COMMISSIONE
EUROPEA

Bruxelles, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

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

{SWD(2013) 31 final}
{SWD(2013) 32 final}

RELAZIONE

Lo scopo della direttiva proposta è assicurare un elevato livello comune di sicurezza delle reti e dell'informazione (SRI) nell'Unione. Questo presuppone il miglioramento della sicurezza di internet e delle reti e dei sistemi informativi privati su cui si fonda il funzionamento delle nostre società e delle nostre economie. A questo scopo si chiede agli Stati membri di aumentare il loro grado di preparazione e di migliorare la collaborazione reciproca, agli operatori di infrastrutture critiche, come l'energia, i trasporti e i principali fornitori di servizi della società dell'informazione (piattaforme di commercio elettronico, reti sociali ecc.) e alle pubbliche amministrazioni, di adottare misure adeguate per gestire i rischi di sicurezza e segnalare alle autorità competenti gli incidenti gravi.

La presente proposta è presentata insieme alla comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza in merito ad una strategia europea per la cibersicurezza. L'obiettivo della strategia è dare vita a un ambiente digitale sicuro e affidabile, promuovendo e proteggendo i diritti fondamentali e altri valori costitutivi dell'UE. La presente proposta costituisce la misura principale della strategia. Le altre misure previste dalla strategia in questo settore riguardano la sensibilizzazione, lo sviluppo di un mercato interno di prodotti e servizi attinenti alla cibersicurezza e la promozione di investimenti in R&S. Questi interventi saranno completati da altre misure destinate a rafforzare la lotta contro la criminalità informatica e a elaborare una politica internazionale dell'UE in materia di cibersicurezza.

1.1. Motivazione e obiettivi della proposta

La sicurezza delle reti e dell'informazione va assumendo un'importanza crescente nella nostra economia e nella nostra società. La SRI è una precondizione importante per creare un ambiente affidabile per lo scambio di servizi su scala mondiale. Tuttavia, i sistemi informativi possono essere vittima di incidenti di sicurezza, causati ad esempio da errori umani, eventi naturali, guasti tecnici o attacchi dolosi. Questi incidenti si stanno facendo sempre più numerosi, frequenti e complessi. Dalla consultazione pubblica online sul tema "Migliorare la sicurezza delle reti e dell'informazione nell'UE"[1] è emerso che il 57% dei rispondenti negli anni scorsi ha avuto esperienza di incidenti a carico della SRI, con gravi ripercussioni sulle loro attività. La mancanza di sicurezza delle reti e dell'informazione può compromettere servizi essenziali che dipendono dall'integrità della rete e dei sistemi informativi. Questo a sua volta può bloccare il funzionamento di imprese, provocare ingenti perdite finanziarie per l'economia dell'UE e avere ripercussioni negative sul benessere della società.

Inoltre i sistemi informativi digitali, che costituiscono uno strumento di comunicazione senza confini, come in particolare internet, sono interconnessi in tutti gli Stati membri e svolgono un ruolo essenziale nel facilitare i movimenti transfrontalieri di beni, servizi e persone. Gravi perturbazioni a carico di questi sistemi in uno Stato membro possono avere ripercussioni negli altri Stati membri e in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi sono quindi essenziali per il completamento del mercato unico digitale e per l'armonioso funzionamento del mercato interno. La probabilità e la frequenza degli incidenti e l'incapacità di garantire una protezione sufficiente compromettono inoltre la fiducia del pubblico nelle reti e nei servizi di informazione. Ad esempio, l'indagine di Eurobarometro del 2012 sulla cibersicurezza evidenzia che per il 38% degli internauti dell'UE la sicurezza dei pagamenti online è fonte di preoccupazione tale da spingerli a cambiare condotta: il 18% è meno

[1] La consultazione pubblica online sul tema "Migliorare la sicurezza delle reti dell'informazione nell'UE" si è svolta dal 23 luglio al 15 ottobre 2012.

propenso ad acquistare merci online e il 15% è meno propenso a usare i servizi bancari online[2].

La situazione attuale nell'UE, frutto dell'approccio puramente facoltativo seguito finora, non offre una protezione sufficiente contro i rischi e gli incidenti a carico della sicurezza delle reti e dell'informazione nell'UE. I dispositivi e le capacità esistenti in questo campo sono semplicemente insufficienti per far fronte alla rapida evoluzione delle possibili minacce alla sicurezza e per assicurare un livello elevato comune di protezione in tutti gli Stati membri.

Nonostante le iniziative avviate, il livello di capacità e di preparazione degli Stati membri è molto variabile: ne consegue una forte frammentazione degli approcci a livello dell'UE. Data l'interconnessione tra le reti e i sistemi, la SRI generale dell'UE è indebolita dagli Stati membri con un livello insufficiente di protezione. Questa situazione ostacola anche la creazione di quel clima di fiducia tra pari indispensabile per la collaborazione e lo scambio di informazioni. Ne consegue che la cooperazione funziona solo tra una minoranza di Stati membri che hanno un livello elevato di capacità.

Attualmente non esiste pertanto un dispositivo effettivo, a livello UE, che permetta un'effettiva cooperazione e lo scambio sicuro di informazioni tra gli Stati membri sugli incidenti e i rischi a carico della SRI. Le possibili conseguenze sono interventi regolamentari non coordinati tra loro, strategie incoerenti e norme divergenti, da cui una protezione insufficiente della sicurezza delle reti e dell'informazione nell'UE. Possono sorgere anche ostacoli per il mercato interno che causano costi di messa in conformità alle imprese che operano in più Stati membri.

Infine, gli operatori che gestiscono infrastrutture critiche o forniscono servizi essenziali per il funzionamento della nostra società non sono soggetti ad obblighi appropriati quanto all'adozione di misure di gestione del rischio e allo scambio di informazioni con le autorità competenti. Pertanto, se da un lato le imprese non godono di incentivi efficaci alla conduzione di una gestione seria del rischio, che implica la valutazione del rischio e l'adozione di misure adeguate per garantire la sicurezza delle reti e dell'informazione, dall'altro una larga parte di incidenti non è segnalata alle autorità competenti e passa inosservata. Le informazioni sugli incidenti sono invece essenziali per permettere alle autorità pubbliche di reagire, adottare provvedimenti di mitigazione adeguati e fissare le opportune priorità strategiche per la SRI.

L'attuale quadro regolamentare fa obbligo soltanto alle compagnie di telecomunicazione di adottare misure di gestione del rischio di incidenti di sicurezza delle reti e dell'informazione e di segnalare questo tipo di incidenti. Ma esistono anche molti altri settori che dipendono dal supporto delle TIC, che dovrebbero quindi essere coinvolti in materia di SRI. Tutta una serie di specifiche infrastrutture e fornitori di servizi sono particolarmente vulnerabili perché dipendono fortemente dal corretto funzionamento delle reti e dei sistemi informativi. Questi settori svolgono un ruolo essenziale nel fornire servizi fondamentali di supporto per la nostra economia e la nostra società e la sicurezza dei loro sistemi riveste un'importanza particolare per il funzionamento del mercato interno: si pensi in particolare alle banche, alle borse, alla generazione, trasmissione e distribuzione di energia, ai trasporti (aerei, ferroviari e marittimi), alla sanità, ai servizi internet e alle amministrazioni pubbliche.

[2] Eurobarometro 390 (2012).

È quindi necessario accelerare il cambiamento nel modo di rapportarsi ai problemi di sicurezza delle reti e dell'informazione nell'Unione europea. Occorre instaurare obblighi regolamentari per creare parità di condizioni e ovviare alle lacune legislative esistenti. Per far fronte a questi problemi e rafforzare il livello di sicurezza nell'Unione la direttiva proposta persegue gli obiettivi sotto descritti.

Primo, la proposta chiede agli Stati membri di garantire la disponibilità di capacità minime a livello nazionale, attraverso la nomina di autorità competenti della sicurezza delle reti e dell'informazione (SRI), la creazione di squadre di pronto intervento informatico (CERT) e l'adozione di strategie e piani nazionali di collaborazione in materia di SRI.

Secondo, le competenti autorità nazionali sono chiamate collaborare in rete per garantire un coordinamento sicuro ed effettivo, che comprende lo scambio coordinato di informazioni e attività di individuazione e risposta a livello dell'UE. Gli Stati membri sono chiamati a scambiarsi informazioni attraverso tale rete e a collaborare per contrastare le minacce e gli incidenti a carico della sicurezza delle reti e dell'informazione in base ad un piano europeo di collaborazione in materia di SRI.

Terzo, rifacendosi al modello della direttiva quadro sulle comunicazioni elettroniche, la proposta mira a garantire lo sviluppo di una cultura della gestione dei rischi e dello scambio di informazioni tra i settori pubblico e privato. Alle imprese attive nei settori critici specifici sopra richiamati e alle pubbliche amministrazioni sarà chiesto di valutare i rischi che corrono e di adottare misure adeguate e proporzionate per garantire la sicurezza delle reti e dell'informazione. Questi soggetti dovranno segnalare alle autorità competenti gli incidenti suscettibili di compromettere gravemente le loro reti e sistemi informativi e aventi un impatto significativo sulla continuità di servizi critici e sulla fornitura di beni.

1.2. Contesto generale

Già nel 2001, nella sua comunicazione sulla sicurezza delle reti e dell'informazione (Proposta di un approccio strategico europeo), la Commissione sottolineava la crescente importanza della sicurezza delle reti e dell'informazione[3]. Tale comunicazione fu seguita nel 2006 dall'adozione di una strategia per una società dell'informazione sicura[4], destinata a sviluppare una cultura della sicurezza delle reti e dell'informazione in Europa, i cui elementi principali sono stati approvati da una risoluzione del Consiglio[5].

Il 30 marzo di 2009 la Commissione ha poi adottato una comunicazione relativa alla protezione delle infrastrutture critiche informatizzate[6] incentrata sulla protezione dell'Europa contro le ciberperturbazioni attraverso il rafforzamento della sicurezza. La comunicazione ha avviato un piano di azione destinato a rafforzare i provvedimenti degli Stati membri in materia di prevenzione e risposta. Tale piano di azione è stato approvato dalle conclusioni della Presidenza della conferenza ministeriale sulla protezione delle infrastrutture critiche informatizzate svoltasi a Tallinn nel 2009. Il 18 dicembre 2009 il Consiglio ha adottato una risoluzione su "Un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione"[7].

---

3 COM(2001) 298.
4 COM(2006) 251 http://www.cc.cec/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_COM_2006_0251_F_IT_ACTE.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.

L'Agenda digitale europea[8], adottata nel maggio 2010, e le relative conclusioni del Consiglio[9] sottolineavano il pensiero comune secondo cui la fiducia e la sicurezza costituiscono prerequisiti fondamentali per un'ampia diffusione delle TIC e quindi per il conseguimento degli obiettivi di una "crescita intelligente" fissati dalla strategia Europa 2020[10]. Nel capitolo "Fiducia e sicurezza", l'Agenda digitale rilevava la necessità, per tutte le parti interessate, di unire le forze per garantire la sicurezza e la resilienza delle infrastrutture TIC, concentrandosi su prevenzione, preparazione e sensibilizzazione, e di elaborare inoltre meccanismi di sicurezza effettivi e coordinati. In particolare, l'azione fondamentale 6 dell'Agenda digitale europea sollecita misure per una politica rafforzata e di alto livello in materia di sicurezza delle reti e dell'informazione.

Nella comunicazione del marzo 2011 relativa alla protezione delle infrastrutture critiche informatizzate "Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale"[11], la Commissione, dopo aver analizzato i risultati conseguiti in seguito all'adozione del piano di azione sulla protezione delle infrastrutture critiche informatizzate del 2009, ha concluso che l'attuazione del piano ha dimostrato l'insufficienza di un approccio esclusivamente nazionale per far fronte alle sfide della sicurezza e della resilienza e ha sottolineato l'opportunità di portare avanti, in Europa, gli sforzi destinati a costruire un approccio coerente e cooperativo nell'UE. Nella comunicazione sulla protezione delle infrastrutture critiche informatizzate del 2011 la Commissione ha annunciato una serie di interventi e ha invitato gli Stati membri a costituire capacità in materia di SRI e di cooperazione transfrontaliera. La maggior parte di questi interventi, che dovevano essere finalizzati entro la fine del 2012, non è però ancora stata attuata.

Nelle conclusioni del 27 maggio 2011 sulla protezione delle infrastrutture critiche informatizzate, il Consiglio dell'Unione europea ha sottolineato l'urgente necessità di rendere i sistemi TIC e le reti resilienti e sicuri nei confronti di qualsiasi turbativa possibile, accidentale o intenzionale, per elevare il livello di preparazione, sicurezza e capacità di resilienza nell'UE, rafforzare le competenze tecniche per permettere all'Europa di raccogliere la sfida della protezione delle reti e delle infrastrutture informatiche e intensificare la cooperazione tra Stati membri sviluppando meccanismi di cooperazione reciproca in caso di incidenti.

1.3. Disposizioni dell'Unione europea e internazionali vigenti in questo settore

Con il regolamento (CE) n. 460/2004 la Comunità europea ha istituito nel 2004 l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[12], allo scopo di contribuire a garantire un elevato livello di protezione e allo sviluppo di una cultura della sicurezza delle reti e dell'informazione nell'UE. Il 30 settembre 2010[13] è stata adottata una proposta di aggiornamento del mandato dell'ENISA, che è all'esame del Consiglio e del Parlamento europeo. Il quadro normativo riveduto per le comunicazioni elettroniche[14], in vigore dal novembre 2009, impone obblighi di sicurezza ai fornitori di comunicazioni elettroniche[15]. Questi obblighi dovevano essere recepiti nel diritto nazionale entro il maggio 2011.

---

8 COM(2010) 245.
9 Conclusioni del Consiglio del 31 maggio 2010 sull'Agenda digitale europea (10130/10).
10 COM(2010) 2020 e conclusioni del Consiglio europeo del 25-26 marzo 2010 (EUCO 7/10).
11 COM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:IT:HTML.
13 COM(2010) 521.
14 V. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.
15 Articoli 13 *bis* e 13 *ter* della direttiva quadro.

Il quadro regolamentare in materia di protezione dei dati[16] fa obbligo a tutti gli attori con funzione di responsabili del trattamento dei dati (ad es. banche o ospedali) di attivare misure di sicurezza per la protezione dei dati personali. Inoltre, nell'ambito della proposta della Commissione del 2012 relativa ad un regolamento generale sulla protezione dei dati[17], i responsabili del trattamento dei dati dovrebbero segnalare alle autorità di controllo le violazioni dei dati personali. Ciò significa ad esempio che non c'è l'obbligo di segnalare una violazione di sicurezza delle reti e dell'informazione a carico di un determinato servizio che non comprometta dati personali (ad es. in caso di interruzione dei sistemi TIC di una centrale che dia luogo a un blackout).

In virtù della direttiva 2008/114 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, il programma europeo per la protezione delle infrastrutture critiche (EPCIP)[18] stabilisce l'approccio generale per la protezione delle infrastrutture critiche nell'UE. Gli obiettivi del programma europeo per la protezione delle infrastrutture critiche sono pienamente coerenti con la presente proposta e la direttiva dovrebbe applicarsi fatta salva la direttiva 2008/114. Il programma europeo non obbliga gli operatori a segnalare importanti violazioni di sicurezza e non istituisce alcun meccanismo attraverso il quale gli Stati membri possono collaborare o reagire agli incidenti.

I colegislatori stanno attualmente discutendo la proposta di direttiva della Commissione relativa agli attacchi contro i sistemi di informazione[19], che intende armonizzare la punibilità di specifici comportamenti. La direttiva copre solo la punibilità di comportamenti specifici, ma non riguarda la prevenzione di rischi e incidenti di sicurezza delle reti e dell'informazione e l'attenuazione delle loro conseguenze. La presente direttiva dovrebbe applicarsi fatta salva la direttiva relativa agli attacchi contro i sistemi informativi.

Il 28 marzo 2012 la Commissione ha adottato una comunicazione relativa all'istituzione di un Centro europeo per la lotta alla criminalità informatica (EC3)[20]. Il centro, istituito l'11 gennaio 2013, farà parte dell'Ufficio europeo di polizia (Europol) e sarà il punto focale della lotta contro la cibercriminalità nell'UE. EC3 è destinato a raggruppare le competenze europee in materia di cibercriminalità per aiutare gli Stati membri a rafforzare le loro capacità, per fornire loro assistenza nelle indagini contro il cibercrimine, in stretta collaborazione con Eurojust, diventando il portavoce degli investigatori europei sulla criminalità informatica a livello di autorità di contrasto e giudiziarie.

Le istituzioni, le agenzie e gli organi europei hanno costituito proprie squadre di pronto intervento informatico (CERT-UE).

Sul piano internazionale, l'attività dell'UE sulla cibersicurezza si svolge a livello sia bilaterale che multilaterale. Il vertice UE-USA del 2010[21] ha visto la creazione del gruppo di lavoro UE-USA sulla cibersicurezza e il cibercrimine. L'UE è attiva anche in alcune sedi multilaterali come l'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), l'Assemblea generale delle Nazioni Unite, l'Unione internazionale delle telecomunicazioni (UIT), l'Organizzazione per la sicurezza e la cooperazione in Europa (OCSE), il Vertice

---

16 Direttiva 2002/58 del 12 luglio 2002.

17 COM(2012) 11.

18 COM(2006) 786 http://www.cc.cec/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_COM_2006_0786_F_IT_ACTE.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:IT:PDF.

20 COM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:IT:PDF.

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

mondiale sulla società dell'informazione (WSIS) e il Forum sulla governance di internet (IGF).

2. ESITO DELLA CONSULTAZIONE DELLE PARTI INTERESSATE E DELLA VALUTAZIONE D'IMPATTO

2.1. Consultazione delle parti interessate e ricorso al parere di esperti

Dal 23 luglio al 15 ottobre 2012 si è svolta una consultazione pubblica online sul tema "Migliorare la sicurezza delle reti dell'informazione nell'UE". La Commissione ha ricevuto in totale 160 risposte al questionario in linea.

Il risultato principale è che le parti interessate si sono espresse generalmente a favore della necessità di migliorare la sicurezza delle reti e dell'informazione in tutta l'Unione. In particolare: l'82,8% dei partecipanti è del parere che le amministrazioni nell'UE dovrebbero adoperarsi maggiormente per garantire un elevato livello di sicurezza delle reti e dell'informazione; l'82,8% ritiene che gli utenti delle informazioni e dei sistemi non sono consapevoli dell'esistenza di minacce e incidenti di sicurezza; il 66,3% sarebbe in linea di massima a favore dell'introduzione di obblighi regolamentari in materia di gestione dei rischi per la sicurezza delle reti e dell'informazione e secondo l'84,8% gli obblighi dovrebbero essere fissati al livello dell'UE. Un numero elevato di rispondenti ritiene che sarebbe importante adottare obblighi in materia di SRI in particolare nei seguenti settori: banche e finanza (91,1%), energia (89,4%), trasporti (81,7%), sanità (89,4%), servizi internet (89,1%) e amministrazioni pubbliche (87,5%). I rispondenti ritengono anche che se dovesse essere introdotto un obbligo di segnalazione delle violazioni di sicurezza delle reti e dell'informazione alle autorità nazionali competenti, tale obbligo dovrebbe essere stabilito a livello dell'UE (65,1%) e vi dovrebbero essere assoggettate anche le amministrazioni pubbliche (93,5%). Infine i rispondenti ritengono che l'eventuale obbligo di attuare la gestione dei rischi in materia di SRI secondo le migliori prassi del momento non comporterebbe, per loro, costi supplementari significativi (63,4%) e che l'eventuale obbligo di segnalare violazioni di sicurezza non causerebbe costi supplementari significativi (72,3%).

Gli Stati membri sono stati consultati in una serie di configurazioni del Consiglio, nel contesto del Forum europeo degli Stati membri (EFMS), in occasione della conferenza dell'UE sulla cibersicurezza organizzata il 6 luglio 2012 dalla Commissione e dal Servizio europeo per l'azione esterna, nonché in occasione di riunioni bilaterali convocate su richiesta di singoli Stati membri.

Si sono tenute anche discussioni con il settore privato nell'ambito del partenariato europeo pubblico-privato per la resilienza[22] e nel corso di riunioni bilaterali. Per quanto riguarda il settore pubblico, la Commissione ha organizzato dibattiti con l'ENISA e le squadre CERT per le istituzioni europee.

2.2. Valutazione d'impatto

La Commissione ha realizzato una valutazione dell'impatto di tre opzioni strategiche:

opzione 1: mantenere lo status quo (scenario di riferimento);

opzione 2: approccio regolamentare consistente in una proposta legislativa che stabilisce un quadro giuridico unionale comune in materia di SRI, relativo alle capacità degli Stati membri, ai meccanismi di cooperazione a livello UE e alle condizioni imposte ai principali operatori privati e alle amministrazioni pubbliche;

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

opzione 3: approccio misto, ossia iniziative facoltative relative alle capacità nazionali in materia di SRI e ai meccanismi di cooperazione a livello UE, combinate con l'imposizione di obblighi regolamentari ai principali operatori privati e alle amministrazioni pubbliche.

La Commissione è giunta alla conclusione che l'opzione 2 presenta gli impatti positivi più rilevanti perché è suscettibile di migliorare considerevolmente la protezione dei consumatori, delle imprese e delle amministrazioni dell'UE contro gli incidenti di sicurezza delle reti e dell'informazione. In particolare, gli obblighi imposti agli Stati membri garantirebbero un adeguato livello di preparazione a livello nazionale e contribuirebbero a creare quel clima di fiducia reciproca che costituisce un prerequisito per l'effettiva collaborazione a livello dell'UE. La creazione di un meccanismo di cooperazione in rete a livello dell'UE permetterebbe di prevenire e reagire in maniera coerente e coordinata agli incidenti e ai rischi transfrontalieri a carico della sicurezza delle reti e dell'informazione. L'imposizione alle amministrazioni pubbliche e ai principali operatori privati di obblighi in materia di gestione dei rischi a carico della SRI costituirebbe un forte incentivo alla gestione efficace dei rischi di sicurezza. L'obbligo di segnalare gli incidenti SRI aventi un impatto significativo rafforzerebbe le capacità di risposta agli incidenti stessi e la trasparenza. Inoltre, mettendo ordine al suo interno, l'Unione potrebbe imporsi a livello internazionale e diventare una partner ancora più credibile per la collaborazione a livello bilaterale e multilaterale. Inoltre, essa potrebbe promuovere con più forza i diritti e i valori fondamentali dell'UE al suo esterno.

La valutazione quantitativa ha dimostrato che l'opzione 2 non creerebbe costi sproporzionati per gli Stati membri. Il costo per il settore privato sarebbe anch'esso limitato poiché molti dei soggetti interessati sono già tenuti, in linea teorica, a conformarsi ai requisiti di sicurezza in vigore (in particolare l'obbligo per il responsabile della protezione dei dati di adottare misure tecniche e organizzative per la sicurezza dei dati personali, comprese misure per la sicurezza delle reti e dell'informazione). Si è tenuto conto anche della spesa per la sicurezza oggi esistente nel settore privato.

La presente proposta rispetta i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo dinanzi a un giudice e il diritto al contraddittorio. La presente direttiva deve essere applicata nel rispetto di tali diritti e principi.

3. ELEMENTI GIURIDICI DELLA PROPOSTA

3.1. Basi giuridiche

L'Unione europea ha il potere di adottare misure destinate all'instaurazione o al funzionamento del mercato interno, conformemente alle disposizioni pertinenti dei trattati (articolo 26 del trattato sul funzionamento dell'Unione europea - TFUE). A norma dell'articolo 114 del TFUE, l'UE può adottare "le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione o il funzionamento del mercato interno".

Come già indicato, i sistemi informativi e le reti svolgono un ruolo essenziale per agevolare i movimenti transnazionali di beni, servizi e persone. Spesso questi sistemi e queste reti sono interconnessi e internet ha una diffusione planetaria. Tenendo conto di questa dimensione transnazionale intrinseca, un'eventuale perturbazione in uno Stato membro può ripercuotersi sugli altri Stati membri e avere conseguenze in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

Il legislatore unionale ha già riconosciuto la necessità di armonizzare le norme in materia di sicurezza delle reti e dell'informazione per garantire lo sviluppo del mercato interno, in particolare con l'adozione del regolamento (CE) n. 460/2004[23] che istituisce l'ENISA, la cui base giuridica è l'articolo 114 del TFUE.

Le disparità derivanti da capacità nazionali disuguali in materia di sicurezza delle reti e dell'informazione e in termini di politiche e di livello di protezione crea barriere nel mercato interno e giustifica un'azione a livello dell'UE.

3.2. Sussidiarietà

L'intervento europeo nel settore della sicurezza delle reti e dell'informazione è giustificato dal principio di sussidiarietà

Innanzitutto, data la natura transnazionale della sicurezza delle reti e dell'informazione, il mancato intervento a livello di Unione creerebbe una situazione in cui ogni Stato membro agirebbe da solo senza tener conto delle interdipendenze tra le reti e sistemi informativi in tutta l'UE. Un coordinamento adeguato tra gli Stati membri garantirebbe la corretta gestione dei rischi a livello della sicurezza delle reti e dell'informazione nel loro contesto transfrontaliero. Le differenze nelle regolamentazioni in materia di SRI rappresentano una barriera per le imprese che desiderano operare in vari paesi e per il conseguimento di economie di scala globali.

In secondo luogo, per creare parità di condizioni e ovviare alle lacune legislative esistenti sono necessari obblighi regolamentari a livello dell'UE. Un approccio esclusivamente facoltativo ha fatto sì che la cooperazione funzioni attualmente solo tra una minoranza di Stati membri che hanno un livello elevato di capacità. Per coinvolgere tutti gli Stati membri è necessario che tutti loro dispongano del livello minimo di capacità occorrente. Le misure in materia di sicurezza delle reti e dell'informazione adottate dalle amministrazioni nazionali devono essere coerenti tra loro per poter contenere e minimizzare le ripercussioni negative di incidenti di sicurezza. Nella rete, attraverso lo scambio di buone pratiche e il coinvolgimento permanente dell'ENISA, le autorità competenti e la Commissione collaboreranno per facilitare un'attuazione convergente della direttiva in tutta l'UE. Inoltre, interventi concertati in materia di sicurezza delle reti e dell'informazione possono avere un impatto molto benefico sulla tutela effettiva dei diritti fondamentali, in particolare il diritto alla protezione dei dati personali e della vita privata. L'intervento a livello dell'UE migliorerebbe quindi l'efficacia delle politiche nazionali esistenti e ne faciliterebbe lo sviluppo.

Le misure proposte sono anche giustificate in termini di proporzionalità. Le condizioni imposte agli Stati membri corrispondono quanto è strettamente necessario per raggiungere un livello adeguato di preparazione e permettere una collaborazione basata sulla fiducia. Questo consente agli Stati membri di tenere nella debita considerazione le peculiarità nazionali e garantisce che i principi comuni dell'UE siano applicati in maniera proporzionata. Il vasto campo di applicazione consentirà agli Stati membri di attuare la direttiva tenendo conto dei reali rischi che affrontano a livello nazionale, come individuati nella strategia nazionale in materia di SRI. Gli obblighi di attuazione della gestione del rischio riguardano solo entità critiche e impongono misure proporzionate ai rischi. La consultazione pubblica ha sottolineato l'importanza di garantire la sicurezza di questi entità critiche. Gli obblighi di segnalazione riguarderebbero solo incidenti aventi un impatto significativo. Come sopra indicato, le misure non imporrebbero costi sproporzionati perché la normativa vigente in

[23] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1).

materia di protezione dei dati già impone a molte delle suddette entità, in veste di responsabili del trattamento dei dati, l'obbligo di garantire la tutela dei dati personali.

Per evitare di imporre oneri sproporzionati ai piccoli operatori, in particolare alle PMI, gli obblighi sono proporzionati al rischio corso dalla rete o dal sistema informativo di cui si tratta e non si applicano alle microimprese. I rischi dovranno essere individuati in primo luogo dalle entità assoggettate a tali obblighi, le quali dovranno decidere le misure di mitigazione del rischio da adottare.

Gli obiettivi perseguiti possono essere raggiunti a livello dell'UE meglio che a livello di singoli Stati membri, data la natura transnazionale degli incidenti e dei rischi a carico della sicurezza delle reti e dell'informazione. L'Unione può dunque intervenire in conformità al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Nel rispetto del principio di proporzionalità, la direttiva proposta non va al di là di quanto necessario per conseguire questi obiettivi.

Per conseguire gli obiettivi, è opportuno conferire alla Commissione il potere di adottare atti delegati a norma dell'articolo 290 del trattato sul funzionamento dell'Unione europea, allo scopo di integrare o di modificare determinati elementi non essenziali dell'atto di base. La proposta della Commissione intende anche sostenere la proporzionalità nell'attuazione degli obblighi imposti agli operatori dei settori pubblico e privato.

Per garantire condizioni uniformi di attuazione dell'atto di base, è opportuno conferire alla Commissione il potere adottare atti di esecuzione in conformità all'articolo 291 del trattato sul funzionamento dell'Unione europea.

Data la vasta portata della direttiva proposta, tenendo conto del fatto che affronta campi soggetti ad una forte regolamentazione e in considerazione degli obblighi legali derivanti dal suo capo IV, è necessario che la notifica delle misure di attuazione sia accompagnata dalla trasmissione di documenti esplicativi. Conformemente alla dichiarazione politica congiunta degli Stati membri e della Commissione sui documenti esplicativi del 28 settembre 2011, gli Stati membri si sono impegnati ad accompagnare, ove ciò sia giustificato, la notifica delle loro misure di attuazione con uno o più documenti intesi a chiarire il rapporto tra gli elementi di una direttiva e le parti corrispondenti degli strumenti nazionali di attuazione. In relazione alla presente direttiva il legislatore ritiene che la trasmissione di tali documenti sia giustificata.

4. INCIDENZE SUL BILANCIO

È opportuno che la cooperazione e lo scambio di informazioni tra Stati membri siano supportati da una infrastruttura sicura. La proposta avrà implicazioni finanziarie sul bilancio dell'UE soltanto se gli Stati membri scelgono di adattare un'infrastruttura esistente (ad es. sTESTA) e chiedono alla Commissione di farlo nell'ambito del QFP 2014-2020. Il costo una tantum si stima a 1 250 000 EUR, che sarebbe posto a carico del bilancio dell'UE, linea di bilancio 09.03.02 (promuovere interconnessione e interoperabilità dei servizi pubblici nazionali online nonché accesso a tali reti — capitolo 09.03, meccanismo per collegare l'Europa — reti di telecomunicazioni) a condizione che vi siano sufficienti fondi disponibili nell'ambito del CEF. In alternativa, gli Stati membri possono ripartirsi il costo una tantum di adattamento di un'infrastruttura esistente oppure decidere di creare un'infrastruttura nuova accollandosene i costi, che si stimano a circa 10 milioni di EUR all'anno.

2013/0027 (COD)

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

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[1],

sentito il garante europeo della protezione dei dati,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Le reti e i sistemi e servizi di informazione svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per l'attività economica e il benessere sociale e in particolare ai fini del funzionamento del mercato interno.

(2) La portata e la frequenza degli incidenti dolosi o accidentali a carico della sicurezza stanno aumentando e rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. Tali incidenti possono impedire il proseguimento di attività economiche, provocare notevoli perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia dell'Unione.

(3) In quanto strumenti di comunicazione non vincolati a frontiere, i sistemi informativi digitali - e in prima linea internet - svolgono un ruolo essenziale per agevolare i movimenti transnazionali di beni, servizi e persone. Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi in uno Stato membro possono ripercuotersi sugli altri Stati membri e avere conseguenze in tutta l'UE. La resilienza e la stabilità delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno.

(4) È opportuno istituire un meccanismo di cooperazione a livello dell'Unione che permetta lo scambio di informazioni e il coordinamento delle attività di individuazione e di risposta attinenti alla sicurezza delle reti e dell'informazione (SRI). Perché tale meccanismo sia effettivo e inclusivo è importante che tutti gli Stati membri dispongano di un livello minimo di capacità e si dotino di una strategia per garantire un livello elevato di sicurezza delle reti e dell'informazione sul loro territorio. È opportuno che anche alle pubbliche amministrazioni e agli operatori di infrastrutture informatiche critiche si applichino obblighi minimi di sicurezza, per promuovere una cultura della gestione dei rischi e garantire la segnalazione degli incidenti più gravi.

[1] GU C […] del […], pag. […].

(5) È necessario che la presente direttiva si applichi a tutte le reti e a tutti i sistemi informativi in modo da coprire tutti i relativi rischi e incidenti. È opportuno tuttavia che gli obblighi fatti alle pubbliche amministrazioni e agli operatori del mercato non si applichino alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro)[2], perché tali imprese sono soggette a specifici obblighi di sicurezza e integrità previsti dall'articolo 13 *bis* di detta direttiva; i suddetti obblighi non devono inoltre applicarsi ai prestatori di servizi fiduciari.

(6) Le capacità esistenti non bastano a garantire un livello elevato di sicurezza delle reti e dell'informazione nell'Unione. I livelli di preparazione negli Stati membri sono molto diversi tra loro il che comporta una frammentazione degli approcci nell'Unione. Ne deriva un livello disomogeneo di protezione dei consumatori e delle imprese che compromette il livello globale di sicurezza delle reti e dell'informazione nell'Unione. La mancanza di obblighi minimi comuni imposti alle pubbliche amministrazioni e agli operatori del mercato rende inoltre impossibile la creazione di un meccanismo globale ed efficace di cooperazione a livello dell'Unione.

(7) Per una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi è pertanto necessario un approccio globale a livello di Unione, che contempli la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni e coordinamento delle azioni, nonché obblighi minimi comuni di sicurezza per tutti gli operatori del mercato interessati e le pubbliche amministrazioni.

(8) Le disposizioni della presente direttiva lasciano impregiudicata la possibilità per ciascuno Stato membro di adottare le misure necessarie per assicurare la tutela dei suoi interessi essenziali in materia di sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza e consentire la ricerca, l'individuazione e il perseguimento dei reati. Conformemente all'articolo 346 del TFUE, nessuno Stato membro è tenuto a fornire informazioni la cui divulgazione sia dallo stesso considerata contraria agli interessi essenziali della propria sicurezza.

(9) Per conseguire e mantenere un livello comune elevato di sicurezza delle reti e dei sistemi informativi è opportuno che ogni Stato membro disponga di una strategia nazionale in materia di SRI che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare. Per poter raggiungere una capacità di risposta tale da permettere un'efficiente collaborazione a livello nazionale e unionale in caso di incidenti è necessario che siano elaborati, a livello nazionale, piani di collaborazione in materia di sicurezza delle reti e dell'informazione, rispondenti a condizioni essenziali.

(10) Per permettere l'efficace attuazione delle disposizioni adottate a norma della presente direttiva è necessario che sia istituito o individuato in ogni Stato membro un organismo responsabile del coordinamento degli aspetti della SRI, che funga da perno della cooperazione transnazionale a livello unionale. Questi organismi devono essere dotati di risorse adeguate sul piano tecnico, finanziario e umano per permettere loro di eseguire in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva.

---

[2] GU L 108 del 24.4.2002, pag. 33.

(11) È necessario che tutti gli Stati membri siano dotati delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi. Per questo è necessario che, in tutti gli Stati membri, siano costituite squadre di pronto intervento informatico rispondenti a determinati requisiti essenziali, in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione.

(12) Basandosi sui notevoli progressi compiuti all'interno del Forum europeo degli Stati membri (EFMS) nel promuovere le discussioni e gli scambi di buone pratiche, come l'elaborazione dei principi della collaborazione europea in caso di crisi cibernetica, è opportuno che la Commissione e gli Stati membri creino una rete che assicuri una comunicazione permanente tra loro e ne sostenga la collaborazione. Tale meccanismo di collaborazione sicuro ed effettivo è destinato a permettere di strutturare e coordinare lo scambio di informazioni e le attività di individuazione e risposta a livello dell'Unione.

(13) L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) dovrebbe assistere gli Stati membri e la Commissione mettendo loro a disposizione le proprie competenze e consulenze e agevolando lo scambio di buone pratiche. In particolare è opportuno che la Commissione consulti l'ENISA nell'applicazione della presente direttiva. Per garantire un'informazione effettiva e tempestiva degli Stati membri e della Commissione è necessario che gli incidenti e i rischi siano segnalati precocemente attraverso la rete di collaborazione. Per creare capacità e conoscenze tra gli Stati membri, la rete di collaborazione dovrebbe anche servire da strumento di scambio di buone pratiche, assistendo i propri membri a creare capacità e conducendo l'organizzazione di valutazioni tra pari e di esercitazioni in materia di SRI.

(14) Nella rete di collaborazione è opportuno creare un'infrastruttura di scambio sicuro di informazioni che consenta lo scambio di informazioni sensibili e riservate tra autorità competenti. Fatto salvo il loro obbligo di segnalare gli incidenti e i rischi di dimensione unionale alla rete di collaborazione, è opportuno che l'accesso a informazioni riservate di altri Stati membri sia concesso soltanto agli Stati membri che dimostrano di possedere processi e risorse finanziarie, tecniche ed umane e un'infrastruttura di comunicazione tali da garantirne la partecipazione effettiva, efficiente e sicura alla rete.

(15) La collaborazione tra il settore pubblico e il settore privato è essenziale visto che la maggioranza delle reti e dei sistemi informativi funziona per opera di operatori privati. Gli operatori del mercato devono essere incoraggiati a portare avanti propri meccanismi informali di collaborazione per garantire la sicurezza delle reti e dell'informazione. È necessario che essi collaborino anche con il settore pubblico e scambino informazioni e buone pratiche in cambio di supporto operativo in caso di incidenti.

(16) Per garantire la trasparenza e una corretta informazione dei cittadini e degli operatori del mercato dell'UE è necessario che le competenti autorità allestiscano un sito comune su cui pubblicare informazioni non riservate sui rischi e sugli incidenti.

(17) Qualora le informazioni siano considerate riservate in virtù di norme unionali e nazionali sulla riservatezza degli affari, è necessario che tale riservatezza sia garantita nello svolgimento delle attività e nella realizzazione degli obiettivi stabiliti dalla presente direttiva.

(18) In base in particolare alle esperienze nazionali in materia di gestione delle crisi e in collaborazione con l'ENISA è opportuno che la Commissione e gli Stati membri elaborino un piano unionale di collaborazione in materia di SRI che definisce meccanismi di collaborazione nella lotta contro i rischi e gli incidenti. Occorre tenere debitamente conto di tale piano ai fini della segnalazione di preallarmi all'interno della rete di collaborazione.

(19) È necessario notificare un preallarme nella rete solo se la portata e la gravità dell'incidente o del rischio di cui si tratta sono o potrebbero essere così significative da richiedere l'informazione o il coordinamento della risposta a livello dell'Unione. È quindi necessario che i preallarmi si limitino agli incidenti o ai rischi, effettivi o potenziali, che presentano una crescita rapida, che superano le capacità nazionali di risposta o che colpiscono più di uno Stato membro. Per garantirne la corretta valutazione è necessario che siano comunicate alla rete di collaborazione tutte le informazioni pertinenti alla valutazione del rischio o dell'incidente.

(20) Dopo aver ricevuto e valutato un preallarme, è opportuno che le autorità competenti adottino una risposta coordinata nell'ambito del piano unionale di collaborazione materia di SRI. È necessario che le autorità competenti e la Commissione siano informate delle misure adottate a livello nazionale in esito alla risposta coordinata.

(21) Data la natura planetaria dei problemi che interessano la sicurezza delle reti e dell'informazione è necessaria una cooperazione internazionale più stretta per migliorare le norme di sicurezza e gli scambi di informazioni e promuovere un approccio globale comune agli aspetti della SRI.

(22) La responsabilità di garantire la sicurezza delle reti e dell'informazione incombe in larga misura alle pubbliche amministrazioni e agli operatori del mercato. È opportuno promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio corso. È altresì fondamentale creare pari condizioni per l'efficace funzionamento della rete di collaborazione in modo da garantire la collaborazione effettiva di tutti gli Stati membri.

(23) La direttiva 2002/21/CE fa obbligo alle imprese che forniscono reti pubbliche di comunicazioni elettroniche o servizi di comunicazione elettronica accessibili al pubblico di adottare misure adeguate per salvaguardarne l'integrità e la sicurezza e introduce obblighi di comunicazione delle violazioni di sicurezza o perdita dell'integrità. La direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)[3] obbliga i fornitori di servizi di comunicazione elettronica accessibili al pubblico ad adottare misure e procedure tecniche e organizzative adeguate a salvaguardare la sicurezza dei loro servizi.

(24) È opportuno che tali obblighi imposti al settore delle comunicazioni elettroniche siano estesi ai principali fornitori di servizi della società dell'informazione, quali definiti dalla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società

[3] GU L 201 del 31.7.2002, pag. 37.

dell'informazione[4], che supportano i servizi della società dell'informazione a valle o attività online come le piattaforme del commercio elettronico, i portali di pagamento su internet, le reti sociali, i motori di ricerca, i servizi nella nuvola e i negozi online di applicazioni. Le eventuali perturbazioni che colpiscono questi servizi essenziali della società dell'informazione impediscono la fornitura di altri servizi della società dell'informazione che si basano sui primi. Gli sviluppatori di programmi informatici e i costruttori di hardware non sono fornitori di servizi della società dell'informazione e sono pertanto esclusi. È necessario che i suddetti obblighi siano estesi anche alle pubbliche amministrazioni e agli operatori di infrastrutture critiche che dipendono pesantemente dalla tecnologia dell'informazione e delle comunicazioni e che sono essenziali per il mantenimento di funzioni vitali, in termini economici o societali, come l'elettricità e il gas, i trasporti, gli enti creditizi, le borse e la sanità. Le eventuali perturbazioni a carico di tali reti e sistemi informativi avrebbero ripercussioni sul mercato interno.

(25) Le misure tecniche e organizzative imposte alle amministrazioni pubbliche e agli operatori del mercato non devono richiedere che una particolare informazione commerciale o un particolare prodotto della tecnologia delle comunicazioni siano concepiti, sviluppati e fabbricati in una maniera particolare.

(26) È necessario che le amministrazioni pubbliche e gli operatori di mercato garantiscano la sicurezza delle reti e dei sistemi di cui hanno il controllo. Si tratta in particolare di reti e sistemi privati gestiti dal loro personale IT interno, oppure la cui sicurezza sia stata esternalizzata. Gli obblighi di notifica e di sicurezza devono applicarsi agli operatori del mercato e alle amministrazioni pubbliche indipendentemente dal fatto che la manutenzione delle loro reti e dei loro sistemi informativi sia eseguita al loro interno o sia esternalizzata.

(27) Per evitare di imporre un onere finanziario e amministrativo sproporzionato a piccoli operatori e piccoli utenti, è necessario che gli obblighi siano proporzionati al rischio corso dalla rete o dal sistema informativo di cui si tratta, tenendo conto dello stato dell'arte di tali misure. Questi obblighi non devono applicarsi alle microimprese.

(28) È opportuno che le autorità competenti procurino in particolare di salvaguardare l'esistenza di canali informali e affidabili di scambio di informazioni tra gli operatori del mercato e tra settore pubblico e privato. La pubblicità degli incidenti segnalati alle autorità competenti deve contemperare l'opportunità che il pubblico sia informato delle minacce esistenti con i possibili danni di immagine e commerciali per le pubbliche amministrazioni e gli operatori di mercato che segnalano gli incidenti. Nell'attuare gli obblighi di notifica è necessario che le autorità competenti tengano adeguatamente conto della necessità di mantenere strettamente riservate le informazioni sulle vulnerabilità del prodotto prima di diffondere i rimedi di sicurezza appropriati.

(29) È necessario che le autorità competenti possiedano i mezzi necessari all'assolvimento dei loro compiti, come la facoltà di ottenere informazioni sufficienti dagli operatori del mercato e dalle amministrazioni pubbliche per valutare il livello di sicurezza delle reti e dei sistemi informativi, nonché dati attendibili e completi su incidenti reali che hanno avuto un impatto sul funzionamento delle reti e dei sistemi informativi.

(30) In molti casi alla base di un incidente vi sono attività criminali. Si può sospettare la natura dolosa di incidenti anche se non vi sono prove sufficientemente chiare fin

[4] GU L 204 del 21.7.1998, pag. 37.

dall'inizio. Al riguardo, una risposta effettiva e esauriente alla minaccia di incidenti di sicurezza presuppone un'adeguata collaborazione tra autorità competenti e autorità di contrasto. In particolare, la promozione di un ambiente sicuro, affidabile e più resiliente richiede la segnalazione sistematica, alle autorità di contrasto, degli incidenti di cui si sospetta la natura dolosa grave. La natura dolosa grave degli incidenti va valutata alla luce delle norme dell'UE sulla cibercriminalità.

(31) I molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti. Gli Stati membri devono adempiere l'obbligo di segnalazione degli incidenti di sicurezza in modo da minimizzare gli oneri amministrativi nel caso in cui l'incidente di sicurezza costituisca anche una violazione di dati personali, in conformità al regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati[5]. Coordinandosi con le autorità competenti e le autorità responsabili della protezione dei dati, l'ENISA può contribuire alla messa a punto di meccanismi e modelli per lo scambio di informazioni, evitando in questo modo che siano necessari due modelli di notifica. Un modello di notifica unico può facilitare la segnalazione di incidenti che compromettono dati personali, alleviando in questo modo gli oneri amministrativi per le imprese e le pubbliche amministrazioni.

(32) La standardizzazione degli obblighi di sicurezza è un'esigenza che nasce dal mercato. Per garantire un'applicazione convergente delle norme di sicurezza è opportuno che gli Stati membri incoraggino il rispetto o la conformità a norme specifiche volte a garantire un livello elevato di sicurezza in tutta l'Unione. A tal fine potrebbe essere necessario elaborare norme armonizzate in conformità al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio[6].

(33) È opportuno che la Commissione riesamini le disposizioni della presente direttiva a scadenze regolari, in particolare per valutare la necessità di modificarle in funzione dell'evoluzione delle tecnologie o delle condizioni del mercato.

(34) Per garantire il corretto funzionamento della rete di collaborazione deve essere conferito alla Commissione il potere di adottare atti a norma dell'articolo 290 del trattato sul funzionamento dell'Unione europea per quanto riguarda la definizione dei criteri che devono essere rispettati perché uno Stato membro sia autorizzato a partecipare al sistema sicuro di scambio di informazioni, la specificazione più precisa degli eventi che richiedono l'invio di un preallarme e la definizione delle circostanze alle quali gli operatori del mercato e le amministrazioni pubbliche sono tenuti a notificare gli incidenti.

(35) È particolarmente importante che la Commissione, nel corso del suo lavoro preparatorio, svolga consultazioni adeguate, anche a livello di esperti. Quando elabora e redige atti delegati la Commissione è tenuta a procedere alla trasmissione

---

5 SEC(2012) 72 definitivo.

6 GU L 316 del 14.11.2012, pag. 12.

contestuale, tempestiva ed appropriata dei relativi documenti al Parlamento europeo e al Consiglio.

(36) Al fine di garantire condizioni uniformi di esecuzione della presente direttiva è opportuno attribuire alla Commissione competenze di esecuzione per quanto riguarda la collaborazione tra le autorità competenti e la Commissione nel quadro della rete di collaborazione, l'accesso all'infrastruttura sicura di scambio di informazioni, il piano unionale di collaborazione in materia di SRI, il formato e le procedure applicabili all'informazione del pubblico in merito agli incidenti e le pertinenti norme e/o le specifiche tecniche in materia di SRI. Tali competenze di esecuzione devono essere esercitate in conformità al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione[7].

(37) Nell'applicazione della presente direttiva la Commissione deve coordinarsi adeguatamente con i comitati settoriali competenti e gli altri organi costituiti a livello dell'Unione in particolare nei settori dell'energia, dei trasporti, delle banche e della sanità.

(38) Le informazioni considerate riservate da un'autorità competente, in conformità con la normativa unionale e nazionale sulla riservatezza degli affari, possono essere scambiate con la Commissione e con altre autorità competenti solo nella misura in cui tale scambio sia strettamente necessario ai fini dell'applicazione della presente direttiva. Lo scambio deve limitarsi alle sole informazioni pertinenti ed essere commisurato allo scopo.

(39) Lo scambio di informazioni sui rischi e sugli incidenti all'interno della rete di collaborazione e il rispetto degli obblighi di notifica degli incidenti alle autorità nazionali competenti possono richiedere il trattamento di dati personali. Tale trattamento di dati personali è necessario per conseguire gli obiettivi di interesse pubblico perseguiti dalla presente direttiva ed è quindi legittimo in virtù dell'articolo 7 della direttiva 95/46/CE. In relazione a tali obiettivi legittimi esso non costituisce un intervento sproporzionato ed inammissibile che pregiudicherebbe la sostanza stessa del diritto di protezione dei dati personali sancito dall'articolo 8 della Carta dei diritti fondamentali. Nell'applicazione della presente direttiva si applica, per quanto di ragione, il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione[8]. In caso di trattamento di dati da parte di istituzioni ed organismi dell'Unione, tale trattamento ai fini dell'attuazione della presente direttiva deve rispettare le disposizioni del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

(40) Poiché gli obiettivi della presente direttiva, ossia garantire un elevato livello di sicurezza delle reti e dell'informazione nell'Unione, non possono essere realizzati in misura sufficiente dai soli Stati membri e possono dunque, a causa della portata e degli effetti dell'azione, essere realizzati meglio a livello di Unione, quest'ultima può adottare provvedimenti in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per

[7] GU L 55 del 28.2.2011, pag. 13.
[8] GU L 145 del 31.5.2001, pag. 43.

conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(41) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto al rispetto della vita privata e delle comunicazioni, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo dinanzi a un giudice e il diritto al contraddittorio. La presente direttiva deve essere applicata nel rispetto di tali diritti e principi,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e campo di applicazione

1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di Sicurezza delle reti e dell'informazione (in seguito SRI) nell'Unione.

2. A tal fine la presente direttiva:

(a) stabilisce obblighi per tutti gli Stati membri in materia di prevenzione, trattamento e risposta nei confronti dei rischi e degli incidenti a carico delle reti e dei sistemi informativi;

(b) crea un meccanismo di collaborazione tra gli Stati membri per garantire un'applicazione uniforme della presente direttiva nell'Unione e, se necessario, una risposta e un trattamento coordinati ed efficienti dei rischi di incidenti a carico delle reti e dei sistemi informativi;

(c) stabilisce obblighi di sicurezza per gli operatori del mercato e le amministrazioni pubbliche.

3. Gli obblighi di sicurezza di cui all'articolo 14 non si applicano né alle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, ai sensi della direttiva 2002/21/CE, le quali sono tenute a rispettare gli obblighi specifici di sicurezza e integrità stabiliti dagli articoli 13 *bis* e 13 *ter* della medesima direttiva, né ai prestatori di servizi fiduciari.

4. La presente direttiva lascia impregiudicate le disposizioni legislative dell'Unione in materia di cibercriminalità e la direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione[9].

5. La presente direttiva lascia impregiudicate anche le disposizioni della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[10], della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni

[9] GU L 345 del 23.12.2008, pag. 75.
[10] GU L 281 del 23.11.1995, pag. 31.

elettroniche e del regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati[11].

6. Lo scambio di informazioni all'interno della rete di collaborazione in virtù delle disposizioni del capo III e le notifiche di incidenti a carico della SRI in virtù dell'articolo 14 possono comportare il trattamento di dati personali. Tale trattamento, necessario per conseguire gli obiettivi di pubblico interesse perseguiti dalla presente direttiva, è soggetto all'autorizzazione degli Stati membri a norma dell'articolo 7 della direttiva 95/46/CE e in virtù della direttiva 2002/58/CE quali recepite negli ordinamenti nazionali.

Articolo 2

Armonizzazione minima

Nulla osta a che gli Stati membri adottino o mantengano in vigore disposizioni atte a garantire un livello di sicurezza più elevato, fermi restando gli obblighi loro imposti dal diritto dell'Unione.

Articolo 3

Definizioni

Ai fini della presente direttiva si intende per:

(1) "rete e sistema informativo",

(a) una rete di comunicazioni elettroniche ai sensi della direttiva 2002/21/CE e

(b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati elettronici e

(c) i dati elettronici conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione;

(2) "sicurezza", la capacità di una rete o di un sistema informativo di resistere, a un determinato livello di riservatezza, a eventi imprevisti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi offerti o accessibili tramite tale rete o sistema informativo;

(3) "rischio", ogni circostanza o evento con potenziali effetti pregiudizievoli per la sicurezza;

(4) "incidente", ogni circostanza o evento con un reale effetto pregiudizievole per la sicurezza;

(5) "servizi della società dell'informazione", i servizi ai sensi dell'articolo 1, punto 2, della direttiva 98/34/CE;

(6) "piano di collaborazione in materia di SRI", un piano che definisce il quadro dei ruoli organizzativi, delle responsabilità e delle procedure per il mantenimento o il ripristino dell'operatività delle reti e dei sistemi informativi qualora si verifichi un rischio o un incidente a loro carico;

[11] SEC(2012) 72 definitivo.

(7) “trattamento dell’incidente”, tutte le procedure necessarie per l’analisi, il contenimento e la risposta a un incidente;

(8) “operatore del mercato”,

(a) fornitore di servizi della società dell’informazione che consentono la fornitura di altri servizi della società dell’informazione; un elenco non esaustivo di tali operatori figura nell’allegato II;

(b) operatore di infrastrutture critiche che sono essenziali per il mantenimento di attività vitali per l’economia e la società nei campi dell’energia, dei trasporti, delle banche, delle borse e della sanità; un elenco non esaustivo di tali operatori figura nell’allegato II;

(9) “norma”, una norma ai sensi del regolamento (UE) n. 1025/2012;

(10) “specifica”, una specifica ai sensi del regolamento (UE) n. 1025/2012;

(11) “prestatore di servizio fiduciario”, una persona fisica o giuridica che presta un servizio elettronico consistente nella creazione, verifica, convalida, nel trattamento e nella conservazione di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito, autenticazione di siti web e certificati elettronici, compresi i certificati di firma elettronica e di sigillo elettronico.

CAPO II

QUADRI NAZIONALI PER LA SICUREZZA DELLE RETI E DELL’INFORMAZIONE

Articolo 4

Principio

Gli Stati membri assicurano un livello elevato di sicurezza delle reti e dei sistemi informativi nel loro territorio in conformità alla presente direttiva.

Articolo 5

Strategia nazionale e piano nazionale di collaborazione in materia di SRI

1. Ogni Stato membro adotta una strategia nazionale in materia di SRI nella quale definisce gli obiettivi strategici e misure strategiche e regolamentari concrete per conseguire e conservare un livello elevato di sicurezza delle reti e dell’informazione. La strategia nazionale in materia di SRI affronta in particolare i seguenti aspetti:

(a) la definizione degli obiettivi e delle priorità della strategia in base ad un’analisi aggiornata dei rischi e degli incidenti;

(b) un quadro di governance per raggiungere obiettivi e priorità della strategia, con una definizione chiara dei ruoli e delle responsabilità degli organismi pubblici e degli altri attori implicati;

(c) l’individuazione delle misure generali di preparazione, risposta e recupero, con meccanismi di collaborazione tra settore pubblico e settore privato;

(d) l’indicazione di programmi di formazione, sensibilizzazione e istruzione;

(e) i piani di ricerca e sviluppo e la descrizione di come essi rispecchino le priorità individuate.

2. La strategia nazionale comprende un piano nazionale di collaborazione in materia di SRI rispondente almeno alle seguenti prescrizioni:

(a) un piano di valutazione dei rischi per individuare i rischi e valutare le conseguenze di potenziali incidenti;

(b) la definizione dei ruoli e delle responsabilità dei vari attori implicati nell'attuazione del piano;

(c) la definizione dei processi di collaborazione e comunicazione che garantiscono la prevenzione, l'individuazione, la risposta, la riparazione e il recupero, con la relativa modulazione in funzione del livello di allerta;

(d) una tabella di marcia per esercitazioni relative alla SRI e formazioni per rafforzare, convalidare e testare il piano; una documentazione degli insegnamenti tratti e il loro inserimento negli aggiornamenti del piano.

3. La strategia nazionale e il piano nazionale di collaborazione in materia di SRI sono comunicati alla Commissione entro un mese dalla loro adozione.

Articolo 6

Autorità nazionale competente in materia di sicurezza delle reti e dei sistemi informativi

1. Ogni Stato membro designa un'autorità nazionale competente in materia di sicurezza delle reti e dei sistemi informativi (la "autorità competente").

2. Le autorità competenti controllano l'applicazione della presente direttiva a livello nazionale e contribuiscono alla coerenza di applicazione della medesima in tutta l'Unione.

3. Gli Stati membri garantiscono che le autorità competenti siano dotate di risorse adeguate sul piano tecnico, finanziario e umano per eseguire in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva. Gli Stati membri provvedono a garantire la collaborazione effettiva, efficiente e sicura delle autorità competenti attraverso la rete di cui all'articolo 8.

4. Gli Stati membri procurano che le autorità competenti ricevano le notifiche degli incidenti da parte delle amministrazioni pubbliche e degli operatori del mercato come specificato all'articolo 14, paragrafo 2 e che siano loro attribuiti i poteri di attuazione e di controllo di cui all'articolo 15.

5. Le autorità competenti consultano le competenti autorità nazionali di contrasto e le autorità nazionali competenti per la protezione dei dati e collaborano con le stesse come necessario.

6. Ogni Stato membro comunica senza indugio alla Commissione l'autorità competente designata, i suoi compiti e qualsiasi ulteriore modifica dei medesimi. Ogni Stato membro rende pubblica l'autorità competente designata.

Articolo 7

Squadre di pronto intervento informatico

1. Ogni Stato membro costituisce una squadra di pronto intervento informatico (in seguito "CERT") col compito di trattare gli incidenti e i rischi secondo una procedura

ben definita e conforme ai requisiti di cui all'allegato I, punto 1. È possibile creare una squadra CERT all'interno dell'autorità competente.

2. Gli Stati membri procurano che le squadre CERT siano dotate di risorse umane, tecniche e finanziarie adeguate per l'adempimento dei loro compiti, precisati nell'allegato I, punto 2.

3. Gli Stati membri procurano che le squadre CERT possano contare su un'infrastruttura di informazione e comunicazione sicura e resiliente a livello nazionale, che sia compatibile e interoperabile con il sistema sicuro di scambio di informazioni di cui all'articolo 9.

4. Gli Stati membri comunicano alla Commissione le risorse e il mandato delle squadre CERT e la procedura di trattamento degli incidenti loro affidata.

5. La squadra CERT opera sotto la supervisione dell'autorità competente la quale rivede periodicamente l'adeguatezza delle sue risorse, il mandato e l'efficacia della procedura di trattamento degli incidenti.

CAPO III

COOPERAZIONE FRA AUTORITÀ COMPETENTI

Articolo 8

Rete di collaborazione

1. Le autorità competenti e la Commissione costituiscono una rete (rete di collaborazione) per collaborare in caso di rischi e incidenti a carico delle reti e dei sistemi informativi.

2. La rete di collaborazione assicura la comunicazione permanente tra la Commissione e le autorità competenti. Se richiesta, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) assiste la rete di collaborazione mettendole a disposizione le proprie competenze e consulenze.

3. All'interno della rete di collaborazione le autorità competenti:

   (a) diffondono preallarmi in merito a rischi e a incidenti in conformità all'articolo 10;

   (b) garantiscono una risposta coordinata in conformità all'articolo 11;

   (c) pubblicano periodicamente informazioni non riservate sui preallarmi in corso e sulla risposta coordinata su un sito comune;

   (d) discutono e valutano insieme, su richiesta di uno Stato membro o della Commissione, una o più strategie nazionali e uno o più piani nazionali di collaborazione in materia di SRI ai sensi dell'articolo 5, nell'ambito della presente direttiva;

   (e) discutono e valutano insieme, su richiesta di uno Stato membro o della Commissione, l'efficacia delle squadre CERT, in particolare in occasione di esercitazioni in materia di SRI eseguite a livello di Unione;

   (f) collaborano e scambiano informazioni su tutti gli aspetti pertinenti col Centro europeo per la lotta alla criminalità informatica di Europol e con altri organismi europei competenti in particolare nei campi della protezione dei dati, dell'energia, dei trasporti, delle banche, delle borse e della sanità;

(g) si scambiano reciprocamente e comunicano alla Commissione informazioni e buone pratiche e si assistono reciprocamente ai fini della creazione di capacità in materia di SRI;

(h) organizzano periodicamente revisioni tra pari in materia di capacità e preparazione;

(i) organizzano esercitazioni in materia di SRI al livello di Unione e partecipano, secondo il caso, a esercitazioni internazionali in materia di SRI.

4. La Commissione stabilisce, mediante atti di esecuzione, le modalità necessarie per agevolare la collaborazione di cui ai paragrafi 2 e 3 tra le autorità competenti e con la Commissione. Tali atti di esecuzione sono adottati secondo la procedura di consultazione di cui all'articolo 19, paragrafo 2.

Articolo 9

Sistema sicuro di scambio di informazioni

1. Lo scambio di informazioni sensibili e riservate all'interno della rete di collaborazione avviene attraverso un'infrastruttura sicura.

2. Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 18, relativi alla definizione dei criteri che devono essere rispettati perché uno Stato membro sia autorizzato a partecipare al sistema sicuro di scambio di informazioni, riguardanti:

(a) la disponibilità di un'infrastruttura di informazione e comunicazione sicura e resiliente a livello nazionale, che sia compatibile e interoperabile con l'infrastruttura sicura della rete di collaborazione a norma dell'articolo 7, paragrafo 3, e

(b) l'esistenza di processi e risorse umane, tecniche e finanziarie adeguate per le proprie autorità competenti e squadre CERT, che ne permettano la partecipazione effettiva, efficiente e sicura al sistema sicuro di scambio di informazioni a norma dell'articolo 6, paragrafo 3, articolo 7, paragrafo 2 e articolo 7, paragrafo 3.

3. La Commissione adotta, mediante atti di esecuzione, decisioni sull'accesso degli Stati membri a tale infrastruttura sicura, in base ai criteri di cui ai paragrafi 2 e 3. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3.

Articolo 10

Preallarmi

1. Le autorità competenti o la Commissione trasmettono preallarmi all'interno della rete di collaborazione in merito ai rischi e agli incidenti che rispondono ad una o più delle seguenti condizioni:

(a) la cui portata aumenta o è suscettibile di aumentare rapidamente;

(b) che superano o sono suscettibili di superare la capacità nazionale di risposta;

(c) che colpiscono o sono suscettibili di colpire più di uno Stato membro.

2. Nei preallarmi le autorità competenti e la Commissione comunicano tutte le informazioni pertinenti in loro possesso che possono essere utili a valutare il rischio o l'incidente.

3. Su richiesta di uno Stato membro o di propria iniziativa la Commissione può chiedere a uno Stato membro di fornire qualunque informazione pertinente su uno specifico rischio o incidente.

4. Qualora il preallarme riguardi un rischio o un incidente di sospetta natura dolosa, le autorità competenti o la Commissione ne informano il Centro europeo per la lotta alla criminalità informatica di Europol.

5. Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 18, per precisare ulteriormente i rischi e gli incidenti per i quali è necessaria la trasmissione dei preallarmi di cui al paragrafo 1.

Articolo 11

Risposta coordinata

1. In seguito ad un preallarme a norma dell'articolo 10 le autorità competenti adottano, dopo aver valutato le informazioni pertinenti, una risposta coordinata in conformità al piano unionale di collaborazione in materia di SRI di cui all'articolo 12.

2. Le varie misure adottate a livello nazionale in esito alla risposta coordinata sono comunicate alla rete di collaborazione.

Articolo 12

Piano unionale di collaborazione in materia di SRI

1. Alla Commissione è conferito il potere di adottare, mediante atti di esecuzione, un piano unionale di collaborazione in materia di SRI. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3.

2. Il piano unionale di collaborazione in materia di SRI comporta:

   (a) ai fini dell'applicazione dell'articolo 10,

      – una definizione del formato e delle procedure di raccolta e scambio di informazioni compatibili e comparabili sui rischi e sugli incidenti da parte delle autorità competenti,

      – una definizione delle procedure e dei criteri di valutazione dei rischi e degli incidenti da parte della rete di collaborazione;

   (b) la procedura da seguire per le risposte coordinate di cui all'articolo 11, con l'individuazione dei ruoli e delle responsabilità e delle procedure di collaborazione;

   (c) una tabella di marcia di esercitazioni relative alla SRI e formazioni per rafforzare, convalidare e testare il piano;

   (d) un programma relativo al trasferimento di conoscenze tra gli Stati membri in materia di creazione di capacità e apprendimento tra pari;

   (e) un programma di sensibilizzazione e formazione tra gli Stati membri.

3. Il piano unionale di collaborazione in materia di SRI è adottato non oltre l'anno successivo all'entrata in vigore della presente direttiva ed è riveduto periodicamente.

Articolo 13

Cooperazione internazionale

Ferma restando la possibilità, per la rete di collaborazione, di intrattenere una cooperazione informale a livello internazionale, l'Unione può concludere accordi internazionali con paesi terzi o organizzazioni internazionali che permettono o organizzano la loro partecipazione ad alcune delle attività della rete di collaborazione. Tali accordi tengono conto della necessità di garantire la protezione adeguata dei dati personali che circolano nella rete di collaborazione.

CAPO IV

SICUREZZA DELLE RETI E DEI SISTEMI INFORMATIVI DELLE PUBBLICHE AMMINISTRAZIONI E DEGLI OPERATORI DEL MERCATO

Articolo 14

Obblighi in materia di sicurezza e notifica degli incidenti

1. Gli Stati membri procurano che le amministrazioni pubbliche e gli operatori del mercato adottino misure tecniche e organizzative adeguate alla gestione dei rischi che corre la sicurezza delle reti e dei sistemi informativi di cui hanno il controllo e che usano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza adeguato al rischio in essere. In particolare sono adottate misure per prevenire e minimizzare l'impatto di incidenti a carico delle reti e dei sistemi informativi relativi ai servizi principali prestati, assicurando in questo modo la continuità dei servizi supportati da tali reti e sistemi informativi.

2. Gli Stati membri procurano che le amministrazioni pubbliche e gli operatori del mercato notifichino all'autorità competente gli incidenti aventi un impatto significativo sulla sicurezza dei servizi principali prestati.

3. Gli obblighi di cui ai paragrafi 1 e 2 si applicano a tutti gli operatori del mercato che prestano servizi all'interno dell'Unione europea.

4. L'autorità competente può informare il pubblico, oppure richiedere alle amministrazioni pubbliche e agli operatori del mercato di informarlo, se ritiene che la divulgazione dell'incidente sia di pubblico interesse. Una volta l'anno l'autorità competente trasmette alla rete di collaborazione una relazione sintetica delle notifiche ricevute e delle misure adottate conformemente al presente paragrafo.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 18 riguardanti la definizione delle circostanze alle quali le amministrazioni pubbliche e gli operatori del mercato sono tenuti a notificare gli incidenti.

6. Fatti salvi gli atti delegati adottati a norma del paragrafo 5, le autorità competenti possono adottare orientamenti e, se necessario, emanare istruzioni sulle circostanze alle quali le amministrazioni pubbliche e gli operatori del mercato sono tenuti a notificare gli incidenti.

7. Alla Commissione è conferito il potere di definire, mediante atti di esecuzione, i formati e le procedure applicabili ai fini del paragrafo 2. Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 19, paragrafo 3.

8. Il disposto dei paragrafi 1 e 2 non si applica alle microimprese quali definite nella raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese[12].

Articolo 15

Attuazione e controllo

1. Gli Stati membri procurano che le autorità competenti siano dotate di tutti i poteri necessari per indagare i casi di mancato rispetto, da parte delle amministrazioni pubbliche o degli operatori del mercato, degli obblighi loro imposti dall'articolo 14 e gli effetti di tale mancato rispetto sulla sicurezza delle reti e dei sistemi informativi.

2. Gli Stati membri procurano che le autorità competenti abbiano il potere di richiedere agli operatori del mercato e alle amministrazioni pubbliche di:

   (a) fornire le informazioni necessarie per valutare la sicurezza delle loro reti e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza;

   (b) sottoporsi ad audit condotto da un organismo qualificato indipendente o da un'autorità nazionale e metterne i risultati a disposizione dell'autorità competente.

3. Gli Stati membri procurano che le autorità competenti abbiano il potere di emanare istruzioni vincolanti per gli operatori del mercato e le amministrazioni pubbliche.

4. Le autorità competenti notificano alle autorità di contrasto gli incidenti di cui sospettano la natura dolosa grave.

5. Le autorità competenti operano in stretta cooperazione con le autorità competenti della protezione dei dati personali nei casi di incidenti che comportano violazioni di dati personali.

6. Gli Stati membri garantiscono che gli obblighi imposti dal presente capo alle pubbliche amministrazioni e agli operatori del mercato possano essere soggetti a controllo giurisdizionale.

Articolo 16

Normazione

1. Per garantire l'attuazione convergente del disposto dell'articolo 14, paragrafo 1, gli Stati membri incoraggiano l'uso di norme e/o specifiche relative alla sicurezza delle reti e dell'informazione.

2. Mediante atti di esecuzione la Commissione redige un elenco delle norme di cui al paragrafo 1. L'elenco è pubblicato nella Gazzetta ufficiale dell'Unione europea.

CAPO V

DISPOSIZIONI FINALI

Articolo 17

Sanzioni

[12] GU L 124 del 20.5.2003, pag. 36.

1. Gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri notificano tali disposizioni alla Commissione entro la data di attuazione della presente direttiva e provvedono a dare immediata notifica di ogni successiva modifica.

2. Gli Stati membri procurano che, se un incidente di sicurezza coinvolge dati personali, le sanzioni previste siano coerenti con le sanzioni contemplate dal regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati[13].

Articolo 18

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. È conferito alla Commissione il potere di adottare gli atti delegati di cui all'articolo 9, paragrafo 2, all'articolo 10, paragrafo 5, e all'articolo 14, paragrafo 5. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 9, paragrafo 2, all'articolo 10, paragrafo 5 e all'articolo 14, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla sua pubblicazione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Non appena adotta un atto delegato, la Commissione lo notifica simultaneamente al Parlamento europeo e al Consiglio.

5. L'atto delegato adottato ai sensi dell'articolo 9, paragrafo 2, dell'articolo 10, paragrafo 5 e dell'articolo 14, paragrafo 5, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 19

Procedura di comitato

[13] SEC(2012) 72 definitivo.

1. La Commissione è assistita da un comitato (in prosieguo "il comitato per la sicurezza delle reti e dell'informazione"). Tale comitato è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 4 del regolamento (UE) n. 182/2011.

3. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 20

Revisione

La Commissione riesamina periodicamente il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La prima relazione è presentata entro tre anni dalla data di attuazione di cui all'articolo 21. A tal fine la Commissione può chiedere agli Stati membri di fornire informazioni senza ritardi.

Articolo 21

Attuazione

1. Gli Stati membri adottano e pubblicano, entro [un anno dalla data di adozione], le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

   Essi applicano tali disposizioni a partire da [un anno e mezzo dalla data di adozione].

   Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della loro pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni essenziali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 22

Entrata in vigore

La presente direttiva entra in vigore il [ventesimo] giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 23

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles,

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*

ALLEGATO I

Requisiti e compiti delle squadre di pronto intervento informatico (CERT)

I requisiti e i compiti delle squadre CERT devono essere adeguatamente e chiaramente definiti nel quadro di una strategia e/o di una regolamentazione nazionale. Essi includono quanto segue:

(1) Requisiti per le squadre CERT

(a) La squadra CERT garantisce un'elevata disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che le permettono di essere contattata e di contattare altri. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla sua base di utenti e ai partner con cui collabora.

(b) La squadra CERT attua e gestisce misure di sicurezza che garantiscono la riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni che riceve e tratta.

(c) Gli uffici della squadra CERT e i sistemi informativi di supporto sono ubicati in siti sicuri.

(d) È istituito un sistema di gestione della qualità del servizio per seguire le prestazioni della squadra CERT e garantire un costante processo di miglioramento. Tale sistema si basa su metriche chiaramente definite che includono livelli formali di servizio e indicatori principali di prestazione.

(e) Continuità operativa:

- la squadra CERT è dotata di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi,
- la squadra CERT dispone di personale sufficiente per garantirne l'operatività 24 ore su 24,
- la squadra CERT opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario costituire sistemi ridondanti e spazi di lavoro di backup perché la squadra CERT possa garantire l'accesso permanente ai mezzi di comunicazione.

(2) Compiti delle squadre CERT

(a) I compiti delle squadre CERT comprendono almeno:

- monitoraggio degli incidenti a livello nazionale,
- emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti,
- risposta agli incidenti,
- informazioni sul rischio dinamico e analisi degli incidenti, nonché sensibilizzazione situazionale,
- massiccia sensibilizzazione del pubblico sui rischi connessi all'attività online,
- organizzazione di campagne sulla sicurezza delle reti e dell'informazione (SRI).

(b) Le squadre CERT stabiliscono relazioni di cooperazione con il settore privato.

(c) Per facilitare la cooperazione, le squadre CERT promuovono l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:

- procedure di trattamento degli incidenti e dei rischi,
- programmi di classificazione degli incidenti, dei rischi e delle informazioni,
- tassonomie delle metriche,
- modelli di scambi di informazione su rischi, incidenti e convenzioni di denominazione dei sistemi.

ALLEGATO II

Elenco degli operatori del mercato

Operatori di cui all'articolo 3, paragrafo 8, lettera a):

1. Piattaforme di commercio elettronico

2. Portali di pagamento su internet

3. Reti sociali

4. Motori di ricerca

5. Servizi nella nuvola (*cloud computing*)

6. Negozi online di applicazioni

Operatori di cui all'articolo 3, paragrafo 8, lettera b):

1. Energia

- Fornitori di elettricità e di gas
- Operatori dei sistemi di distribuzione dell'elettricità e/o del gas e distributori al dettaglio ai consumatori finali
- Gestori dei sistemi di trasporto, di impianti di stoccaggio o di impianti di GNL nel settore del gas naturale
- Operatori dei sistemi di trasmissione nel settore dell'energia elettrica
- Oleodotti e depositi di petrolio
- Operatori del mercato dell'energia elettrica e del gas
- Operatori di impianti di produzione, raffinazione e trattamento di petrolio e gas naturale

2. Trasporti

- Vettori aerei (trasporto aereo di merci e passeggeri)
- Vettori marittimi (compagnie di navigazione per il trasporto marittimo e costiero di passeggeri e per il trasporto marittimo e costiero di merci)
- Trasporto ferroviario (gestori dell'infrastruttura, imprese integrate e operatori di trasporto ferroviario)
- Aeroporti
- Porti
- Operatori attivi nel controllo della gestione del traffico
- Servizi logistici ausiliari a) deposito e stoccaggio, b) movimentazione merci e c) altre attività di supporto ai trasporti)

3. Settore bancario: enti creditizi ai sensi dell'articolo 4, punto 1, della direttiva 2006/48/CE.

4. Infrastrutture dei mercati finanziari: Borse e stanze di compensazione di tipo controparte centrale

5. Settore sanitario: istituti sanitari (compresi ospedali e cliniche private) e altri soggetti che forniscono assistenza sanitaria

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati nella struttura ABM/ABB

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria

1.7. Modalità di gestione prevista

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

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.

1.2. Settore/settori interessati nella struttura ABM/ABB[37]

- 09 – Reti di comunicazione, contenuti e tecnologie

1.3. Natura della proposta/iniziativa

☒ La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[38]

☐ La proposta/iniziativa riguarda la **proroga di un'azione esistente**

☐ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivo/obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

Lo scopo della direttiva proposta è assicurare un livello comune elevato di sicurezza delle reti e dell'informazione (SRI) nell'Unione.

1.4.2. Obiettivi specifici e attività ABM/ABB interessate

La proposta stabilisce misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione.

Gli obiettivi specifici sono:

1. istituire un livello minimo di sicurezza delle reti e dell'informazione negli Stati membri aumentando il livello generale di preparazione e risposta;

2. migliorare la collaborazione a livello dell'Unione in materia di sicurezza delle reti e dell'informazione per lottare efficacemente contro le minacce e gli incidenti transfrontalieri. Sarà creata un'infrastruttura di scambio sicuro di informazioni per consentire lo scambio di informazioni sensibili e riservate tra autorità competenti;

3. creare una cultura di gestione del rischio e migliorare lo scambio di informazioni tra i settori pubblico e privato.

Attività ABM/ABB interessate

La direttiva copre entità (imprese e organizzazioni, comprese le PMI) in una serie di settori (energia, trasporti, enti creditizi e borse, sanità e facilitatori di servizi internet fondamentali), oltre che le amministrazioni pubbliche; essa riguarda anche i legami con le autorità di contrasto e la protezione dei dati e gli aspetti di sicurezza delle reti e dell'informazione nelle relazioni esterne.

- 09 – Reti di comunicazione, contenuti e tecnologie

- 02 – Imprese

---

[37] ABM: Activity Based Management (gestione per attività) – ABB: Activity Based Budgeting (bilancio per attività).

[38] A norma dell'articolo 49, paragrafo 6, lettera a) o b), del regolamento finanziario.

- 32 - Energia

- 06 - Mobilità e trasporti

- 17 - Salute e tutela dei consumatori

- 18 – Affari interni

- 19 - Relazioni esterne

- 33 - Giustizia

- 12 - Mercato interno

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Notevole miglioramento della protezione dei consumatori, delle imprese e delle amministrazioni dell'UE contro incidenti, minacce e rischi per la sicurezza delle reti e dell'informazione.

Per ulteriori dettagli si rinvia alla sezione 8.2 (Impatto dell'opzione 2 – Approccio regolamentare) del documento di lavoro dei servizi della Commissione sulla valutazione d'impatto che accompagna la presente proposta legislativa.

1.4.4. Indicatori di risultato e di impatto

Precisare gli indicatori che permettono di seguire l'attuazione della proposta/iniziativa.

Gli indicatori relativi al monitoraggio e alla valutazione figurano nella sezione 10 della valutazione d'impatto.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità da coprire nel breve e lungo termine

Ogni Stato membro dovrà dotarsi di:

- una strategia nazionale in materia di sicurezza delle reti e dell'informazione (SRI);

- un piano di collaborazione in materia di sicurezza delle reti e dell'informazione (SRI);

- un'autorità nazionale competente in materia di sicurezza delle reti e dell'informazione (SRI), nonché di

- una squadra di pronto intervento informatico (CERT).

A livello dell'UE gli Stati membri dovranno collaborare attraverso una rete.

Le amministrazioni pubbliche e i principali operatori privati dovranno effettuare la gestione del rischio in materia di SRI e notificare alle autorità competenti gli incidenti a carico della sicurezza delle reti e dell'informazione aventi un impatto significativo.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

Data la natura transfrontaliera della sicurezza delle reti e dell'informazione le divergenze nelle pertinenti politiche e legislazioni rappresentano un ostacolo per le imprese che intendono operare in vari paesi e per il raggiungimento di economie globali di scala. La mancanza di un intervento livello dell'UE creerebbe una situazione in cui ogni Stato membro agirebbe da solo senza tener conto delle interdipendenze tra le reti e sistemi informativi.

Gli obiettivi prefissati possono quindi essere raggiunti attraverso un'azione a livello dell'UE meglio che attraverso l'azione dei singoli Stati membri.

1.5.3. Insegnamenti tratti da esperienze analoghe

La proposta è motivata dalla constatazione che sono necessari obblighi regolamentari per creare parità di condizioni e porre rimedio a determinate lacune legislative. In questo campo, un approccio esclusivamente facoltativo ha fatto sì che la cooperazione funzioni solo tra una minoranza di Stati membri che hanno un livello elevato di capacità.

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

La proposta è del tutto coerente con l'Agenda digitale europea e quindi con la strategia Europa 2020. È anche coerente e complementare con il quadro normativo per le comunicazioni elettroniche dell'UE, con la direttiva sulle infrastrutture critiche europee e con la direttiva sulla protezione dei dati.

La presente proposta accompagna la comunicazione congiunta della Commissione e dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza relativa ad una strategia europea per la cibersicurezza e ne costituisce parte integrante.

1.6. Durata e incidenza finanziaria

– ☐ Proposta/iniziativa di durata limitata

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

– ☒ Proposta/iniziativa di durata illimitata

– Il periodo di attuazione inizierà immediatamente dopo l'adozione (prevista nel 2015) durerà 18 mesi. L'applicazione della direttiva inizierà tuttavia dopo l'adozione e comporterà la creazione dell'infrastruttura sicura a supporto della collaborazione tra gli Stati membri;

– vi farà seguito un funzionamento a pieno ritmo.

1.7. Modalità di gestione prevista[39]

– ☒ Gestione centralizzata diretta da parte della Commissione

– ☒ Gestione centralizzata indiretta con delega delle funzioni di esecuzione a:

– ☐Agenzie esecutive

– ☒ Organismi creati dalle Comunità[40]

– ☐ Organismi pubblici nazionali/organismi investiti di attribuzioni di servizio pubblico

– ☐ Persone incaricate di attuare azioni specifiche di cui al titolo V del trattato sull'Unione europea, che devono essere indicate nel pertinente atto di base ai sensi dell'articolo 49 del regolamento finanziario

– ☐ Gestione concorrente con gli Stati membri

– ☐ Gestione decentrata con paesi terzi

– ☐ Gestione congiunta con organizzazioni internazionali, compresa l'Agenzia spaziale europea

Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".

Osservazioni
L'ENISA, a un'agenzia decentralizzata creata dalle Comunità, può assistere gli Stati membri e la Commissione nell'attuazione della direttiva in base al suo mandato e mediante riassegnazione delle risorse previste per tale agenzia dal quadro finanziario pluriennale 2014-2020.

[39] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] A norma dell'articolo 185 del regolamento finanziario.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La Commissione riesaminerà periodicamente il funzionamento della direttiva e presenterà una relazione in proposito al Parlamento europeo e al Consiglio.

La Commissione valuterà anche il corretto recepimento della direttiva da parte degli Stati membri.

La proposta riguardante il CEF prevede anche la possibilità di procedere a una valutazione delle modalità di realizzazione dei progetti e dell'impatto della loro attuazione, al fine di stabilire se gli obiettivi previsti, compresi quelli in materia di tutela dell'ambiente, siano stati raggiunti.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

- ritardi nell'attuazione del progetto di creazione dell'infrastruttura sicura

2.2.2. Modalità di controllo previste

Le convenzioni e le decisioni di attuazione delle azioni in virtù del CEF prevedranno la supervisione e il controllo finanziario da parte della Commissione o di un rappresentante da essa ha autorizzato, nonché verifiche della Corte dei conti e controlli in loco svolti dall'Ufficio europeo per la lotta antifrode (OLAF).

2.2.3. Costi e benefici dei controlli e probabile tasso di non conformità

Controlli ex ante e ex post basati sul rischio e la possibilità di controlli in loco permetteranno di mantenere i costi dei controlli a un livello ragionevole.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste.

La Commissione adotta provvedimenti opportuni volti a garantire che, nella realizzazione delle azioni finanziate ai sensi della presente direttiva, gli interessi finanziari dell'Unione siano tutelati mediante l'applicazione di misure preventive contro la frode, la corruzione e ogni altra attività illecita, mediante controlli efficaci e, ove fossero rilevate irregolarità, mediante il recupero delle somme indebitamente versate e, se del caso, sanzioni efficaci, proporzionate e dissuasive.

La Commissione o i suoi rappresentanti e la Corte dei conti hanno potere di revisione contabile, esercitabile sulla base di documenti e sul posto, su tutti i beneficiari di sovvenzioni, contraenti e subcontraenti che hanno ottenuto finanziamenti dell'Unione nell'ambito del programma.

L'Ufficio europeo per la lotta antifrode (OLAF) può effettuare controlli e verifiche sul posto presso gli operatori economici che siano direttamente o indirettamente interessati da tali finanziamenti, secondo le procedure stabilite dal regolamento (Euratom, CE) n. 2185/96, per accertare eventuali frodi, casi di corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a convenzioni o decisioni di sovvenzione o a contratti relativi ai finanziamenti stessi.

Fatti salvi i commi precedenti, gli accordi di cooperazione con paesi terzi e organizzazioni internazionali, le convenzioni e decisioni di sovvenzione e i contratti conclusi in applicazione del presente regolamento devono abilitare espressamente la Commissione, la Corte dei conti e l'OLAF a svolgere tali revisioni, controlli e verifiche sul posto.

Il CEF prevede che i contratti di sovvenzione e gli appalti seguano i contratti tipo che precisano le misure antifrode generalmente applicabili.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero [Denominazione…...….]	Diss./Non diss. (41)	di paesi EFTA[42]	di paesi candidati 43	di paesi terzi	ai sensi dell'articolo 18, paragrafo 1, lettera a *bis*), del regolamento finanziario
	09 03 02 promuovere l'interconnessione e l'interoperabilità dei servizi pubblici nazionali online nonché l'accesso a tali reti	Diss.	NO	NO	NO	NO

- Nuove linee di bilancio di cui è chiesta la creazione:

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero [Denominazione…...….]	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 18, paragrafo 1, lettera a *bis*), del regolamento finanziario
	[XX.YY.YY.YY]		SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

41 SD = Stanziamenti dissociati / SND = Stanziamenti non dissociati.

42 EFTA: Associazione europea di libero scambio.

43 Paesi candidati e, se del caso, paesi potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale:	1	Crescita intelligente e inclusiva

DG: <…….>			2015* [44]	Anno **2016**	Anno **2017**	Anno **2018**	Anni successivi (2019-2021) e oltre			**TOTALE**
• Stanziamenti operativi										
09 03 02	Impegni	(1)	1,250**	0,000						**1,250**
	Pagamenti	(2)	0,750	0,250	0,250					**1,250**
Stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici[45]			**0,000**							**0,000**
Numero della linea di bilancio		(3)	**0,000**							**0,000**
TOTALE degli stanziamenti per la DG <….>	Impegni	=1+1a +3	1,250	0,000						**1,250**
	Pagamenti	=2+2a +3	0,750	0,250	0,250					**1,250**

• TOTALE degli stanziamenti operativi	Impegni	(4)	1,250	0,000						**1,250**
	Pagamenti	(5)	0,750	0,250	0,250					**1,250**
• TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)	**0,000**							

[44] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

[45] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

TOTALE degli stanziamenti per la RUBRICA 1 del quadro finanziario pluriennale	Impegni	=4+ 6	1,250	0,000						**1,250**
	Pagamenti	=5+ 6	0,750	0,250	0,250					**1,250**

* Il calendario preciso dipenderà dalla data di adozione della proposta da parte del legislatore (ossia se la direttiva sarà approvata nel corso del 2014 l'adattamento di un'infrastruttura esistente inizierà nel 2015, altrimenti un anno più tardi).

** Se gli Stati membri scelgono di usare un'infrastruttura esistente e di coprire il costo di adattamento una tantum avvalendosi del bilancio dell'UE, come spiegato nei punti 1.4.3 e 1.7, il costo di personalizzazione di una rete a sostegno della cooperazione tra gli Stati membri, conformemente al capo III della direttiva (preallarme, risposta coordinata ecc.) si stima a 1 250 000 EUR. Quest'importo è leggermente più alto di quello indicato nella valutazione d'impatto ("circa 1 milione di EUR") perché si basa su una stima più precisa degli elementi costitutivi necessari per la costruzione di tale infrastruttura. Gli elementi costitutivi necessari e i relativi costi si basano su una stima del CCR che si fonda sull'esperienza di elaborazione di sistemi simili in altri settori come la sanità pubblica; essi comprenderebbero: un sistema di allerta rapida e di notifica per la sicurezza delle reti e dell'informazione (SRI) (275 000 EUR); una piattaforma di scambio di informazioni (400 000 EUR); un sistema di preallarme e di reazione (275 000 EUR); una "sala situazione" (300 000 EUR), per un totale di 1 250 000 EUR. Un piano di attuazione più dettagliato sarà presentato nel quadro dello studio di fattibilità atteso nell'ambito del contratto specifico SMART 2012/0010: 'Studio di fattibilità e attività preparatorie della realizzazione di un sistema di preallarme e di reazione contro ciberattacchi e ciberperturbazioni'.

Se la proposta/iniziativa incide su più rubriche:

• TOTALE degli stanziamenti operativi	Impegni	(4)	0,000	0,000						
	Pagamenti	(5)	0,000	0,000						
• TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)	**0,000**	**0,000**						
TOTALE degli stanziamenti per le RUBRICHE da 1 a 4 del quadro finanziario pluriennale (Importo di riferimento)	Impegni	=4+ 6	1,250	0,000						1,250
	Pagamenti	=5+ 6	0,750	0,250	0,250					1,250

Rubrica del quadro finanziario pluriennale	**5**	"Spese amministrative"

Mio EUR (al terzo decimale)

		Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anni successivi (2019-2021) e oltre			**TOTALE**
DG:CNECT									
• Risorse umane		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Altre spese amministrative		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
TOTALE DG CNECT	Stanziamenti	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Mio EUR (al terzo decimale)

		Anno **2015**[46]	Anno **2016**	Anno **2017**	Anno **2018**	Anni successivi (2019-2021) e oltre			**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Pagamenti	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

3.2.2. Incidenza prevista sugli stanziamenti operativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

– Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **2015***		Anno **2016**		Anno **2017**		Anno **2018**		Anni successivi (2019-2021) e oltre						**TOTALE**	
	RISULTATI																	
	Tipo di risultato [47]	Costo medio	Numero	Costo	Numero	Costo	Numero	Costo	Numero	Costo	Numero	Costo	Numero	Costo	Numero	Costo	Numero totale	Costo totale
OBIETTIVO SPECIFICO 2[48] Infrastruttura sicura di scambio di informazioni																		
- Risultato	Adatta-mento dell'infra struttura																	
Totale parziale Obiettivo specifico 2			1	1,250**													1	1,250
COSTO TOTALE				1,250														1,250

47 I risultati sono i prodotti e i servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di chilometri di strade costruiti ecc.).

48 Quale descritto nella sezione 1.4.2. "Obiettivo/obiettivi specifici…".

* Il calendario preciso dipenderà dalla data di adozione della proposta da parte del legislatore (ossia se la direttiva sarà approvata nel corso del 2014 l'adattamento di un'infrastruttura esistente inizierà nel 2015, altrimenti un anno più tardi).

** Vedere sezione 3.2.1.

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.3.1. Sintesi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2015**[49]	Anno **2016**	Anno **2017**	Anno **2018**	Anni successivi (2019-2021) e oltre			**TOTALE**
RUBRICA 5 del quadro finanziario pluriennale								
Risorse umane	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Altre spese amministrative	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Totale parziale RUBRICA 5 del quadro finanziario pluriennale	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Esclusa la RUBRICA 5 [50] **del quadro finanziario pluriennale**								
Risorse umane	0,000	0,000						**0,000**
Altre spese di natura amministrativa								
Totale parziale esclusa la RUBRICA 5 del quadro finanziario pluriennale	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTALE	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Gli stanziamenti amministrativi richiesti saranno coperti dagli stanziamenti della DG CNECT già assegnati alla gestione dell'azione e/o riassegnati all'interno della DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) può assistere gli Stati membri e la Commissione nell'attuazione della direttiva in base al suo mandato e mediante riassegnazione delle risorse previste per tale agenzia dal quadro finanziario pluriennale 2014-2020, ossia senza assegnazione di risorse finanziarie o umane aggiuntive.

49 L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

50 Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.2. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane

– ☑ La proposta/iniziativa comporta l'utilizzazione di risorse umane della Commissione, come spiegato di seguito:

In linea di massima non saranno necessarie risorse umane supplementari. Le risorse umane necessarie saranno molto limitate e vi farà fronte il personale della DG che è già assegnato alla gestione dell'azione.

Stima da esprimere in numeri interi (o, al massimo, con un decimale)

		Anno **2015**	Anno **2016**	Anno **2017**	Anno **2018**	Anni successivi (2019-2021) e oltre		
• Posti della tabella dell'organico (funzionari e agenti temporanei)								
09 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)		4	4	4	4	4	4	4
XX 01 01 02 (nelle delegazioni)								
XX 01 05 01 (ricerca indiretta)								
10 01 05 01 (ricerca diretta)								
• Personale esterno (in equivalenti a tempo pieno: ETP)[51]								
09 01 02 01 (AC, END e INT della "dotazione globale")		1	1	1	1	1	1	1
XX 01 02 02 (AC, AL, END, INT e JED nelle delegazioni)								
XX 01 04 *yy*[52]	- in sede[53]							
	- nelle delegazioni							
XX 01 05 02 (AC, END e INT – Ricerca indiretta)								
10 01 05 02 (AC, END e INT – Ricerca diretta)								
Altre linee di bilancio (specificare)								
TOTALE		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG CNECT già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) può assistere gli Stati membri e la Commissione nell'attuazione della direttiva in base al suo mandato attuale e mediante riassegnazione delle risorse previste per tale agenzia dal quadro finanziario pluriennale 2014-2020, ossia senza assegnazione di risorse finanziarie o umane aggiuntive.

51 AC = agente contrattuale; INT = personale interinale (*intérimaire*); JED = giovane esperto in delegazione (*jeune expert en délégation*); AL = agente locale; END = esperto nazionale distaccato;

52 Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

53 Principalmente per i fondi strutturali, il Fondo europeo agricolo per lo sviluppo rurale (FEASR) e il Fondo europeo per la pesca (FEP).

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	- Elaborazione di atti delegati a norma dell'articolo 14, paragrafo 3 - Elaborazione di atti di esecuzione a norma dell'articolo 8, dell'articolo 9, paragrafo 2, dell'articolo 12, dell'articolo 14, paragrafo 5 e dell'articolo 16 - Contribuire alla collaborazione in rete a livello sia strategico che operativo - Avvio di dibattiti internazionali ed eventuale conclusione di accordi internazionali
Personale esterno	Supporto a tutti i compiti sopra illustrati in funzione delle necessità.

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

– ☑ La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

– ☐ La proposta/iniziativa implica una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

L'impatto finanziario stimato sulle spese operative della proposta si verificherà se gli Stati membri scelgono di adattare un'infrastruttura esistente e chiedono alla Commissione di realizzarne l'adattamento nell'ambito del QFP 2014-2020. Il relativo costo una tantum sarà coperto nell'ambito del CEF purché siano disponibili fondi sufficienti. In alternativa gli Stati membri possono spartirsi i costi dell'adattamento dell'infrastruttura o i costi di creazione di un'infrastruttura nuova.

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[54].

Non pertinente.

3.2.5. Partecipazione di terzi al finanziamento

– La proposta/iniziativa non prevede il cofinanziamento da parte di terzi

3.3. Incidenza prevista sulle entrate

– ☑ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

[54] Cfr. punti 19 e 24 dell'Accordo interistituzionale.