



**CONSIGLIO
DELL'UNIONE EUROPEA**

**Bruxelles, 16 maggio 2014 (23.05)
(OR. en)**

9757/14

**Fascicolo interistituzionale:
2013/0027 (COD)**

**TELECOM 111
DATAPROTECT 69
CYBER 27
MI 419
CSC 103
CODEC 1264**

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.: 7404/14 TELECOM 73 DATAPROTECT 39 CYBER 14 MI 242 CSC 49
CODEC 688

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
- Progetto di relazione sullo stato di avanzamento dei lavori

La presente relazione è stata elaborata sotto la responsabilità della presidenza greca. Descrive i lavori finora svolti dagli organi preparatori del Consiglio, riporta lo stato di avanzamento dei lavori in occasione dell'esame della suddetta proposta e delinea orientamenti in vista della preparazione dei negoziati con il Parlamento europeo al momento opportuno.

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 TFUE.¹ La proposta rientra nella strategia dell'Unione europea per la cibersecurity: un ciberspazio aperto e sicuro², riguardo al quale il Consiglio ha adottato conclusioni il 25 giugno 2013.³ I Consigli TTE del 6 giugno⁴ e del 5 dicembre⁵ hanno preso atto dei progressi compiuti nell'esame della proposta di direttiva SRI.
2. Il Comitato economico e sociale europeo⁶ e il Comitato delle regioni⁷ hanno adottato pareri in merito alla proposta rispettivamente il 22 maggio e il 3-4 luglio 2013. Il 13 marzo 2014 il Parlamento europeo ha adottato in prima lettura una risoluzione legislativa e una serie di emendamenti (138) elaborati dalla commissione per il mercato interno (IMCO), in qualità di commissione competente per questo fascicolo, assieme alla commissione per l'industria (ITRE) e alla commissione per le libertà civili (LIBE), in qualità di commissioni associate.⁸

¹ Doc. 6342/13.

² Doc. 6225/13.

³ Doc. 11357/13.

⁴ Docc. 10076/13 e 10457/13.

⁵ Docc. 16630/13 e 17341/13.

⁶ TEN/513.

⁷ 2013/C 280/05.

⁸ Doc. 7451/14.

3. Durante la presidenza greca, il Gruppo "Telecomunicazioni e società dell'informazione" ha continuato l'esame della proposta articolo per articolo durante 6 riunioni⁹. Sulla base delle discussioni nel Gruppo, per le quali la presidenza aveva preparato documenti di riflessione¹⁰, e delle osservazioni scritte presentate dalla maggioranza degli Stati membri, la presidenza greca ha elaborato la presente relazione sullo stato di avanzamento dei lavori che evidenzia le questioni di fondo relative alla proposta e, ove possibile, individua la strada che gli Stati membri hanno in linea di principio, concordato di percorrere. Parallelamente alla presente relazione e a fini illustrativi, la presidenza ha elaborato una prima versione modificata del testo della proposta¹¹ che è stata presentata al Gruppo il [xxx] e sulla base della quale i lavori potrebbero avanzare ulteriormente sotto presidenza italiana al fine di avviare contatti con il PE al momento opportuno.

ASPETTI DI MERITO

CAPO I: disposizioni generali (articoli da 1 a 3)

4. Le delegazioni concordano, in generale, sull'oggetto e sul campo di applicazione dell'articolo 1 ("Oggetto") proposti e ritengono che la proposta di direttiva costituisca un elemento essenziale della strategia generale dell'Unione europea per la cibersicurezza. La presidenza ritiene che la maggioranza degli Stati membri possa essere a favore di un parziale perfezionamento dell'articolo 1 sulla seguente falsariga:

- *nel paragrafo 1, il termine "garantire" dovrebbe essere sostituito con "raggiungere" per rispecchiare il fatto che gli Stati membri non possono, né singolarmente né come gruppo, "garantire" un livello di totale impermeabilità della SRI;*
- *piuttosto che creare un nuovo "meccanismo di collaborazione" tra gli Stati membri, le disposizioni di cui al paragrafo 2, lettera b), dovrebbero far riferimento agli accordi in essere per "riunire" gli Stati membri al fine di attuare la direttiva a livello politico/strategico. Si potrebbe esplorare una collaborazione operativa più concreta, ad esempio nel contesto delle squadre di pronto intervento informatico (CERT)¹²;*

⁹ Il 27/2, il 13 e il 28/3, il 10 e il 28/4, il 21/5/2014.

¹⁰ Doc. 7404/14.

¹¹ Doc. [XXX].

¹² CERT significa "squadra di pronto intervento informatico" (computer emergency response team). Poiché CERT è un marchio registrato dell'UE, è stata posta la questione se sia necessario utilizzare una terminologia diversa nella direttiva, ad esempio "gruppo di intervento per la sicurezza informatica in caso di incidente" (CSIRT - Computer Security Incident Response Team).

- *gli Stati membri coinvolti in un incidente e/o le squadre CERT dovrebbero decidere se e in quale misura le informazioni pertinenti (ed eventualmente i dati personali) dovrebbero essere condivise tenendo in considerazione, allo stesso tempo, gli interessi della sicurezza nazionale e della normativa pertinente, in particolare per quanto riguarda la protezione dei dati personali o gli attacchi contro i sistemi informativi;*
 - *è necessario un chiarimento dal punto di vista giuridico per determinare se la base giuridica del mercato interno utilizzata sia adeguata e consenta alla direttiva di ricomprendere le "amministrazioni pubbliche".*
5. Le delegazioni sostengono, in linea generale, l'articolo 2 ("Armonizzazione minima").
6. Con riguardo alle "definizioni" di cui all'articolo 3, pur osservando che debbano essere rivedute nel corso dello svolgimento dei lavori, la presidenza ritiene che le delegazioni sostengano, in linea generale, la seguente falsariga:
- *nell'elenco delle definizioni si dovrebbe introdurre una nuova definizione in materia di "servizi essenziali" poiché questo consentirebbe di individuare meglio quali attori forniscono detti servizi "essenziali" e di valutare il rischio o la "minaccia" relativi alla sicurezza di tali servizi;*
 - *la direttiva dovrebbe fare riferimento ad un elenco di settori comuni delle infrastrutture critiche e fornire criteri per determinare quali operatori compongono tali infrastrutture. Le opinioni degli Stati membri non si sono ancora pienamente concretizzate per quanto concerne il livello di dettaglio da includere nella direttiva (e nell'ALLEGATO II, in particolare), ad esempio se la direttiva debba o meno contemplare anche i "servizi della società dell'informazione" e i "facilitatori di internet";*
 - *si dovrebbe riflettere ulteriormente sulla necessità di inserire ulteriori definizioni quali i servizi informatici critici, il piano nazionale di gestione dei rischi, la strategia e il piano di collaborazione in materia di SRI.*

Capo II: quadri nazionali per la SRI (articoli da 4 a 7)

7. Le delegazioni sostengono, in generale, la soppressione dell'articolo 4 ("Principio").
8. Per quanto riguarda l'articolo 5 ("Strategia nazionale in materia di SRI"), la presidenza ha preso nota di un ampio sostegno a favore del seguente orientamento:
- *sebbene lo sviluppo di una strategia in materia di SRI, compreso un piano di collaborazione, trovi in linea di principio sostegno, il testo di tale articolo dovrebbe concentrarsi più sui principi generali "a prova di futuro" che sui requisiti concreti per la strategia e il piano di collaborazione in materia di SRI, in quanto tale approccio consentirebbe di contribuire nel modo migliore alla costruzione della fiducia.*

9. Per quanto riguarda l'articolo 6 ("Autorità competente") e tenendo a mente il principio di sussidiarietà, le delegazioni sembrano sostenere un approccio che tenga in debito conto le prassi in uso negli Stati membri:

- *la direttiva dovrebbe consentire agli Stati membri sufficiente flessibilità nella designazione o nella gestione di una o più autorità competenti settoriali e orientate alla politica;*
- *ogni Stato membro dovrebbe tuttavia designare un "punto di contatto unico".*

10. Per quanto riguarda l'articolo 7 ("CERT"), gli Stati membri sono generalmente favorevoli al requisito della direttiva di istituire o mantenere una o più squadre CERT, che potrebbero corrispondere all'"autorità competente" o al "punto di contatto unico", e concordano con gli orientamenti proposti in relazione alle squadre CERT figuranti nel doc. 7404/14, e in particolare:

- *gli Stati membri dovrebbero disporre di flessibilità sufficiente in termini di organizzazione tecnica e di risorse finanziarie e umane per le squadre CERT, e questo dovrebbe riflettersi nel testo del presente articolo e dell'ALLEGATO II, però la direttiva dovrebbe dar prova di fermezza circa il grado di ambizione da conseguire e i requisiti da stabilire per le squadre CERT e per la collaborazione tra quest'ultimi.*

Capo III: cooperazione (articoli da 8 a 13)

11. Il Capo III della proposta concerne l'architettura della collaborazione in materia di SRI.

Secondo la presidenza tutti gli Stati membri riconoscono che attraverso un qualche tipo di collaborazione si potrebbero raggiungere in tutta l'UE livelli simili ed elevati di preparazione in ambito SRI, il che faciliterebbe altresì una risposta comune e coordinata alle sfide della SRI se, e dove, se ne presenta l'esigenza. Tuttavia, le opinioni si devono ulteriormente concretizzare circa il modo in cui tale rete di collaborazione strategico/politica dovrebbe configurarsi e quale ruolo avrebbe, a patto che debba averlo, nel fornire risposte operative coordinate in caso di incidenti informatici nazionali, ed eventualmente, transfrontalieri.

12. Per quanto riguarda l'articolo 8 ("Rete di collaborazione"), la presidenza ritiene che le delegazioni sostengano, in linea generale, il seguente approccio:

- *la presente direttiva dovrebbe definire un approccio politico/strategico per quanto riguarda la rete di collaborazione che da un lato si fonda sulle capacità da sviluppare a norma del già citato capo II e, dall'altro, se del caso, fornisce una guida per l'elaborazione di modalità dettagliate per una collaborazione operativa, essendo quest'ultima già trattata altrove (ad es. ENISA, CERT);*
- *in caso di emergenza la risposta dovrebbe incentrarsi sulle capacità nazionali, come le squadre CERT e/o le autorità competenti e, laddove necessario, in casi (transfrontalieri) che devono essere meglio specificati, si potrebbe creare un'ulteriore collaborazione volontaria all'interno di una comunità di collaborazione operativa che comprende tutte le 28 squadre CERT nazionali con l'obiettivo di fornire una risposta coordinata dell'UE;*
- *la rete di collaborazione dovrebbe dar vita, su base volontaria, a verifiche inter pares delle capacità e della preparazione.*

13. Per quanto riguarda l'articolo 9 ("Sistema sicuro di scambio di informazioni"), la presidenza ha rilevato che la maggior parte degli Stati membri è contraria a fissare requisiti obbligatori nella direttiva per la condivisione di informazioni (sensibili dal punto di vista commerciale) all'interno della rete di collaborazione e contraria all'istituzione o al funzionamento di una infrastruttura sicura dedicata. Le delegazioni hanno anche espresso serie preoccupazioni per quanto riguarda la proposta in merito al ruolo che la Commissione svolgerebbe in tale contesto. Tenendo conto di quanto sopra esposto, la presidenza ritiene che si dovrebbe redigere nuovamente il presente articolo sulla seguente falsariga:

- *la direttiva non dovrebbe contenere requisiti obbligatori per la condivisione delle informazioni e il testo dell'articolo 9 dovrebbe conformarsi o, in alternativa, si potrebbe sopprimere l'articolo visto che all'interno della rete di collaborazione si possono scambiare informazioni non sensibili e non classificate o che le squadre CERT possono scambiare informazioni pertinenti.*

14. Per quanto riguarda l'articolo 10 ("Preallarmi"), le delegazioni appaiono in grado di sostenere gli orientamenti generali figuranti nel doc. 7404/14, e in particolare:

- *la trasmissione di preallarmi dovrebbe restare volontaria e lo scambio di informazioni pertinenti all'interno della rete di collaborazione dovrebbe in primo luogo contribuire a costruire la fiducia tra il settore privato e le autorità nazionali competenti nonché tra le stesse autorità nazionali competenti;*
- *dato che lo scambio di informazioni sui reati in materia di attacchi contro i sistemi di informazione è contemplato dalla direttiva 2013/40, non occorre che la direttiva affronti tale aspetto (ovverosia soppressione del paragrafo 4);*
- *gli Stati membri dovrebbero decidere se e quali informazioni fornire alla rete di coordinamento (ovverosia soppressione del paragrafo 5);*
- *i preallarmi non dovrebbero ostacolare o ritardare le azioni nazionali per far fronte alle minacce e agli incidenti.*

15. Anche per quanto riguarda l'articolo 11 ("Risposta coordinata"), la presidenza ha registrato un ampio sostegno agli orientamenti illustrati nel doc. 7404/14, e in particolare:

- *piuttosto che creare una competenza europea de facto per coordinare una risposta dell'UE agli incidenti (nazionali), è necessaria un'ulteriore riflessione tesa a chiarire quando e in quali casi sarebbe necessaria una "risposta coordinata dell'UE": in caso di gravi crisi informatiche transfrontaliere o anche in caso di incidenti quotidiani più circoscritti?*
- *Tenendo presente la competenza nazionale sulle questioni inerenti alla sicurezza la direttiva dovrebbe, al fine di conseguire un coordinamento politico a livello dell'UE in caso di crisi informatiche su larga scala, basarsi sugli accordi in essere anziché creare meccanismi nuovi e potenzialmente lenti;*
- *oltre a un coordinamento politico a livello dell'UE, la direttiva dovrebbe favorire la collaborazione tecnico/pratica (ad esempio tra le squadre CERT), all'interno della quale si potrebbero sviluppare ulteriori requisiti per una risposta operativa alla crisi.*

16. La presidenza rileva che, sebbene la posizione finale degli Stati membri sull'articolo 12 ("Piano unionale in materia di SRI") dipenda dall'esito degli articoli da 8 a 11, la maggior parte delle delegazioni potrebbe sostenere una modifica del testo della proposta che segua l'approccio seguente:

- *la direttiva potrebbe definire un "quadro" di collaborazione unionale in materia di SRI piuttosto che un "piano", che si incentra sul coordinamento e lo sviluppo delle politiche, che utilizza appieno le competenze pertinenti dell'ENISA e che venga periodicamente riesaminato dalla rete di collaborazione istituita a norma dell'articolo 8;*
- *il "quadro" di collaborazione dovrebbe comprendere temi quali le modalità di comunicazione da una squadra CERT all'altra, lo scambio di migliori pratiche, la sensibilizzazione, le esercitazioni e le formazioni, e trarre vantaggio dalle competenze dell'ENISA al riguardo.*

17. Per quanto riguarda l'articolo 13 ("Cooperazione internazionale"), la presidenza prende atto che gli Stati membri desiderano che il testo rispecchi la circostanza che tutti i membri partecipanti al quadro di collaborazione dovrebbero accettare la partecipazione al medesimo di paesi terzi o di organizzazioni internazionali.

Capo IV: sicurezza delle reti (articoli da 14 a 16), Capo V: disposizioni finali (articoli da 17 a 23) e Allegati I e II: CERT e operatori del mercato

18. Per quanto riguarda l'articolo 14 ("obblighi in materia di sicurezza e notifica degli incidenti"), la presidenza ha rilevato che gli Stati membri, nei quali la prassi nazionale di notifica volontaria ha raggiunto una collaborazione soddisfacente tra le parti interessate e le autorità pubbliche, preferirebbero che la direttiva si basasse su tale esperienza. Altri Stati membri chiedono se non si dovrebbero introdurre anche requisiti per la segnalazione obbligatoria. Tutti gli Stati membri concordano sulla necessità di un ulteriore chiarimento per quanto riguarda i vari obblighi di notifica presenti in diversi atti legislativi dell'UE. Alla luce di quanto sopra, la presidenza raccomanda il seguente approccio:

- *la direttiva proposta potrebbe definire requisiti per la segnalazione obbligatoria in caso di incidenti che, coinvolgendo diversi Stati membri, provocano un impatto transfrontaliero significativo;*
- *in caso di incidenti interni con un impatto circoscritto, gli Stati membri dovrebbero godere di flessibilità per decidere, conformemente all'articolo 2, se e come segnalare a livello nazionale;*

- *la direttiva dovrebbe definire i parametri per determinare l'impatto degli incidenti (settoriali) ma spetterebbe agli Stati membri decidere, sulla base di tali parametri, se un determinato incidente debba o meno essere segnalato;*
- *gli Stati membri dovrebbero godere di flessibilità in merito alle modalità di segnalazione alle autorità settoriali competenti le quali, a loro volta, possono segnalare al "punto di contatto unico" nazionale.*

19. Per quanto riguarda l'articolo 15 ("Attuazione e controllo"), e sulla base delle opinioni delle delegazioni, la presidenza suggerisce che:

- *la direttiva dovrebbe offrire sufficiente spazio alle soluzioni nazionali allo scopo di coinvolgere il settore privato più di quanto attualmente proposto, ad esempio per quanto riguarda gli audit di sicurezza, lo sviluppo di capacità tecniche, i corsi di formazione, ecc.;*
- *la direttiva dovrebbe anche prevedere la possibilità di consentire, se del caso, l'esistenza di più autorità settoriali competenti, che hanno anche responsabilità in merito all'attuazione e al controllo.*

20. Per quanto riguarda la questione della "normazione" ai sensi dell'articolo 16, la presidenza conclude che le delegazioni non ravvisano la necessità immediata di una riformulazione dell'articolo.

21. Per quanto riguarda l'articolo 17 ("Sanzioni"), in particolare il paragrafo 2, è necessaria un'ulteriore riflessione al fine di chiarire meglio il rapporto tra la direttiva SRI e il prossimo regolamento sulla protezione dei dati.

22. Infine, la presidenza ha rilevato che le delegazioni desiderano ritornare, in futuro, sul "periodo di attuazione" e sull'"entrata in vigore" (articoli 21 e 22) e che la messa a punto dell'ALLEGATO I per quanto riguarda l'ampiezza dei compiti e dei requisiti delle squadre CERT e dell'ALLEGATO II per quanto riguarda i settori e i soggetti che devono essere coperti da un elenco "esaustivo" o "indicativo" dovrà essere riveduta successivamente, sulla base di negoziati sulla sostanza degli articoli della proposta.

CONCLUSIONE

23. La presidenza greca ha osservato che gli Stati membri sono tutti, senza eccezioni, ben consapevoli dell'urgente necessità di migliorare la sicurezza delle reti e dell'informazione e di intervenire, al riguardo, a livello dell'UE. In tale contesto, gli Stati membri hanno dedicato all'esame della proposta della Commissione la massima attenzione e negli ultimi mesi sono stati compiuti notevoli progressi nell'individuare la direzione verso cui, come sopra indicato, la proposta dovrebbe ulteriormente svilupparsi.
24. Per quanto concerne le disposizioni relative ai capi I, II e IV e sulla base delle discussioni svoltesi in seno agli organi preparatori del Consiglio, la presidenza ritiene che gli orientamenti e le conclusioni proposti nella presente relazione sullo stato di avanzamento dei lavori debbano costituire una base sufficiente per sviluppare ulteriormente la proposta sotto la prossima presidenza italiana. Tali orientamenti e conclusioni sono stati riuniti tenendo presente la necessità di trovare il giusto equilibrio tra il miglioramento della sicurezza informatica, il rafforzamento della necessaria fiducia e il pieno uso, per ragioni di efficienza, delle esperienze attuali evitando altresì la duplicazione delle competenze degli organismi e dei meccanismi esistenti.
25. Per quanto concerne il capo III, gli Stati membri convengono, come osservato in precedenza (punto 11), sulla necessità di rafforzare la collaborazione strategico/politica sulla SRI a livello dell'UE. Vari Stati membri ritengono che la direttiva debba prevedere criteri e requisiti più specifici in materia di collaborazione operativa in caso di incidenti a carico della SRI. La maggior parte degli Stati membri, tuttavia, considera la collaborazione politico/strategica prioritaria per il rafforzamento della necessaria fiducia mentre le modalità per una collaborazione operativa potrebbero essere, al contempo, ulteriormente elaborate nell'ambito dei meccanismi e degli organismi esistenti. Come sopra proposto (punti da 11 a 17), la presidenza non crede che la collaborazione politico/strategica e la collaborazione operativa rappresentino opzioni che si escludono reciprocamente, ma ritiene che la direttiva debba avere come priorità la collaborazione politico/strategica fornendo, al contempo, una guida in tema di collaborazione operativa per gli organismi e i meccanismi esistenti.

*

* *

La presidenza trasmetterà al Consiglio la presente relazione sullo stato di avanzamento dei lavori, invitandolo a prenderne atto, previo esame in sede di COREPER il 28 maggio.