servizi, requisiti minimi di sicurezza,

— a livello internazionale, per poter assicurare che l'UE parli con una voce sola nei vari contesti internazionali come ONU, G8, OCSE, ISO.

4.4 *Per un rafforzamento delle azioni UE di coordinamento responsabile*

4.4.1 Il CESE attribuisce molta importanza anche alla creazione di una rete europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Network*), attraverso la quale si possano promuovere inchieste, studi e *workshop* sui meccanismi di sicurezza e sulla loro interoperabilità, sulla criptografia avanzata e sulla protezione della vita privata.

4.4.2 Il CESE ritiene che per questo settore così delicato sarebbe opportuno ottimizzare il ruolo della ricerca europea attraverso una opportuna sintesi del contenuto dei programmi seguenti:

— Programma europeo di ricerca sulla sicurezza (ESRP) ([24]), lanciato nell'ambito del Settimo programma quadro di RST,

([21]) Cfr. nota 19, terzo trattino.

([22]) ETSI, *European Telecomunications Standards Institute*: cfr. in particolare il *workshop* del 16 e 17 gennaio 2006. L'ETSI ha elaborato, fra l'altro, delle specifiche sulle intercettazioni illegali (TS 102 232; 102 233; 102 234), sugli accessi Internet lan wireless (TR 102 519) e sulle firme elettroniche, e ha sviluppato algoritmi di sicurezza per GSM GPRS e UMTS.

([23]) Tale *Focal Point inter DG* potrebbe essere finanziato nell'ambito della priorità IST del programma specifico Cooperazione del Settimo programma quadro di RST, o dal programma europeo di ricerca sulla sicurezza ESRP.

([24]) Cfr. Settimo programma quadro di RST&D — programma specifico Cooperazione — priorità tematica «Sicurezza», con un bilancio di 1,35 miliardi di euro per il periodo 2007-2013.

— Programma *Safer Internet Plus*,

— Programma europeo per la protezione delle infrastrutture critiche (EPCIP) ([25]).

4.4.3 A questi suggerimenti si potrebbe aggiungere il lancio di una «Giornata europea del computer sicuro», sostenuta da campagne nazionali di educazione nelle scuole e da azioni di aggiornamento dei consumatori sulle procedure di protezione delle informazioni diffuse tramite PC e sui progressi tecnologici registrati nel vasto e mutevole campo degli elaboratori elettronici.

4.4.4 Il Comitato ha più volte sottolineato che «la velocità con cui le imprese ricorreranno all'uso delle TIC dipende dalle garanzie di sicurezza che verranno date e dalla fiducia nelle transazioni elettroniche. La disponibilità dei consumatori a rendere noti i dati della carta di credito su una *homepage* dipende, essenzialmente, dalla percezione che essi hanno della sicurezza di questo genere di transazione» ([26]).

4.4.5 Il Comitato è convinto che, dato l'enorme potenziale di crescita del settore, è necessario da un lato attivare delle politiche specifiche e dall'altro adeguare le politiche attuali ai nuovi sviluppi. È in particolare necessario collegare con una strategia integrata le iniziative europee in materia di sicurezza informatica, rimuovendo i confini settoriali e garantendo una diffusione omogenea e sicura delle TIC nella società.

4.4.6 Secondo il Comitato, alcune strategie importanti, come quella oggetto del presente parere, procedono con eccessiva lentezza a causa delle difficoltà burocratiche e culturali frapposte dagli Stati membri alle indispensabili decisioni che devono essere assunte a livello comunitario.

4.4.7 Il Comitato è anche dell'avviso che le risorse comunitarie siano insufficienti per realizzare i numerosi e urgenti progetti, necessari a dare delle risposte concrete ai nuovi problemi della globalizzazione ma in grado di raggiungere dei risultati solo se realizzati a livello europeo.

4.5 *Per maggiori garanzie di protezione del consumatore a livello dell'UE*

4.5.1 Il Comitato è consapevole che gli Stati membri hanno varato misure tecnologiche di sicurezza e procedure di gestione della sicurezza secondo esigenze loro proprie e con la tendenza a concentrarsi su aspetti diversi. Anche per questo motivo risulta difficile fornire una risposta univoca, davvero efficace ai problemi di sicurezza. Ad eccezione di alcune reti amministrative, non esiste una cooperazione transfrontaliera sistematica tra gli Stati membri, nonostante sia noto che le questioni di sicurezza non possono essere affrontate isolatamente dai singoli paesi.

4.5.2 Il Comitato rileva peraltro che il Consiglio, con la decisione quadro 2005/222/GAI, ha varato un sistema di cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri per garantire un approccio coerente da parte di questi ultimi, mediante il ravvicinamento delle loro legislazioni penali nel settore degli attacchi contro i sistemi di informazione, in tema di:

— accesso illecito ai sistemi di informazione,

— interferenza illecita per quanto riguarda i sistemi, mediante atto intenzionale teso a ostacolare gravemente o a interrompere il funzionamento di un sistema di informazione,

— interferenza illecita per quanto riguarda i dati, mediante atto intenzionale di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione,

— istigazione, favoreggiamento o complicità in ordine ai reati di cui sopra.

4.5.3 Inoltre, la decisione indica i criteri per stabilire la responsabilità delle persone giuridiche e le eventuali sanzioni che possono essere loro applicate qualora quest'ultima sia stata accertata.

4.5.4 Nell'ambito del dialogo con le autorità pubbliche degli Stati membri, il Comitato appoggia la proposta della Commissione perché dette autorità avviino un esercizio di valutazione comparativa delle proprie politiche nazionali in materia di sicurezza delle reti e dei sistemi informatici, ivi comprese quelle specifiche per il settore pubblico. Tale suggerimento, peraltro, era già contenuto in un parere del CESE del 2001 ([27]).

4.6 *Per una cultura della sicurezza più diffusa*

4.6.1 Per quanto attiene al coinvolgimento dell'industria della sicurezza informatica, quest'ultima deve garantire realmente, per proteggere il diritto dei propri clienti alla vita privata e alla riservatezza dei dati personali, l'uso dei sistemi di sorveglianza materiale delle proprie installazioni e della codificazione delle comunicazioni, in funzione dell'evoluzione delle tecniche ([28]).

([25]) COM(2005) 576 def. del 17.11.2005.
([26]) Cfr. nota 19, secondo trattino.
([27]) Cfr. nota 19, quarto trattino.
([28]) Cfr. direttiva 97/66/CE *Trattamento dei dati personali nel settore telecomunicazioni* (GU L 24 del 30.1.1998).

4.6.2 Per quanto concerne l'azione di sensibilizzazione, il Comitato ritiene fondamentale che venga creata una vera e propria «cultura della sicurezza», concepita in modo pienamente compatibile con la libertà d'informazione, di comunicazione e di espressione. Esso ricorda d'altro canto che numerosi utenti non sono consapevoli di tutti i rischi legati alla pirateria informatica mentre molti operatori, venditori o fornitori di servizi non riescono a valutare l'esistenza e l'ampiezza degli aspetti vulnerabili.

4.6.3 Se la tutela della vita privata e dei dati personali sono obiettivi prioritari, i consumatori hanno anche il diritto di essere protetti in maniera realmente efficace contro la schedatura abusiva di profili nominativi attraverso software «spia» (*spyware* e *web bugs*) o mediante altri metodi. Dovrebbe anche essere frenata la pratica dello *spamming* ([29]) (invio massiccio di messaggi non sollecitati) che spesso deriva da questi abusi. Tali intrusioni hanno infatti un costo per le vittime ([30]).

4.7 *Per un'Agenzia UE più forte e attiva*

4.7.1 Il Comitato vede con favore un ruolo più incisivo e rafforzato dell'Agenzia europea per la sicurezza delle reti e dell'informazione (AESRI/ENISA) sia per l'azione di sensibilizzazione sia anche, e soprattutto, per azioni di informazione e formazione di operatori e utenti, come peraltro da esso già indicato nel suo recente parere ([31]) in tema di fornitura di servizi pubblici di comunicazione elettronica.

4.7.2 Per quanto concerne infine le azioni proposte in tema di responsabilizzazione di ciascun gruppo di soggetti interessati, queste appaiono orientate ad una stretta osservanza del principio di sussidiarietà. Esse infatti ricadono sugli Stati membri o sul settore privato, in relazione alle specifiche responsabilità.

4.7.3 L'Agenzia dovrebbe potersi giovare dei contributi offerti dalla rete europea per la sicurezza delle reti e dell'informazione (*European Network and Information Security Network*) per l'organizzazione di attività congiunte; essa dovrebbe parimenti sfruttare il portale comunitario plurilingue di allerta rischi informatici per poter fornire informazioni personalizzate e interattive, con linguaggi facilitati, soprattutto agli utenti singoli di ogni età e alle piccole e medie imprese.

Bruxelles, 16 febbraio 2007.

Il Presidente

del Comitato economico e sociale europeo

Dimitris DIMITRIADIS

([29]) In francese, «pollupostage».

([30]) Cfr. pareri CESE sui temi: *Reti di comunicazioni elettronica* (GU C 123 del 25.4.2001, pag. 50), *Commercio elettronico* (GU C 169 del 16.6.1999, pag. 36) e *Ripercussioni del commercio elettronico sul mercato unico* (GU C 123 del 25.4.2001, pag. 1).

([31]) Cfr. nota 19, primo trattino.