Consiglio dell'Unione europea

Bruxelles, 17 maggio 2016
(OR. en)

5581/1/16
REV 1 ADD 1

Fascicolo interistituzionale: 2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

MOTIVAZIONE DEL CONSIGLIO

Oggetto:	Posizione del Consiglio in prima lettura in vista dell'adozione della DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione – Motivazione del Consiglio – Adottata dal Consiglio in data 17 maggio 2016

I. INTRODUZIONE

1. Il 12 febbraio 2013 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 denominata "la direttiva"), avente come base giuridica l'articolo 114 del TFUE.

2. Il Comitato economico e sociale europeo ha votato il suo parere il 22 maggio 2013, mentre il Comitato delle regioni ha votato il suo il 3 e il 4 luglio 2013.

3. Il Parlamento europeo ha votato la sua risoluzione legislativa in prima lettura il 13 marzo 2014[1], adottando 138 emendamenti.

4. Il Consiglio e il Parlamento europeo hanno avviato i negoziati al fine di raggiungere un accordo rapido in seconda lettura nell'ottobre 2014. I negoziati si sono conclusi positivamente il 7 dicembre 2015 con il raggiungimento, da parte del Parlamento europeo e del Consiglio, di un accordo provvisorio su un testo di compromesso.

5. Il 18 dicembre 2015 il Comitato dei rappresentanti permanenti ha confermato il testo di compromesso della direttiva concordato dalle due istituzioni.

6. Il 28 gennaio 2016 il presidente della commissione IMCO del Parlamento europeo ha trasmesso una lettera al presidente del Comitato dei rappresentanti permanenti in cui dichiarava che, qualora il Consiglio avesse trasmesso formalmente al Parlamento europeo la propria posizione quale concordata, previa messa a punto dei giuristi-linguisti, avrebbe raccomandato alla plenaria di accettare la posizione del Consiglio senza emendamenti nella seconda lettura del Parlamento.

7. Il 29 febbraio 2016 il Consiglio ha confermato il proprio accordo politico sul testo di compromesso della direttiva.

---

[1] Risoluzione legislativa del Parlamento europeo del 13 marzo 2014 sulla 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 (SRI) nell'Unione.

II. OBIETTIVO

8. Dal risultato dei negoziati emerge che la direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea così da migliorare il funzionamento del mercato interno.

III. ANALISI DELLA POSIZIONE DEL CONSIGLIO IN PRIMA LETTURA

A. Aspetti generali

9. A seguito del voto della plenaria, il Parlamento europeo e il Consiglio hanno condotto negoziati allo scopo di concludere un accordo in seconda lettura sulla base di una posizione in prima lettura del Consiglio che il Parlamento possa approvare senza modifiche. Il testo della posizione in prima lettura del Consiglio rispecchia pienamente il compromesso raggiunto dai colegislatori.

B. Questioni fondamentali

10. I principali elementi del compromesso raggiunto con il Parlamento europeo sono di seguito illustrati:

a. *Capacità nazionali*

11. In base al compromesso gli Stati membri hanno taluni obblighi in relazione alle proprie capacità nazionali in materia di cibersicurezza. In primo luogo gli Stati membri sono tenuti ad adottare una strategia nazionale che definisca gli obiettivi strategici e le opportune misure strategiche e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi.

12. In secondo luogo gli Stati membri designano una o più autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi affinché controllino l'applicazione della direttiva a livello nazionale.

13. In terzo luogo gli Stati membri sono altresì tenuti a designare un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi che svolgerà una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri e con il gruppo di cooperazione e la rete di CSIRT. Il punto di contatto unico trasmetterà inoltre una relazione annuale al gruppo di cooperazione in merito alle notifiche ricevute.

14. Infine gli Stati membri designano uno o più gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") che abbiano il compito di trattare gli incidenti e i rischi. Il testo di compromesso stabilisce, nell'allegato I, i requisiti e i compiti dei CSIRT.

b. *Cooperazione*

15. Al fine di sostenere e agevolare la cooperazione strategica fra Stati membri, di sviluppare la fiducia e nell'ottica di conseguire un livello comune elevato di sicurezza delle reti e dei servizi informativi nell'Unione, il testo di compromesso istituisce un gruppo di cooperazione. Il gruppo sarà composto da rappresentanti degli Stati membri, della Commissione e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e avrà i compiti specifici elencati nel testo, quali lo scambio di migliori pratiche e informazioni relative a una serie di questioni o la discussione delle capacità e dello stato di preparazione degli Stati membri.

16. Inoltre, il compromesso istituisce una rete di CSIRT nazionali al fine di contribuire allo sviluppo della fiducia fra gli Stati membri e di promuovere una cooperazione operativa rapida ed efficace. La rete sarà composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE e la Commissione parteciperà alla rete in qualità di osservatore. L'ENISA assicurerà il segretariato e sosterrà attivamente la cooperazione fra i CSIRT. Il testo prevede un elenco di compiti che dovranno essere svolti dalla rete, quali lo scambio di informazioni su servizi, operazioni e capacità di cooperazione dei CSIRT, il sostegno agli Stati membri nel far fronte a incidenti transfrontalieri o, in determinate circostanze, lo scambio e la discussione di informazioni connesse a incidenti e rischi associati.

c. *Obblighi in materia di sicurezza e notifica*

17. La direttiva stabilisce taluni obblighi per due categorie di operatori di mercato: gli operatori di servizi essenziali e i fornitori di servizi digitali.

18. L'allegato II della direttiva elenca una serie di settori importanti per la società e l'economia, segnatamente l'energia, i trasporti, il settore bancario, le infrastrutture dei mercati finanziari, il settore sanitario, la fornitura e distribuzione di acqua potabile e le infrastrutture digitali. In tali settori gli Stati membri identificheranno gli operatori di servizi essenziali, sulla base di criteri precisi stabiliti nella direttiva.

19. L'allegato III della direttiva elenca tre tipi di servizi digitali, i cui fornitori dovranno rispettare gli obblighi della direttiva: i mercati online, i motori di ricerca online e i servizi nella nuvola (cloud computing). Tutti i fornitori di servizi digitali che prestano i servizi elencati dovranno rispettare gli obblighi della direttiva, a esclusione delle piccole e microimprese.

20. Le due categorie di operatori di mercato saranno tenute ad adottare misure organizzative e tecniche per gestire i rischi posti alla sicurezza delle reti e dei sistemi informativi e minimizzare l'impatto degli incidenti a carico della sicurezza di tali sistemi. Inoltre, gli incidenti aventi un certo livello di impatto sui servizi in questione dovranno essere notificati alle autorità nazionali competenti o ai CSIRT. La direttiva stabilisce criteri per determinare il livello dell´impatto di tali incidenti.

21. Essa adotta un approccio differenziato in relazione alle due categorie di operatori. Gli obblighi in materia di sicurezza e notifica sono meno rigidi per i fornitori di servizi digitali che per gli operatori di servizi essenziali, il che rispecchia il grado di rischio che perturbazioni a carico di tali servizi possono comportare per società ed economia. Inoltre, considerato che i fornitori di servizi digitali sono spesso attivi in molti Stati membri e al fine di assicurare un elevato livello di armonizzazione, la direttiva impedisce agli Stati membri di imporre ulteriori obblighi in materia di sicurezza e notifica a detti fornitori.

22. Il testo di compromesso stabilisce altresì che i soggetti che non sono stati identificati come operatori di servizi essenziali e non sono fornitori di servizi digitali possono notificare taluni incidenti su base volontaria.

d. *Recepimento*

23. Gli Stati membri dovranno recepire la direttiva entro 21 mesi dalla data di entrata in vigore e disporranno di ulteriori 6 mesi per identificare i propri operatori di servizi essenziali.

IV. CONCLUSIONE

24. La posizione del Consiglio rispecchia pienamente il compromesso raggiunto nei negoziati tra il Parlamento europeo e il Consiglio, con l'accordo della Commissione. Il compromesso è confermato dalla lettera inviata il 28 gennaio 2016 dal presidente della commissione IMCO al presidente del Comitato dei rappresentanti permanenti.