CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 22 novembre 2013 (03.12)
(OR. en)

16630/13

Fascicolo interistituzionale: 2013/0027 (COD)

TELECOM 322
DATAPROTECT 178
CYBER 33
MI 1064
CODEC 2676

NOTA

della:	presidenza
alle:	delegazioni
n. prop. Comm.:	6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313 + ADD1 +ADD2
n. doc. prec.:	16333/13 TELECOM 313 DATAPROTECT 170 CYBER 30 MI 1039 CODEC 2717
Oggetto:	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 - *Relazione sullo stato di avanzamento dei lavori*

La presente relazione è stata elaborata sotto la responsabilità della presidenza lituana. Descrive i lavori finora svolti dagli organi preparatori del Consiglio e riporta l'andamento dei lavori in occasione dell'esame della suddetta proposta.

ASPETTI PROCEDURALI

1. In data 12 febbraio la Commissione ha presentato una 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* (in seguito: direttiva SRI), avente come base giuridica l'articolo 114 del TFUE[1]. La proposta rientra nella strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro[2], riguardo a cui il Consiglio ha adottato conclusioni il 25 giugno 2013[3]. Il Consiglio TTE del 6 giugno 2013 ha preso atto dei progressi compiuti nell'esame della proposta di direttiva SRI[4].

2. Il Comitato economico e sociale europeo[5] e il Comitato delle regioni[6] hanno adottato pareri in merito alla proposta rispettivamente il 22 maggio e il 3-4 luglio. Al Parlamento europeo, la commissione competente per questo fascicolo è la commissione per il mercato interno (IMCO), assieme alla commissione per l'industria (ITRE) e alla commissione per le libertà civili (LIBE) come commissioni associate. Riguardo alla tempistica, la commissione LIBE prevede di procedere alla votazione a novembre, la commissione ITRE a dicembre e la commissione IMCO ha in programma l'adozione di una relazione ed una serie di emendamenti per il 22 e 23 gennaio 2014.

3. Durante la presidenza lituana, il Gruppo "Telecomunicazioni e società dell'informazione" ha esaminato la proposta in cinque riunioni[7]. Poiché numerose delegazioni hanno potuto esprimere soltanto opinioni preliminari ed hanno mantenuto riserve di esame sul testo (o su parti di esso), la presidenza lituana non ha potuto allegare un testo riveduto alla presente relazione sullo stato di avanzamento dei lavori. Tuttavia, durante le discussioni, le delegazioni hanno sollevato varie questioni e preoccupazioni di fondo, come riferito nel prosieguo, che dovranno essere rispecchiate in una revisione del testo della proposta.

---

1 Doc. 6342/13
2 Doc. 6225/13
3 Doc. 11357/13
4 Docc. 10076/13 e 10457/13
5 TEN/513
6 2013/C 280/05.
7 Il 18/7, 26/9, 8/10, 5/11 e 19/11/2013.

ASPETTI DI MERITO

4. La relazione sullo stato di avanzamento dei lavori destinata al Consiglio TTE di giugno[8] contiene una descrizione generale dei principali elementi della proposta di direttiva SRI. Sebbene tutte le delegazioni riconoscano del tutto la necessità di un'azione volta ad affrontare gli incidenti a carico della SRI e a frenare gli attacchi informatici, le opinioni divergono riguardo a come meglio garantire la sicurezza della rete in tutta l'UE. Mentre alcune delegazioni confermano nell'esame articolo per articolo della proposta che preferirebbero un approccio flessibile, con norme vincolanti in tutta l'UE limitatamente a infrastrutture critiche e a requisiti di base, integrate da misure facoltative e volontarie, altre delegazioni come pure la Commissione ritengono che soltanto misure giuridicamente vincolanti possano arrecare i necessari livelli di sicurezza UE. Questa differenza di principi spiega le differenze tra le posizioni adottate sulle disposizioni specifiche contenute nella proposta, come chiarito più avanti.

5. *Strategia SRI e organismo competente per la SRI*: considerato l'obiettivo di avere a disposizione un livello minimo di capacità necessarie a prevenire, gestire e rispondere ai rischi e agli incidenti a cui sono esposti i sistemi informatici, gli Stati membri dell'UE sarebbero tenuti ad adottare strategie nazionali in materia di SRI, a designare autorità nazionali competenti in tale materia e a costituire le Computer Emergency Response Team (CERT) per la SRI.

   Le delegazioni riconoscono che gravi perturbazioni in uno Stato membro possono ripercuotersi sugli altri Stati membri e potrebbero sostenere il principio di un organismo di coordinamento a livello nazionale. Tuttavia, specialmente gli Stati membri che già hanno adottato strategie SRI, hanno designato organismi competenti ed hanno costituito una CERT nazionale, sembrano considerare con occhio critico il capo II della proposta che riguarda i *quadri nazionali per la sicurezza delle reti e dell'informazione*: essi intendono garantire che i requisiti che gli Stati membri dovranno soddisfare siano coerenti con le attuali pratiche nazionali e restino entro i limiti di queste ultime. Talune delegazioni ritengono che l'organismo competente dovrebbe essere un punto di contatto e delegare i compiti alle autorità di regolamentazione nazionali dotate delle competenze di settore necessarie. Ciò dovrebbe garantire inoltre che i requisiti stabiliti siano conformi alle disposizioni nazionali in materia di sicurezza. Talune delegazioni mettono in risalto che occorre incrementare le misure di rafforzamento della fiducia per un maggiore affidamento, piuttosto che porre l'accento su disposizioni amministrative e burocratiche.

[8] Doc. 10076/13.

Altre delegazioni desiderano ottenere ulteriori chiarimenti circa la terminologia utilizzata nel suddetto capo, come "rischi" e "minacce" e si chiedono quali siano i requisiti esatti, domandando altresì se tali requisiti debbano riguardare soltanto il settore privato o anche quello pubblico. Per quanto riguarda l'autorità competente e la descrizione del suo compito, vi sono molte questioni che richiedono ulteriori chiarimenti, come quella se l'autorità debba assumere compiti operativi, trovando l'opposizione di molti Stati membri, e quale dovrebbe essere la ripartizione delle responsabilità con la CERT nazionale.

6. *Gestione del rischio e notifica degli incidenti*: "gli operatori del mercato" e le amministrazioni pubbliche dovrebbero valutare adeguatamente i rischi posti ai loro sistemi informativi, adottare misure idonee a prevenire e gestire gli incidenti e segnalare alle autorità competenti ogni incidente grave che abbia significative ripercussioni sui principali servizi prestati alle autorità competenti.

   Riguardo al capo IV della proposta, che tratta la *sicurezza delle reti e dei sistemi informativi delle pubbliche amministrazioni e degli operatori del mercato*, numerose delegazioni sono in dubbio se, oltre agli "operatori di infrastrutture critiche", debbano essere contemplati dalla proposta anche i "fornitori di servizi della società dell'informazione". Tale preoccupazione relativa al campo d'applicazione è strettamente legata alla definizione di "operatori del mercato" di cui al capo I e all'elenco non esaustivo di cui all'allegato II. Molte delegazioni hanno chiesto maggiore chiarezza sulla definizione e maggiore flessibilità per gli Stati membri nel definire quali settori costituiscano infrastrutture critiche nazionali. Alcune delegazioni vorrebbero circoscrivere i requisiti proposti al solo settore privato e altre chiedono che gli obblighi di comunicazione connessi alle violazioni di sicurezza stabiliti nel suddetto capo siano su base volontaria, in linea con le attuali pratiche nazionali. Si pone anche la questione del motivo per il quale non sono contemplati i produttori di hardware/software e le microimprese, e gli Stati membri nutrono preoccupazioni circa la coerenza degli obblighi di comunicazione connessi alle violazioni di sicurezza con quelli previsti in altri atti legislativi dell'UE, come nel quadro normativo per le comunicazioni elettroniche, per il cui effetto i fornitori di reti o servizi di comunicazione elettronica o i prestatori di servizi fiduciari non sono soggetti ai requisiti dell'attuale proposta. In generale, molte delegazioni chiedono se o come gli Stati membri potranno effettivamente "garantire" che gli attori mettano in sicurezza le loro reti e segnalino gli incidenti; in tal senso, è emersa tra le questioni da chiarire l'adeguatezza dell'articolo 114 del TFUE come base giuridica. Si registrano altresì preoccupazioni in relazione alle implicazioni delle segnalazioni riguardo a questioni attinenti alla vita privata e alla riservatezza delle informazioni.

7. *Rete di collaborazione*: per garantire una risposta coordinata agli incidenti, se necessario, è opportuno creare una rete di collaborazione sugli incidenti e i rischi a carico della SRI per permettere una comunicazione permanente tra la Commissione e le 28 autorità competenti.

   Il capo III della proposta, che verte sulla *cooperazione fra autorità competenti*, richiederà un esame più approfondito. Occorrerà discutere ulteriormente i compiti della rete di collaborazione, anche se molte delegazioni ritengono che essa non debba assumere alcun compito operativo; a tal riguardo, alcune obiettano che sarebbe meglio riferirsi ad un *meccanismo* anziché ad una *rete*. Anche varie questioni organizzative necessitano di essere ulteriormente chiarite, come chi presiederà la rete di collaborazione, quali costi essa comporterebbe e come sarebbero il rapporto e la ripartizione di responsabilità con la collaborazione delle CERT nazionali, con ENISA e con Europol. Talune delegazioni obiettano che lo scambio di informazioni nella rete dovrebbe essere fatto su base volontaria e mettono in discussione la necessità del "sistema sicuro di scambio di informazioni" proposto e dedicato. Il meccanismo di preallarme proposto solleva interrogativi e preoccupazioni in gran numero, ad esempio quali informazioni saranno scambiate in quale determinato momento e con quali possibili conseguenze per l'incidente o il rischio. Inoltre, parecchi Stati membri mettono in dubbio il campo di applicazione del meccanismo di risposta coordinata proposto e richiedono un quadro di cooperazione sulla SRI piuttosto che un piano operativo di risposta agli incidenti. Occorre discutere ulteriormente quando e a quali condizioni sia richiesta una risposta coordinata.

8. Riguardo ai due capi I e V della proposta, cioè le *Disposizioni generali* (che sono state esaminate durante la presidenza irlandese) e le *Disposizioni finali* rispettivamente, si è proceduto ad un primo scambio di pareri, però occorrerà ritornare su talune disposizioni per un ulteriore esame, come le seguenti: applicazione degli obblighi di sicurezza proposti in rapporto a quelli contenuti nella direttiva quadro (2002/21/CE); definizioni di "rischio", "incidente" e “operatore del mercato” (in relazione con *l'Elenco degli operatori del mercato* contenuto nell'allegato II); applicazione (ad esempio, la segnalazione di incidenti alla polizia); normalizzazione; atti di esecuzione (tutte le delegazioni si sono opposte al ricorso ad atti delegati in questo settore di attività) e periodo di recepimento (per il recepimento nella legislazione nazionale nonché per la pubblicazione della strategia nazionale in materia di SRI).

PROSPETTIVE

9. L'esame articolo per articolo della proposta dimostra che le delegazioni stanno cercando di ottenere dalla Commissione chiarezza, ma anche giustificazione, riguardo alle misure proposte a confronto delle attuali situazioni nazionali e dei meccanismi (nazionali ed internazionali) di segnalazione volontaria di incidenti e di cooperazione, come quelli esistenti nell'ambito delle comunità CERT europee e internazionali (ad es. gruppo di CERT nazionali europee) e che potrebbero includere il ruolo di facilitazione di ENISA. Nell'ulteriore esame della proposta in seno al Gruppo "Telecomunicazioni e società dell'informazione", pare che la sfida principale sarà concordare un approccio che crei il corretto equilibrio tra norme vincolanti in tutta l'UE e misure facoltative, volontarie, che conducano tutte quante a livelli simili di preparazione in ambito SIR tra gli Stati membri e consentano all'UE di rispondere efficacemente alle sfide in tale ambito.

10. Saranno ben gradite ulteriori proposte redazionali che le delegazioni vorranno fornire alla presidenza e che saranno prese in debita considerazione nell'ulteriore esame della proposta.

*

* *

Previo esame in sede di COREPER il 27 novembre, la presidenza presenterà al Consiglio la presente relazione sull'andamento dei lavori invitandolo a prenderne atto.