Parere del Comitato economico e sociale europeo in merito alla «Proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione»

COM(2013) 48 final — 2013/0027 (COD)

(2013/C 271/25)

Relatore: **McDONOGH**

Il Consiglio, in data 21 febbraio 2013, e il Parlamento europeo, in data 15 aprile 2013, hanno deciso, conformemente al disposto dell'articolo 114 del Trattato sul funzionamento dell'Unione europea, di consultare il Comitato economico e sociale europeo in merito alla:

Proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte ad garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione.

COM(2013) 48 final – 2013/0027 (COD).

La sezione specializzata Trasporti, energia, infrastrutture, società dell'informazione, incaricata di preparare i lavori del Comitato in materia, ha adottato il proprio parere in data 30 aprile 2013.

Alla sua 490ª sessione plenaria, dei giorni 22 e 23 maggio 2013, (seduta del 22 maggio), il Comitato economico e sociale europeo ha adottato il seguente parere con 163 voti favorevoli, 1 voto contrario e 4 astensioni.

1. **Conclusioni e raccomandazioni**

1.1 Il Comitato economico e sociale europeo (CESE) prende atto della proposta di direttiva, che andrebbe esaminata nel più ampio contesto della *Strategia dell'Unione europea per la cibersicurezza* ([1]), un documento pubblicato di recente che delinea una visione globale per la sicurezza delle reti e dell'informazione al fine di garantire una crescita sicura dell'economia digitale facendo avanzare al tempo stesso i valori europei di libertà e democrazia.

1.2 Il CESE accoglie favorevolmente la proposta di direttiva all'esame il cui obiettivo è di garantire un elevato livello comune di sicurezza delle reti e dell'informazione in tutta l'UE. Armonizzare e gestire la sicurezza delle reti e dell'informazione a livello europeo è essenziale per il completamento del mercato unico digitale e per il corretto funzionamento del mercato interno nel suo complesso. Il Comitato condivide le preoccupazioni della Commissione circa il gravissimo danno che potrebbe essere arrecato all'economia e al benessere dei cittadini in caso di mancato funzionamento del sistema di sicurezza delle reti e dell'informazione. La direttiva proposta tuttavia non risponde alle aspettative del Comitato di un'azione legislativa forte su questo tema d'importanza cruciale.

1.3 Il CESE esprime profondo disappunto in quanto numerosi Stati membri non hanno compiuto passi avanti verso l'effettiva attuazione delle misure nel campo della sicurezza delle reti e dell'informazione a livello nazionale. Il Comitato è preoccupato per l'aumento dei rischi che questa situazione crea per i cittadini e per l'impatto negativo che avrà sul completamento del mercato unico digitale. Tutti gli Stati membri dovrebbero adoperarsi senza ulteriori ritardi per adempiere agli obblighi tuttora non rispettati in materia di sicurezza delle reti e dell'informazione.

1.4 Questa mancanza di passi avanti è all'origine di un nuovo divario digitale tra una *élite* formata da paesi con un grado di sicurezza delle reti e dell'informazione molto elevato e gli Stati membri in ritardo. Tale divario incide negativamente sulla fiducia e la collaborazione a livello UE per quanto concerne la sicurezza delle reti e dell'informazione. Se non verrà affrontato con urgenza, questo problema potrebbe provocare disfunzioni nel mercato unico legate alle diverse capacità dei vari paesi.

1.5 Come sostenuto in precedenti pareri ([2]), il CESE è dell'avviso che le misure sperimentali e volontarie non funzionino e che sia necessario imporre forti obblighi regolamentari agli Stati membri onde garantire l'armonizzazione, la gestione e l'applicazione delle misure in materia di sicurezza delle reti e dell'informazione a livello europeo. Purtroppo, il CESE ritiene che la proposta di direttiva all'esame non risponda alla necessità di una normativa chiara e risolutiva. A suo parere un regolamento che definisca obblighi vincolanti ben precisi per gli Stati membri fornirebbe, più efficacemente di una direttiva, l'elevato livello comune richiesto per quanto concerne la sicurezza delle reti e dell'informazione.

1.6 Nonostante l'intenzione della Commissione di adottare atti delegati al fine di garantire una serie di condizioni armonizzate per l'attuazione di alcune parti della direttiva, il Comitato giudica che il testo proposto presenti una mancanza di standard, di definizioni chiare e di obblighi vincolanti, il che offre agli Stati membri un'eccessiva flessibilità nell'interpretarne e nel recepirne gli elementi di maggior rilievo. Il CESE chiede che il documento all'esame contenga definizioni più precise degli standard, dei requisiti e delle procedure che gli Stati membri, le pubbliche autorità, gli operatori del mercato e i facilitatori di servizi internet fondamentali sono tenuti ad osservare.

([1]) *Un ciberspazio aperto e sicuro*, JOIN(2013) 1.

([2]) Parere del CESE sul tema *Proteggere le infrastrutture critiche informatizzate* (GU C 255 del 22.9.2010, pag. 98) e sul tema *Attacchi contro i sistemi d'informazione* (GU C 218 del 23.7.2011, pag. 130).

1.7 Per rafforzare l'elaborazione della strategia e l'attuazione nel campo della sicurezza delle reti e dell'informazione nell'UE, il Comitato chiede che venga istituita un'apposita autorità a livello UE, analoga all'autorità centrale creata nel settore dell'aviazione (AESA) ([3]). Questa autorità dovrebbe stabilire delle norme - e vigilare sulla loro effettiva applicazione - per tutti gli elementi che compongono la sicurezza delle reti e dell'informazione nell'UE, dalla certificazione e l'impiego di dispositivi terminali sicuri alla sicurezza delle reti e dei dati.

1.8 Il CESE si rende perfettamente conto dei maggiori rischi per la sicurezza informatica e la protezione dei dati derivanti dall'adozione del *cloud computing* in Europa ([4]). Chiede pertanto che il documento proposto introduca esplicitamente requisiti e obblighi specifici e aggiuntivi in materia di sicurezza per quanto concerne la fornitura e l'uso di servizi offerti dal *cloud computing*.

1.9 Perché vi sia un'adeguata assunzione di responsabilità nell'ambito della sicurezza delle reti e dell'informazione, la proposta dovrebbe specificare chiaramente che gli enti incaricati di adempiere agli obblighi previsti dalla direttiva stessa hanno il diritto di ritenere i fornitori di software e hardware responsabili per qualsiasi difetto dei loro prodotti o servizi che possa contribuire direttamente ad incidenti nel campo della sicurezza delle reti e dell'informazione.

1.10 Il CESE chiede agli Stati membri di attribuire una particolare importanza all'aumento delle conoscenze in materia di sicurezza delle reti e dell'informazione e delle competenze delle piccole e medie imprese (PMI) in materia di sicurezza informatica. Richiama inoltre l'attenzione della Commissione sul successo delle «competizioni tra hacker» negli Stati Uniti ([5]) e in taluni Stati membri ([6]), e sulla necessità sia di una maggiore sensibilizzazione alla sicurezza informatica sia alla formazione della prossima generazione di esperti nel campo della sicurezza delle reti e dell'informazione.

1.11 Poiché è importante che tutti gli Stati membri rispettino le prescrizioni sulla sicurezza delle reti e dell'informazione nell'intera UE, il CESE chiede alla Commissione di riflettere su quali finanziamenti a titolo del quadro finanziario pluriennale (QFP) possano essere destinati all'osservanza delle norme in questo campo, con l'obiettivo di aiutare gli Stati membri che necessitino di un'assistenza finanziaria.

1.12 La spesa in materia di ricerca, sviluppo e innovazione (RS&I) per le tecnologie relative alla sicurezza delle reti e dell'informazione dovrebbe essere una priorità fondamentale nell'ambito del programma quadro dell'UE per la ricerca e l'innovazione «Orizzonte 2020», affinché l'Europa si tenga costantemente pronta ad affrontare le nuove e diverse minacce informatiche man mano che si presentano.

1.13 Per aiutare a stabilire con chiarezza quali entità abbiano la responsabilità giuridica in base alla direttiva proposta, il Comitato auspica che venga introdotto l'obbligo per gli Stati membri di pubblicare un repertorio, consultabile online, di tutti i fornitori di infrastrutture critiche informatizzate che devono soddisfare i criteri di gestione dei rischi e di rendicontazione prescritti dalla direttiva Una tale prova di trasparenza e di assunzione di responsabilità da parte dei poteri pubblici servirebbe a rafforzare tanto la fiducia quanto il rispetto delle norme.

1.14 Il CESE richiama l'attenzione della Commissione sul gran numero di propri precedenti pareri dedicati al tema della sicurezza delle reti e dell'informazione, nei quali sottolineava l'esigenza di una società dell'informazione sicura e insisteva sulla necessità di proteggere le infrastrutture critiche ([7]).

2. **Contenuto essenziale della proposta della Commissione**

2.1 La Commissione ha pubblicato la proposta di direttiva sulla sicurezza delle reti e dell'informazione contemporaneamente alla *Strategia dell'Unione europea per la cibersicurezza*, i cui obiettivi sono rafforzare la resilienza dei sistemi d'informazione, ridurre la criminalità informatica, potenziare la politica internazionale dell'UE in materia di sicurezza e difesa informatiche e, infine, sviluppare le risorse industriali e tecnologiche per la sicurezza informatica, promuovendo nel contempo i diritti fondamentali e altri valori costitutivi dell'Unione.

2.2 Con «sicurezza delle reti e dell'informazione» s'intende la protezione di Internet e di altre reti, sistemi informativi e servizi di sostegno a questi strumenti su cui si fonda il funzionamento della nostra società. La sicurezza delle reti e dell'informazione è essenziale per un corretto funzionamento del mercato interno.

2.3 L'approccio puramente facoltativo alla sicurezza delle reti e dell'informazione adottato finora dall'UE non fornisce un'adeguata protezione contro i rischi in materia. Le capacità esistenti in questo campo non sono sufficienti a tenere il ritmo delle nuove e diverse minacce che sorgono nel settore e ad assicurare un elevato livello comune di protezione in tutti gli Stati membri.

([3]) Agenzia europea per la sicurezza aerea (AESA): http://easa.europa.eu/

([4]) Parere del CESE sul tema *Il* cloud computing *in Europa* (GU C 24 del 28.1.2012, pag. 40) e sul tema *Sfruttare il potenziale del* cloud computing *in Europa* (GU C 76 del 14.3.2013, pag. 59).

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) Parere del CESE sul tema *Una strategia per una società dell'informazione sicura*, GU C 97 del 28.4.2007, pag. 21.
Parere del CESE sul tema *Proteggere le infrastrutture critiche informatizzate*, GU C 255 del 22.9.2010, pag. 98.
Parere del CESE sul tema *«Nuovo» regolamento ENISA*, GU C 107 del 6.4.2011, pag. 58.
Parere del CESE sul tema *Regolamento generale sulla protezione dei dati*, GU C 229 del 31.7.2012, pag. 90.
Parere del CESE sul tema *Attacchi contro i sistemi di informazione*, GU C 218 del 23.7.2011, pag. 130.
Parere del CESE sul tema *Transazioni elettroniche nel mercato interno*, GU C 351 del 15.11.2012, pag. 73.
Parere del CESE sul tema *Sfruttare il potenziale del* cloud computing *in Europa*, GU C 76 del 14.3.2013, pag. 59.

2.4 Attualmente, i livelli di capacità e di preparazione variano notevolmente da uno Stato membro all'altro, il che porta ad adottare approcci frammentati alla sicurezza delle reti e dell'informazione nell'UE. Dato che le reti e i sistemi sono interconnessi, gli Stati membri che presentano un grado insufficiente di protezione finiscono per indebolire la sicurezza globale delle reti e dell'informazione dell'intera Unione. Questa situazione inoltre ostacola la creazione di un clima di fiducia tra pari, che rappresenta il presupposto essenziale per la cooperazione e la condivisione delle informazioni. Di conseguenza, la cooperazione esiste solo tra un numero limitato di Stati membri che registrano un elevato livello di capacità.

2.5 La direttiva all'esame, proposta in conformità dell'articolo 114 del TFUE, persegue l'obiettivo di facilitare il completamento e il corretto funzionamento del mercato unico digitale. Essa si prefigge di:

— stabilire un livello comune minimo di sicurezza delle reti e dell'informazione negli Stati membri aumentando così il livello generale di preparazione e risposta agli incidenti;

— migliorare la collaborazione a livello dell'UE in materia di sicurezza delle reti e dell'informazione per lottare contro le minacce e gli incidenti transfrontalieri;

— creare una cultura di gestione dei rischi e migliorare lo scambio di informazioni tra i settori pubblico e privato.

2.6 La proposta di direttiva stabilisce una serie di obblighi giuridici, tra cui i seguenti:

a) ogni Stato membro è tenuto ad adottare una strategia nazionale nel campo della sicurezza delle reti e dell'informazione, e a designare un'autorità nazionale competente in materia, dotata di adeguate risorse finanziarie e umane, al fine di prevenire, gestire e rispondere ai rischi e incidenti in questo ambito;

b) occorre creare un meccanismo di cooperazione tra gli Stati membri e la Commissione che consenta di lanciare preallarmi su rischi e incidenti; occorre inoltre collaborare e realizzare periodicamente delle valutazioni tra pari;

c) determinati tipi di enti in tutta l'UE devono adottare misure di gestione dei rischi e riferire alle loro autorità nazionali competenti circa gli incidenti aventi un impatto significativo sulla sicurezza dei loro servizi principali. Tra gli enti incaricati dell'adempimento di tali obblighi figurano gli operatori di infrastrutture critiche informatizzate in alcuni settori (servizi finanziari, trasporti, energia, sanità), i facilitatori di servizi della società dell'informazione (in particolare *cloud computing*, piattaforme di commercio elettronico, pagamento via internet, motori di ricerca, *app store* [portali per scaricare o acquistare applicazioni o altri prodotti] e reti sociali) e le pubbliche amministrazioni.

2.7 Gli Stati membri dovranno attuare la direttiva entro 18 mesi dalla sua adozione da parte del Consiglio e del Parlamento europeo (prevista nel corso del 2014).

3. **Osservazioni generali**

3.1 La crescita di Internet e della società digitale ha un profondo impatto sulla vita di tutti i giorni. Tuttavia, con l'aumento della nostra dipendenza da Internet, la nostra libertà, la nostra ricchezza e la nostra qualità della vita sono sempre più dipendenti da una solida sicurezza delle reti e dell'informazione: ad esempio, se in un caso di emergenza Internet non funziona e non è possibile avere accesso ai dati clinici informatizzati, il paziente può anche morire. La sicurezza delle infrastrutture critiche informatizzate in Europa è sempre più minacciata e il nostro livello di sicurezza delle reti e dell'informazione non è adeguato.

3.2 Lo scorso anno, il direttore di Europol ha dichiarato di essere «molto preoccupato da questa fiducia, ampiamente mal riposta, nell'indistruttibilità di Internet» ([8]). Spesso si ha notizia di nuovi attacchi informatici su infrastrutture essenziali ad opera di criminali, terroristi o governi di altri paesi. Le vittime di questi attacchi preferiscono tenere la cosa nascosta perché temono danni d'immagine: nelle ultime settimane tuttavia, si è assistito ad attacchi informatici contro l'infrastruttura Internet dell'Europa ([9]), e dei sistemi bancari ([10]), attacchi impossibili da nascondere per la loro portata eccessivamente distruttiva. In una relazione ([11]), si afferma che nel 2011 i Paesi Bassi hanno subito 92 milioni di attacchi informatici e la Germania 82 milioni. Secondo le stime del governo britannico, sempre nel 2011 il Regno Unito ha subito 44 milioni di attacchi informatici, con un costo per l'economia di 30 miliardi di euro ([12]).

3.3 Nel 2007, il Consiglio dell'UE ha affrontato il problema della sicurezza delle reti e dell'informazione in Europa ([13]). Ma l'approccio politico seguito da allora ([14]) è stato principalmente improntato all'azione volontaria degli Stati membri. Di questi ultimi, solo una minoranza ha adottato azioni concrete. Il Comitato fa osservare che numerosi Stati membri non hanno ancora pubblicato una strategia nazionale sulla sicurezza informatica né hanno messo a punto un piano d'emergenza in caso d'incidente informatico. Alcuni di loro non hanno ancora provveduto a istituire una squadra di pronto intervento informatico (*Computer Emergency Response Team* - CERT). Infine, un certo numero di Stati membri non ha ancora ratificato la Convenzione del Consiglio d'Europa sulla criminalità informatica ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UK Cyber Security Strategy – Landscape Review: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Risoluzione del Consiglio 2007/C 68/01.
([14]) COM(2006) 251 e COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 I dieci Stati membri più avanzati in materia di sicurezza delle reti e dell'informazione hanno formato il gruppo EGC (gruppo europeo governativo di gruppi di intervento per la sicurezza informatica in caso di incidente), composto di squadre che collaborano per garantire la sicurezza delle reti e dell'informazione e per dare una risposta ad eventuali incidenti. L'adesione all'EGC è al momento chiusa: gli altri 17 Stati membri meno avanzati e la CERT-EU ([16]), di recente creazione, sono per ora esclusi da questo gruppo di élite. Un nuovo divario digitale si sta formando, quello tra i paesi più avanzati in materia di sicurezza delle reti e dell'informazione e gli altri paesi. Se non sarà colmato, tale divario attaccherà il cuore del mercato unico digitale e ostacolerà la creazione di un clima di fiducia limitando al tempo stesso l'armonizzazione e l'interoperabilità. Inoltre, senza un'azione decisa, il divario tra gli Stati membri più avanzati e meno avanzati potrebbe aumentare e questo provocherebbe ulteriori disfunzioni nel mercato interno legate alle differenze di capacità tra i vari paesi.

3.5 Il successo della strategia sulla sicurezza informatica e l'efficacia della direttiva proposta nel campo della sicurezza delle reti e dell'informazione dipenderà dall'esistenza di un settore forte in Europa e da un numero sufficiente di lavoratori dotati di competenze specializzate in materia. Il CESE si compiace che la proposta di direttiva faccia riferimento all'esigenza che gli Stati membri investano nelle conoscenze, nella sensibilizzazione e nella formazione in materia di sicurezza delle reti e dell'informazione. Tuttavia il Comitato chiede anche che gli Stati membri portino avanti sforzi particolari per informare, istruire e sostenere il settore delle PMI in materia di sicurezza informatica. Le grandi imprese possono acquisire facilmente le conoscenze necessarie mentre le PMI hanno bisogno di un sostegno.

3.6 Il CESE è pronto a collaborare con l'ENISA (l'Agenzia europea per la sicurezza delle reti e dell'informazione) al fine di promuovere la sicurezza delle reti e dell'informazione durante il mese della sicurezza informatica, un evento che si terrà più avanti nel corso dell'anno. Per quanto concerne l'obiettivo, fissato sia dalla strategia sulla sicurezza informatica sia dalla proposta di direttiva all'esame, di sviluppare una cultura della sicurezza in tutta l'Unione e di incrementare il livello di competenze nel campo della sicurezza delle reti e dell'informazione, il Comitato richiama l'attenzione della Commissione sulle cosiddette «competizioni tra hacker» in voga tra gli adolescenti, che hanno contribuito a sensibilizzare, sia in alcuni Stati membri sia negli Stati Uniti, l'opinione pubblica su questo fenomeno.

3.7 Il Comitato si compiace inoltre che la strategia sulla sicurezza informatica preveda che una parte dei finanziamenti a favore della ricerca, sviluppo e innovazione siano destinati alle tecnologie nel campo della sicurezza delle reti e dell'informazione.

3.8 Lo sviluppo del *cloud computing* comporta la necessità di far fronte ad un gran numero di nuovi pericoli nel campo della sicurezza informatica. Oggi, ad esempio, i criminali informatici dispongono di un'enorme potenza di elaborazione fornita dai computer con una spesa relativamente modica. Inoltre, i dati di migliaia di imprese si trovano ora immagazzinati in banche dati centralizzate che sono vulnerabili ad attacchi mirati. Il CESE ha già raccomandato una maggiore resilienza informatica nel campo del *cloud computing* ([17]).

([16]) La CERT-EU è un gruppo permanente di risposta alle emergenze informatiche al servizio delle istituzioni, delle agenzie e degli organi dell'UE.

([17]) Parere del CESE sul tema *Il* cloud computing *in Europa*, GU C 24 del 28.1.2012, pag. 40 e *Sfruttare il potenziale del* cloud computing *in Europa*, GU C 76 del 14.3.2013, pag. 59.

3.9 Il Comitato ha già chiesto di introdurre un sistema volontario di carta d'identità elettronica a livello europeo, per le operazioni online, che sia di complemento ai sistemi esistenti a livello nazionale. Un sistema del genere offrirebbe una protezione più efficace contro le frodi, un clima di maggiore fiducia tra gli operatori economici, costi più bassi per la fornitura di servizi di migliore qualità e una protezione rafforzata per i cittadini.

4. **Osservazioni specifiche**

4.1 Purtroppo, la proposta di direttiva sulla sicurezza delle reti e dell'informazione presentata dalla Commissione è troppo incerta, non è sufficientemente precisa e dipende in modo eccessivo dall'autoregolamentazione degli Stati membri. La mancanza di standard, di definizioni chiare e di obblighi vincolanti, in particolare al Capo IV, offre agli Stati membri un'eccessiva flessibilità nell'interpretare e nel recepire gli elementi di maggior rilievo del testo legislativo. Per il CESE, un regolamento, che definisca in modo appropriato obblighi giuridici vincolanti per gli Stati membri, sarebbe più efficace di una direttiva.

4.2 Il CESE rileva che l'articolo 6 della proposta di direttiva stabilisce che ciascuno Stato membro designa una «autorità competente» incaricata di controllare l'applicazione della direttiva e di garantirne un'attuazione uniforme in tutta l'Unione. Osserva inoltre che l'articolo 8 istituisce una «rete di collaborazione» che, grazie alle competenze di cui è dotata insieme a quelle di cui dispone la Commissione, guida e dirige a livello dell'intera Unione e, se necessario, provvede all'effettiva applicazione delle norme anche a livello dei singoli Stati membri. Sulla base di questa struttura di *governance*, il CESE ritiene che l'UE dovrebbe prendere in considerazione l'istituzione di un'autorità di livello UE in materia di sicurezza delle reti e dell'informazione con compiti simili a quelli dell'Agenzia europea per la sicurezza aerea (AESA), la quale stabilisce le norme e gestisce l'applicazione e il rispetto delle misure di sicurezza per quanto concerne gli aeromobili, gli aeroporti e le compagnie aeree.

4.3 L'autorità europea proposta dal CESE al precedente punto 4.2. potrebbe basarsi sul lavoro in materia di sicurezza informatica già portato avanti dall'ENISA, dal Comitato europeo di normalizzazione (CEN), dalle CERT, dal gruppo EGC e da altri enti. Questa autorità dovrebbe stabilire delle norme - e vigilare sulla loro effettiva applicazione - per tutti gli elementi che compongono la sicurezza delle reti e dell'informazione, dalla certificazione e l'impiego di dispositivi terminali sicuri alla sicurezza delle reti e dei dati.

4.4 A causa dell'elevato grado di dipendenza tra gli Stati membri nel garantire la sicurezza delle reti e dell'informazione in tutta l'UE e dati i costi potenzialmente molto alti in caso di incidente per tutte le parti interessate, il CESE chiede che la legislazione preveda sanzioni esplicite e proporzionate in caso di mancata osservanza, e che tali sanzioni siano armonizzate al fine di rispecchiare la dimensione paneuropea della responsabilità e il livello di danno che potrebbe derivarne non solo per il mercato nazionale ma anche per l'intera l'Unione. L'articolo 14 della proposta, relativo alle sanzioni, è generico, concede agli Stati membri un eccessivo potere discrezionale in materia e non fornisce orientamenti adeguati che tengano conto degli effetti transfrontalieri e paneuropei.

4.5 Oggi i governi e i fornitori di servizi essenziali non rendono pubbliche le disfunzioni dei sistemi di sicurezza e di resilienza, salvo quando sono obbligati a farlo. Questa mancanza di trasparenza compromette la capacità dell'Europa di reagire tempestivamente ed efficacemente alle minacce alla sicurezza informatica, oltre che la capacità di rafforzare la sicurezza generale delle reti e dell'informazione grazie ad un apprendimento condiviso. Il Comitato plaude alla decisione della Commissione di rendere obbligatoria, per gli operatori delle infrastrutture critiche informatizzate, la segnalazione di tutti gli incidenti aventi un impatto significativo nel campo della sicurezza delle reti e dell'informazione. Ritiene infatti che il principio di una comunicazione degli incidenti su base volontaria rimarrebbe lettera morta, dato che gli operatori sono indotti a passare sotto silenzio le eventuali disfunzioni per non intaccare il loro buon nome e per timore di doversi assumere delle responsabilità.

4.6 Tuttavia, l'articolo 14 della direttiva, relativo alla notifica degli incidenti, non stabilisce con precisione che cosa si intenda per incidente «avente un impatto significativo» sulla sicurezza e concede agli enti interessati e agli Stati membri un eccessivo margine di discrezione per quanto concerne la notifica o meno degli incidenti per la sicurezza delle reti e dell'informazione. Per essere efficace, una norma deve poggiare su requisiti non ambigui. Dato che la proposta di direttiva è eccessivamente vaga sulla definizione fondamentale dei requisiti, non è possibile ritenere le parti responsabili di una loro mancata osservanza, come prevede l'articolo 17 del testo.

4.7 Dato che i servizi di sicurezza delle reti e dell'informazione vengono forniti principalmente da società private, è importante promuovere elevati livelli di fiducia e cooperazione tra tutte le aziende responsabili delle infrastrutture critiche. Il partenariato europeo pubblico-privato per la resilienza (EP3R), lanciato dalla Commissione nel 2009, è un'iniziativa apprezzabile che va incoraggiata. Il CESE ritiene però che essa vada potenziata e sostenuta da un obbligo regolamentare nell'atto legislativo sulla sicurezza delle reti e dell'informazione inteso a rendere vincolante la cooperazione tra i principali soggetti interessati che non si impegnino in modo adeguato.

4.8 Gli Stati membri dovrebbero pubblicare un repertorio, consultabile online, di tutti gli enti presenti nella loro giurisdizione che sono tenuti a soddisfare i requisiti di sicurezza e gli obblighi in materia di notifica degli incidenti stabiliti dall'art. 14 della direttiva. Una tale prova di trasparenza, oltre a chiarire in che modo ciascuno Stato membro decide di applicare le definizioni di cui all'articolo 3 del testo all'esame, contribuirebbe a rafforzare la fiducia dei cittadini e a promuovere tra di essi una cultura di gestione dei rischi.

4.9 Il CESE osserva che gli elaboratori di software e i fabbricanti di hardware sono espressamente esclusi dall'ambito di applicazione della direttiva in quanto non sono fornitori di servizi per la società dell'informazione. Il Comitato tuttavia ritiene che nel testo proposto occorra specificare che gli enti tenuti a soddisfare gli obblighi previsti dalla direttiva potranno presentare ricorso contro i fornitori di software e hardware per qualsiasi difetto nei loro prodotti o servizi in grado di contribuire direttamente a creare incidenti nel campo della sicurezza delle reti e dell'informazione.

4.10 Anche se la Commissione ritiene che l'attuazione della proposta di direttiva sulla sicurezza delle reti e dell'informazione costerà circa 2 miliardi di euro l'anno da dividere fra il settore pubblico e quello privato in Europa, il Comitato fa osservare che gli Stati membri attualmente in difficoltà finanziarie dovranno lottare per trovare i fondi necessari al rispetto delle norme previste. Occorre pertanto esaminare la possibilità di fornire un sostegno per l'osservanza delle disposizioni in materia di sicurezza delle reti e dell'informazione nell'ambito del quadro finanziario pluriennale a titolo di diversi strumenti, tra cui il Fondo europeo di sviluppo regionale (FESR) ed eventualmente il Fondo Sicurezza interna.

Bruxelles, 22 maggio 2013

Il presidente
del Comitato economico e sociale europeo
Henri MALOSSE