CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 1 ottobre 2010 (06.10)
(OR. en)

14358/10

Fascicolo interistituzionale: 2010/0275 (COD)

TELECOM 99
MI 346
DATAPROTECT 70
JAI 794
CAB 16
INST 361
CODEC 943

PROPOSTA

Mittente:	Commissione europea
Data:	1 ottobre 2010
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

Si trasmette in allegato, per le delegazioni, la proposta della Commissione inviata con lettera del Signor Jordi AYET PUIGARNAU al Signor Pierre de BOISSIEU, Segretario generale del Consiglio dell'Unione europea.

All.: COM(2010) 521 definitivo

COMMISSIONE EUROPEA

Bruxelles, 30.9.2010
COM(2010) 521 definitivo

2010/0275 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

1.1. Contesto politico

L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) è stata istituita nel marzo 2004 con il regolamento (CE), n. 460/2004[1] per un periodo iniziale di cinque anni, al fine di "assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito [dell'Unione] e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione europea, contribuendo in tal modo al corretto funzionamento del mercato interno". Il regolamento (CE) n. 1007/2008[2] ha prolungato il mandato dell'ENISA fino a marzo 2012.

Con la proroga del mandato dell'ENISA nel 2008 è stato anche avviato un dibattito sull'orientamento generale delle iniziative europee intese a garantire la sicurezza delle reti e dell'informazione (NIS, network and information security); la Commissione ha contribuito al dibattito avviando una consultazione pubblica sui possibili obiettivi di un rafforzamento della strategia in materia a livello di Unione. Nel corso della consultazione pubblica, svoltasi da novembre 2008 a gennaio 2009, sono pervenuti quasi 600 contributi[3].

Il 30 marzo 2009 la Commissione ha adottato una comunicazione sulla protezione delle infrastrutture critiche informatizzate (CIIP, *Critical Information Infrastructure Protection*)[4] incentrata sulla protezione dell'Europa dai ciberattacchi e dalle ciberperturbazioni rafforzando la preparazione, la sicurezza e la resilienza e stabilendo un piano d'azione che prevede, per l'ENISA, un ruolo principalmente di supporto agli Stati membri. La conferenza ministeriale dell'UE sulla protezione delle infrastrutture critiche informatizzate, tenutasi a Tallinn (Estonia) il 27 e 28 aprile 2009[5], ha largamente appoggiato il piano d'azione. Le conclusioni della presidenza dell'UE alla conferenza sottolineano l'importanza di "*sfruttare il sostegno operativo*" dell'ENISA, affermano che l'ENISA "*offre un valido strumento per consolidare l'impegno alla cooperazione in questo campo*" e sottolineano la necessità di ripensare e riformulare il mandato dell'Agenzia "*per mettere al centro le priorità e le esigenze dell'UE*; *per raggiungere una capacità di reazione più flessibile, sviluppare le capacità e competenze europee e rafforzare l'efficienza operativa e l'impatto globale dell'Agenzia*." In questo modo l'ENISA potrebbe diventare "*una risorsa permanente per ciascuno Stato membro e l'Unione europea nel suo insieme*".

---

1 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).

2 Il regolamento (CE) n. 1007/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, che modifica il regolamento (CE) n. 460/2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione per quanto riguarda la durata dell'Agenzia (GU L 293 del 31.10.2008, pag. 1).

3 La sintesi dei risultati della consultazione pubblica "*Towards a Strengthened Network and Information Security Policy in Europe*" è allegata alla valutazione dell'impatto annessa alla presente proposta (allegato 11).

4 COM(2009) 149 del 30.3.2009.

5 Documento di riflessione http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf Conclusioni della presidenza: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

Dopo le discussioni in seno al consiglio Telecomunicazioni dell'11 giugno 2009, durante il quale gli Stati membri hanno espresso il loro accordo a prolungare il mandato dell'ENISA e ad aumentarne le risorse, alla luce dell'importanza della sicurezza delle reti e dell'informazione e alle sfide in costante evoluzione del settore, il dibattito si è concluso durante la presidenza svedese dell'Unione. La risoluzione del Consiglio del 18 dicembre 2009 su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione[6] riconosce il ruolo e il potenziale dell'ENISA e "*la necessità di sviluppare ulteriormente l'ENISA perché diventi un organismo efficace*". La risoluzione sottolinea inoltre la necessità di modernizzare e rafforzare l'Agenzia affinché possa essere di sostegno alla Commissione e agli Stati membri per colmare il divario tra l'aspetto tecnologico e quello strategico, fungendo da centro di conoscenze dell'UE per le tematiche connesse alla sicurezza delle reti e dell'informazione.

1.2. Contesto generale

Le tecnologie dell'informazione e della comunicazione (TIC) fanno ormai parte integrante dell'economia e della società dell'Unione europea. Le TIC sono esposte a minacce che superano i confini nazionali e che mutano con l'evolvere delle tecnologie e del mercato. Poiché le TIC sono globali, interconnesse e interdipendenti da altre infrastrutture, non è possibile garantirne la sicurezza e la resilienza con un approccio esclusivamente nazionale e non coordinato. Allo stesso tempo, le sfide legate alla sicurezza delle reti e dell'informazione evolvono rapidamente e le reti e i sistemi informatici devono essere protetti in modo efficace da ogni tipo di interruzione e guasto, compresi gli attacchi ad opera dell'uomo.

Le politiche in materia di sicurezza delle reti e dell'informazione svolgono un ruolo fondamentale nell'ambito dell'Agenda digitale europea[7], iniziativa faro della strategia "Europa 2020", per sfruttare e far progredire il potenziale delle TIC e tradurre tale potenziale in crescita sostenibile e innovazione. L'Agenda digitale fissa come priorità incoraggiare l'adozione delle TIC e rafforzare la fiducia verso la società dell'informazione.

L'ENISA è stata istituita per assicurare un elevato ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione. L'esperienza accumulata con l'Agenzia e le difficoltà e le sfide che si sono presentate hanno reso evidente la necessità di modernizzare il mandato dell'Agenzia per rispondere meglio alle esigenze dell'UE in relazione ai seguenti fattori:

- frammentazione degli approcci nazionali per affrontare le sfide in costante mutamento;
- mancanza di modelli di collaborazione nell'attuazione delle strategie in materia di sicurezza delle reti e dell'informazione;
- preparazione insufficiente a causa della limitata capacità di allarme rapido e di reazione a livello europeo;
- carenza di dati affidabili e limitata conoscenza dei problemi in evoluzione in Europa;

---

[6] Risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (GU C 321 del 29.12.2009, pag. 1). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:it:PDF.

[7] COM(2010) 245 del 19.5.2010.

- scarsa consapevolezza dei rischi e delle problematiche legate alla sicurezza delle reti e dell'informazione;

- difficoltà di integrare gli aspetti inerenti la sicurezza nelle strategie attuate per contrastare in modo più efficace la criminalità informatica.

1.3. Obiettivi strategici

L'obiettivo generale del regolamento proposto è consentire all'Unione europea, agli Stati membri e alle parti interessate di raggiungere un elevato livello di capacità e preparazione per prevenire, rilevare e reagire in modo più adeguato ai problemi legati alla sicurezza delle reti e dell'informazione. In questo modo si consoliderà la fiducia, che è alla base dello sviluppo della società dell'informazione, aumenterà la competitività delle imprese europee e garantirà il corretto funzionamento del mercato interno.

1.4. Disposizioni vigenti nel settore della proposta

La presente proposta integra le iniziative strategiche, di carattere normativo e non normativo, in materia di sicurezza delle reti e dell'informazione adottate a livello di Unione per potenziare la sicurezza e la resilienza delle TIC:

- il piano d'azione lanciato dalla comunicazione CIIP prevedeva l'istituzione di:

    (1) un forum europeo degli Stati membri (EFMS) destinato a favorire la discussione e lo scambio di informazioni relative alle buone pratiche per condividere obiettivi e priorità strategiche in relazione alla sicurezza e alla resilienza delle infrastrutture TIC, traendo diretto vantaggio dall'attività dell'Agenzia e dal sostegno che essa è in grado di fornire;

    (2) un partenariato pubblico-privato europeo per la resilienza (EP3R), il quadro europeo flessibile per la gestione della resilienza delle infrastrutture TIC, il cui compito è favorire la cooperazione tra il settore privato e quello pubblico per raggiungere obiettivi legati alla sicurezza e alla resilienza, esigenze di base e buone pratiche e misure in materia.

- Il programma di Stoccolma, adottato dal Consiglio europeo l'11 dicembre 2009, promuove strategie per garantire la sicurezza delle reti e consentire di reagire più rapidamente in caso di attacchi informatici nell'Unione.

- Grazie a queste iniziative l'Agenda digitale europea si traduce in risultati concreti. Le politiche in materia di sicurezza delle reti e dell'informazione svolgono un ruolo chiave nella parte della strategia volta a stimolare la fiducia e la sicurezza nella società dell'informazione. Esse sostengono inoltre le misure e le strategie adottate dalla Commissione a tutela della riservatezza (in particolare il concetto di "privacy by design", ossia fin dalla progettazione) e dei dati personali (riesame del quadro), la rete di cooperazione per la tutela dei consumatori, la gestione dell'identità e il programma per l'uso sicuro di Internet.

1.5. Evoluzione dell'attuale strategia in materia di sicurezza delle reti e dell'informazione in relazione alla proposta

Diversi sviluppi attuali della strategia sulla sicurezza, in particolare quelli annunciati nell'Agenda digitale, si basano sul sostegno e le competenze forniti dall'ENISA. Tra questi si annoverano:

- Rafforzare la cooperazione strategica in questo settore intensificando le attività nell'ambito del **forum europeo degli Stati membri (EFMS)** che, con il sostegno diretto dell'ENISA, contribuirà a:

  – stabilire le modalità per istituire una rete europea efficace basata sulla cooperazione transfrontaliera tra squadre di pronto intervento informatico (CERT) nazionali/governative;

  – individuare gli obiettivi e le priorità a lungo termine per esercitazioni paneuropee su larga scala relative agli incidenti legati alla sicurezza delle reti e dell'informazione;

  – ricorrere a requisiti minimi negli appalti pubblici per favorire la sicurezza e la resilienza in reti e sistemi pubblici;

  – individuare incentivi economici e normativi a favore della sicurezza e della resilienza;

  – valutare lo "stato di salute" della sicurezza delle reti e dell'informazione in Europa.

- Rafforzare la cooperazione e i partenariati tra il settore pubblico e quello privato, sostenendo il **partenariato pubblico-privato europeo per la resilienza (EP3R)**. L'ENISA svolge un ruolo sempre più importante come facilitatore degli incontri e delle attività dell'EP3R. Rientrano tra le prossime azioni dell'EP3R:

  – discussioni su provvedimenti e strumenti innovativi per aumentare la sicurezza e la resilienza, come:

  (1) prescrizioni di base in materia di sicurezza e resilienza, in particolare per gli appalti pubblici relativi a prodotti o servizi TIC, per garantire condizioni concorrenziali omogenee assicurando nel contempo adeguata preparazione e prevenzione;

  (2) esaminare questioni inerenti la responsabilità degli operatori economici, ad esempio quando applicano requisiti di sicurezza minimi;

  (3) incentivi di natura economica per lo sviluppo e la diffusione di pratiche per la gestione dei rischi e di processi e prodotti in materia di sicurezza;

  (4) sistemi di valutazione e gestione dei rischi per valutare e gestire gli incidenti gravi secondo parametri comuni;

  (5) cooperazione tra il settore pubblico e quello privato in caso di incidenti su larga scala;

(6) organizzazione di un **vertice sui fattori economici** che ostacolano e quelli che favoriscono la sicurezza e la resilienza.

- Mettere in atto i requisiti di sicurezza del pacchetto normativo sulle comunicazioni elettroniche, per cui occorrono la competenza e l'assistenza dell'ENISA:

  – per sostenere gli Stati membri e la Commissione, tenendo conto, se del caso, dei pareri espressi dal settore privato, nella definizione di un quadro di norme e procedure atte ad attuare le disposizioni in materia di notifica delle violazioni della sicurezza (di cui all'articolo 13 *bis* della direttiva quadro rivista).

  – istituire un forum annuale nel quale gli enti nazionali competenti o le autorità nazionali di regolamentazione e le parti interessate del settore privato possano discutere gli insegnamenti tratti e scambiare buone pratiche sull'applicazione di misure legislative relative alla sicurezza delle reti e dell'informazione.

- Facilitare **esercitazioni di preparazione alla ciber-sicurezza su scala UE** con il sostegno della Commissione e il contributo dell'ENISA, in vista dell'estensione di tali esercitazioni, in un secondo momento, a livello mondiale.

- **Creare una CERT per le istituzioni europee**. L'azione fondamentale n. 6 dell'Agenda digitale prevede che la Commissione presenti "misure volte a raggiungere una politica rafforzata e di alto livello in materia di sicurezza delle reti e dell'informazione, che comprenda […] misure che permettano di rispondere più rapidamente ai cyber-attacchi, compresa una CERT per le istituzioni dell'UE"[8]. Per raggiungere questo obiettivo, la Commissione e le altre istituzioni europee dovranno svolgere delle analisi e istituire una squadra di pronto intervento informatico alla quale l'ENISA può fornire supporto tecnico e competenze.

- Mobilitare gli Stati membri e sostenerli nel completamento e, se necessario, nella creazione di **CERT nazionali/governativi per istituire una rete efficace di CERT che copra tutta l'Europa.** Questa attività sarà utile anche per la messa a punto di un Sistema europeo di condivisione delle informazioni e di allarme (EISAS) per i cittadini e le PMI, che dovrà essere istituito sfruttando risorse e capacità nazionali entro la fine del 2012.

- **Sensibilizzare il pubblico** per quanto riguarda le difficoltà inerenti la sicurezza delle reti e dell'informazione:

  – la Commissione collaborerà con l'ENISA per fornire orientamenti per la promozione delle norme, delle buone pratiche e una cultura della gestione dei rischi. Sarà elaborata una prima serie di indicazioni;

  – l'ENISA organizza, in collaborazione con gli Stati membri, il "**mese europeo per la sicurezza delle reti e dell'informazione per tutti**", nell'ambito del quale saranno organizzati concorsi a livello nazionale ed europeo aventi per oggetto la sicurezza informatica.

---

[8] Nella risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione si afferma anche che: *"Il Consiglio […] riconosce […] che è importante esaminare gli effetti, i rischi e le prospettive strategici ai fini della creazione dei CERT per le istituzioni dell'UE e prendere in considerazione l'eventuale ruolo futuro dell'ENISA in tale settore".*

1.6. Coerenza con altri obiettivi e politiche dell'Unione

La proposta è coerente con le strategie e gli obiettivi dell'Unione europea ed è pienamente conforme all'obiettivo di contribuire al corretto funzionamento del mercato interno potenziando la capacità di preparazione e di reazione di fronte alle difficoltà inerenti la sicurezza delle reti e dell'informazione.

2. RISULTATI DELLE CONSULTAZIONI E DELLE VALUTAZIONI DI IMPATTO

2.1. Consultazione delle parti interessate

La presente iniziativa è il frutto di un ampio dibattito, svoltosi secondo un approccio inclusivo e nel rispetto dei principi di partecipazione, apertura, responsabilità, efficacia e coerenza. Nel quadro di questo ampio processo è stata condotta una valutazione dell'Agenzia (2006/2007), seguita da raccomandazioni del consiglio di amministrazione dell'ENISA, da due consultazioni pubbliche (nel 2007 e nel 2008-2009) e da una serie di seminari in materia.

La prima consultazione pubblica, svoltasi dal 13 giugno al 7 settembre 2007 e avviata parallelamente alla comunicazione della Commissione sulla valutazione intermedia dell'ENISA, era incentrata sul futuro dell'Agenzia ed ha raccolto complessivamente 44 contributi inviati online e due trasmessi per iscritto. Sono intervenute molteplici parti interessate, tra cui ministeri degli Stati membri, enti normativi, associazioni di categoria e per la difesa dei consumatori, organi accademici, aziende e singoli cittadini.

Le risposte hanno messo in evidenza diversi aspetti interessanti relativi all'evoluzione dei tipi di minacce, la necessità di apportare, tramite il regolamento, maggiore chiarezza e flessibilità al funzionamento dell'ENISA affinché questa possa adattarsi meglio alle sfide, l'importanza di assicurare un'interazione efficace con le parti interessate e la possibilità di aumentarne limitatamente le risorse.

La seconda consultazione pubblica, svoltasi dal 7 novembre 2008 al 9 gennaio 2009, era intesa a individuare gli obiettivi prioritari per rafforzare la politica in materia di sicurezza delle reti e dell'informazione a livello di UE e stabilire le modalità per raggiungere tali obiettivi. Sono pervenuti quasi 600 contributi, da autorità degli Stati membri, organi accademici/enti di ricerca, associazioni di categoria, aziende private e altre parti interessate (ad esempio organizzazioni e società di consulenza che si occupano di protezione dei dati e privati cittadini).

La vasta maggioranza dei contributi[9] era a sostegno dell'estensione del mandato dell'Agenzia e chiedeva un ruolo più ampio per quanto riguarda il coordinamento delle attività inerenti la sicurezza a livello europeo, nonché un aumento delle risorse destinate all'Agenzia. Sono state indicate come priorità la necessità di un approccio più coordinato alle minacce informatiche in tutta Europa, una cooperazione transnazionale per fare fronte agli attacchi informatici su larga scala, il rafforzamento della fiducia e un migliore scambio di informazioni tra le parti interessate.

Sulla base di uno studio preparatorio condotto da un contraente esterno, a settembre 2009 ha avuto inizio la valutazione di impatto della proposta. È stata coinvolta una vasta gamma di

[9] Allegato XII della valutazione dell'impatto.

parti interessate e di esperti, tra cui enti degli Stati membri che si occupano di sicurezza delle reti e dell'informazione, autorità nazionali di regolamentazione, operatori delle telecomunicazioni, fornitori di servizi internet e relative associazioni del settore, associazioni per la tutela dei consumatori, produttori di TIC, CERT, esponenti del mondo accademico e utenti professionali. È stato istituito un gruppo direttivo interservizi fra le direzioni generali competenti della Commissione per sostenere il processo di valutazione d'impatto.

2.2. Valutazione dell'impatto

Mantenere l'Agenzia è stata individuata come soluzione appropriata per raggiungere gli obiettivi strategici in materia[10]. Al termine di un primo esame, sono state selezionate cinque opzioni da sottoporre ad ulteriore analisi:

- Opzione 1 – Nessuna politica;
- Opzione 2 – Status quo (mantenere un mandato simile e lo stesso livello di risorse);
- Opzione 3 - Ampliare i compiti dell'ENISA e includere le autorità incaricate del rispetto delle norme e della tutela della privacy come parti interessate a pieno titolo;
- Opzione 4 – Aggiungere ai compiti dell'agenzia la lotta contro gli attacchi informatici e la reazione agli incidenti informatici;
- Opzione 5 - Aggiungere ai compiti dell'agenzia l'assistenza alle autorità incaricate del rispetto delle norme e giudiziarie nella lotta contro la criminalità informatica.

Dopo un'analisi comparativa costi-benefici, l'opzione 3 è stata ritenuta la più efficace per raggiungere gli obiettivi fissati dalla strategia.

L'opzione 3 prevede un ampliamento del ruolo dell'ENISA per:

- creare e mantenere una rete di contatti tra le parti interessate e una rete di conoscenze per assicurare che l'ENISA riceva informazioni esaustive in merito al panorama della sicurezza delle reti e dell'informazione in Europa;
- fungere da centro di supporto per lo sviluppo e l'attuazione delle strategie in materia di sicurezza delle reti e dell'informazione (in particolare per quanto riguarda la privacy online, la firma elettronica, l'identificazione elettronica e le norme sugli appalti pubblici relative alla sicurezza);
- sostenere la politica dell'Unione in materia di infrastrutture critiche informatizzate e resilienza (ad es. esercitazioni, l'EP3R, il sistema europeo di condivisione delle informazioni e di allarme, ecc.);
- creare un quadro a livello di UE per la raccolta di dati relativi alla sicurezza delle reti e dell'informazione, anche mettendo a punto metodi e pratiche per la notifica legale e la condivisione di tali dati;
- studiare l'economia della sicurezza delle reti e dell'informazione;

[10] Allegato IV della valutazione dell'impatto.

- favorire la cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere un approccio comune globale alla sicurezza delle reti e dell'informazione e avere un impatto sulle iniziative internazionali di alto livello in Europa;
- svolgere compiti non operativi legati agli aspetti inerenti la sicurezza delle reti e dell'informazione nell'ambito dell'applicazione della legge e della cooperazione giudiziaria in materia di criminalità informatica.

3. ELEMENTI GIURIDICI DELLA PROPOSTA

3.1. Sintesi delle misure proposte

Il regolamento proposto è inteso a rafforzare e modernizzare l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e a stabilire un nuovo mandato della durata di 5 anni.

La proposta comprende alcuni cambiamenti cruciali rispetto al regolamento originario:

(1) **Maggiore flessibilità, adattabilità e capacità di concentrare gli sforzi.** I compiti dell'Agenzia sono stati ampiamente aggiornati e riformulati per ampliarne l'ambito di intervento; i compiti sono stabiliti in maniera sufficientemente precisa da definire gli obiettivi da raggiungere. Ciò permette di inquadrare meglio la missione dell'Agenzia, ne aumenta la capacità di raggiungere gli obiettivi fissati e ne consolida il ruolo di sostegno all'attuazione delle politiche dell'Unione.

(2) **Migliore allineamento dell'Agenzia al processo politico e normativo dell'Unione**. Le istituzioni e gli organismi dell'UE possono rivolgersi all'Agenzia per ottenere assistenza e consulenze, conformemente agli sviluppi in ambito strategico e normativo: il Consiglio ha cominciato a rivolgersi direttamente all'Agenzia nelle sue risoluzioni e il Parlamento europeo e il Consiglio hanno assegnato all'Agenzia dei compiti relativi alla sicurezza delle reti e dell'informazione nell'ambito del quadro normativo sulle comunicazioni elettroniche.

(3) **Interfaccia con la lotta contro la criminalità informatica**. Per raggiungere questi obiettivi, l'Agenzia tiene conto della lotta contro la criminalità informatica. Le autorità incaricate del rispetto delle norme e quelle preposte alla tutela della privacy sono diventate parti in causa a pieno titolo dell'Agenzia, in particolare nel gruppo permanente di parti interessate.

(4) **Rafforzamento della struttura di governance**. La proposta rafforza il ruolo di supervisione del consiglio di amministrazione dell'Agenzia, nel quale sono rappresentati gli Stati membri e la Commissione. Ad esempio, il consiglio di amministrazione può fornire indicazioni generali su questioni riguardanti il personale, compito che era in precedenza di sola responsabilità del direttore esecutivo. Può inoltre istituire organismi di lavoro che lo assistano nello svolgimento delle sue funzioni, compreso il monitoraggio dell'attuazione delle sue decisioni.

(5) **Razionalizzazione delle procedure**. Le procedure che sono risultate inutilmente gravose sono state semplificate. Ad esempio è stata semplificata la procedura relativa alle norme interne del consiglio di amministrazione e il parere sul programma di lavoro dell'ENISA è fornita dai servizi della Commissione e non più tramite l'adozione di una decisione della Commissione. Al consiglio di amministrazione sono inoltre

assegnate risorse adeguate qualora sia necessario prendere decisioni esecutive e applicarle (ad esempio se un membro del personale presenta una denuncia contro il direttore esecutivo o il consiglio di amministrazione stesso).

(6) **Graduale aumento delle risorse**. Per rispettare le priorità rafforzate dell'Unione e le sfide sempre più vaste, e nel rispetto della proposta della Commissione per il prossimo quadro finanziario pluriennale, è stato previsto un graduale aumento delle risorse umane e finanziarie assegnate all'Agenzia tra il 2012 e il 2016. Sulla base della proposta del regolamento della Commissione che fissa il quadro finanziario pluriennale dopo il 2013 e tenendo conto delle conclusioni della valutazione di impatto, la Commissione presenterà una scheda finanziaria legislativa modificata.

(7) **Possibilità di estendere il mandato del direttore esecutivo**. Il consiglio di amministrazione può estendere di tre anni il mandato del direttore esecutivo.

3.2. Base giuridica

La base giuridica della proposta è l'articolo 114 del trattato sul funzionamento dell'Unione europea[11] (TFUE).

In conformità alla giurisprudenza della Corte di giustizia europea[12], prima dell'entrata in vigore del trattato di Lisbona, l'**articolo 95 del trattato CE** doveva essere considerato la base giuridica appropriata per la creazione di un organismo volto a garantire un elevato ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione. Con l'espressione "misure di ravvicinamento" nell'articolo 95, gli autori del trattato intendevano conferire al legislatore europeo la discrezione di scegliere le misure più adeguate per raggiungere il risultato desiderato. Aumentare la sicurezza e la resilienza delle infrastrutture TIC è pertanto un elemento importante per contribuire al corretto funzionamento del mercato interno.

Ai sensi del trattato di Lisbona, l'**articolo 114 del TFUE**[13] descrive in modo quasi identico la responsabilità relativa al mercato interno. Per le ragioni di cui sopra, tale articolo continuerà ad essere la base giuridica applicabile per l'adozione di misure volte a migliorare la sicurezza delle reti e dell'informazione. La responsabilità del mercato interno è ora una competenza condivisa dall'Unione e dagli Stati membri (articolo 4, paragrafo 2, lettera a), del TFUE). Questo significa che l'Unione e gli Stati membri possono adottare misure (vincolanti) e che gli Stati membri agiranno nella misura in cui l'Unione non ha esercitato la propria competenza o ha deciso di cessare di esercitarla (articolo 2, paragrafo 2, del TFUE).

Le misure relative alla responsabilità del mercato interno richiederanno la procedura legislativa ordinaria (articolo 289 e 294 del TFUE), simile[14] alla precedente procedura di codecisione (articoli 251 del trattato CE).

Con il trattato di Lisbona è venuta meno la distinzione tra pilastri e la prevenzione e la lotta contro il crimine sono diventate competenze condivise dell'Unione. Per questo motivo l'ENISA ha la possibilità di svolgere il ruolo di piattaforma per gli aspetti della lotta alla

---

11 GU C 115 del 9.5.2008, pag. 94.

12 CGUE 2.5.2006, C-217/04, Regno Unito di Gran Bretagna e Irlanda del Nord contro Parlamento europeo e Consiglio dell'Unione europea.

13 Vedi sopra.

14 La procedura legislativa ordinaria differisce in particolare in termini di requisiti di maggioranza in seno al Consiglio e al Parlamento europeo.

criminalità informatica legati alla sicurezza delle reti e dell'informazione e di condividere opinioni e buone pratiche con le autorità responsabili della difesa dagli attacchi informatici, dell'applicazione delle norme e della tutela della vita privata.

3.3. Principio di sussidiarietà

La proposta è conforme al principio di sussidiarietà: la politica in materia di sicurezza delle reti e dell'informazione richiede un approccio collaborativo e gli obiettivi della proposta non possono essere raggiunti dagli Stati membri individualmente.

Se l'Unione si astenesse da qualsiasi intervento nelle politiche nazionali in materia di sicurezza delle reti e dell'informazione, gli Stati membri sarebbero i soli responsabili delle azioni in questo ambito, nonostante l'evidente interdipendenza dei sistemi informatici esistenti. Una misura che garantisca un'adeguata coordinazione tra gli Stati membri, volta a garantire che i rischi legati alla sicurezza possano essere affrontati in maniera adeguata nel contesto transfrontaliero in cui si presentano, è perciò conforme al principio di sussidiarietà. Inoltre, l'azione dell'UE aumenterebbe l'efficacia delle politiche nazionali esistenti e apporterebbe quindi un valore aggiunto.

Infine, un'azione strategica coordinata e collaborativa nell'ambito della sicurezza delle reti e dell'informazione avrà ripercussioni positive ai fini della tutela dei diritti fondamentali, in particolare il diritto alla protezione dei dati personali e della privacy. La necessità di proteggere i dati è cruciale nel contesto attuale perché i cittadini dell'Unione affidano sempre di più i propri dati a sistemi informatici complessi, per scelta o per necessità, senza necessariamente essere in grado di valutare correttamente i rischi legati alla loro protezione. Quando si verificano incidenti i cittadini potrebbero non essere in grado di adottare le misure necessarie e non è detto che gli Stati membri possano affrontare in modo efficace eventuali incidenti di portata internazionale in assenza di una coordinazione a livello europeo della sicurezza delle reti e dell'informazione.

3.4. Principio di proporzionalità

La proposta è conforme al principio di proporzionalità poiché non va al di là di quanto necessario per il raggiungimento degli obiettivi fissati.

3.5. Scelta dello strumento

Strumento proposto: un regolamento direttamente applicabile in ogni Stato membro.

4. INCIDENZA SUL BILANCIO

La proposta ha un'incidenza sul bilancio dell'Unione.

Poiché vengono stabiliti i compiti da includere nel nuovo mandato dell'ENISA, è previsto che l'Agenzia disponga delle risorse necessarie per compiere le proprie attività in modo soddisfacente. La valutazione dell'Agenzia, l'ampio processo di consultazione delle parti interessate a tutti i livelli e la valutazione di impatto evidenziano un generale accordo sul fatto che le dimensioni dell'Agenzia sono al disotto della sua massa critica e che si rende necessario un aumento delle risorse. Le conseguenze e gli effetti di un aumento del personale e del bilancio a disposizione dell'Agenzia sono analizzati nella valutazione di impatto allegata alla proposta.

Il finanziamento dell'UE dopo il 2013 sarà esaminato nell'ambito di un dibattito che coinvolgerà tutta la Commissione e verterà sulle proposte relative al periodo post-2013.

5. INDICAZIONI SUPPLEMENTARI

5.1. Durata

Il regolamento copre un periodo di cinque anni.

5.2. Clausola di riesame

Il regolamento prevede una valutazione dell'Agenzia per il periodo trascorso dalla precedente valutazione (2007). Sarà valutata l'efficacia nel conseguimento degli obiettivi stabiliti dal regolamento per determinare se l'Agenzia continua ad essere uno strumento efficace e la necessità di estenderne ulteriormente la durata. In base a quanto accertato, il consiglio di amministrazione presenterà alla Commissione delle raccomandazioni in merito alle possibili modifiche da apportare al presente regolamento, all'Agenzia e ai suoi metodi di lavoro. Per consentire alla Commissione di presentare in tempo utile eventuali proposte per un'estensione del mandato, la valutazione dovrà essere completata entro la fine del secondo anno del mandato previsto dal regolamento.

5.3. Misure provvisorie

La Commissione è consapevole che al Parlamento europeo e al Consiglio i dibattimenti per l'approvazione della proposta potrebbero allungare notevolmente la procedura legislativa, con il rischio che si crei un vuoto legislativo qualora il nuovo mandato dell'Agenzia non fosse adottato prima della scadenza del mandato attuale. La Commissione propone quindi, insieme al presente regolamento, un regolamento che prolunga il mandato attuale dell'Agenzia per 18 mesi per lasciare tempo sufficiente alle discussioni e alle necessarie procedure.

2010/0275 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

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,

visto il parere del Comitato economico e sociale europeo[15],

visto il parere del Comitato delle regioni[16],

previa trasmissione della proposta ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Le comunicazioni elettroniche e i relativi servizi e infrastrutture sono ormai fattori determinanti dello sviluppo economico e sociale. Svolgono un ruolo vitale per la società e sono diventati strumenti altrettanto comuni dell'acqua corrente o dell'energia elettrica. Il loro malfunzionamento può causare danni economici ingenti e questo sottolinea l'importanza di adottare provvedimenti volti ad aumentare la protezione e la resilienza per garantire la continuità dei servizi critici. La sicurezza delle comunicazioni, delle infrastrutture e dei servizi elettronici, in particolare la loro integrità e disponibilità, è posta di fronte a difficoltà sempre maggiori. Si tratta di questioni di rilevanza sempre maggiore per la società, anche perché la complessità del sistema e i possibili incidenti, errori e attacchi possono avere conseguenze gravi sulle infrastrutture fisiche che forniscono servizi essenziali per il benessere dei cittadini dell'UE.

(2) Il panorama delle minacce è in costante cambiamento e gli incidenti legati alla sicurezza possono minare la fiducia degli utenti. Se le interruzioni gravi delle comunicazioni elettroniche e dei relativi servizi e infrastrutture possono avere un notevole impatto sull'economia e la società, anche le violazioni quotidiane alla sicurezza e i problemi e gli inconvenienti che ne derivano possono minare la fiducia dei cittadini nella tecnologia, nelle reti e nei servizi elettronici.

---

15 GU C […] del […], pag. […].
16 GU C […] del […], pag. […].

(3) La valutazione periodica dello stato della sicurezza delle reti e dell'informazione in Europa, basata su dati affidabili a livello europeo, è quindi importante per i responsabili delle politiche, il settore e gli utenti.

(4) I rappresentanti degli Stati membri, riuniti nel Consiglio europeo del 13 dicembre 2003, hanno deciso che l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), istituita sulla base della proposta presentata dalla Commissione, avrebbe avuto sede in Grecia, nella località che sarebbe stata decisa dal governo greco.

(5) Nel 2004 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 460/2004[17] che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione al fine di contribuire ad assicurare un elevato ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore. Nel 2008 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 1007/2008[18] che proroga il mandato dell'Agenzia fino a marzo 2012.

(6) Dalla creazione dell'Agenzia, le sfide legate alla sicurezza delle reti e dell'informazione sono cambiate con l'evolvere della tecnologia, del mercato e del panorama socioeconomico e sono state al centro di ulteriori riflessioni e dibattiti. In risposta all'evolvere delle difficoltà, l'Unione ha aggiornato le priorità della strategia in materia di sicurezza delle reti e dell'informazione in diversi documenti, tra i quali la comunicazione della Commissione "Una strategia per una società dell'informazione sicura – Dialogo, partenariato e responsabilizzazione"[19] (2006), la risoluzione del Consiglio su una strategia per una società dell'informazione sicura in Europa[20] (2007), la comunicazione "Proteggere le infrastrutture critiche informatizzate - Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni"[21](2009), le conclusioni della presidenza alla conferenza ministeriale dell'UE sulla protezione delle infrastrutture critiche informatizzate (CIIP) e la risoluzione del Consiglio su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (2009).[22]. È stata riconosciuta la necessità di modernizzare e rafforzare l'Agenzia, affinché contribuisca all'impegno delle istituzioni europee e degli Stati membri per sviluppare la capacità europea di affrontare le sfide legate alla sicurezza delle reti e dell'informazione. Recentemente la Commissione ha adottato l'Agenda digitale europea[23], un'iniziativa faro nell'ambito della strategia "Europa 2020". Questo vasto programma intende sfruttare e sviluppare il potenziale delle TIC per tradurlo in crescita sostenibile e innovazione. Stimolare la fiducia nella società dell'informazione è uno degli obiettivi centrali dell'Agenda digitale, che prevede l'intervento della Commissione con diverse azioni in questo settore, tra cui anche la presente proposta.

---

17 GU L 77 del 13.3.2004, pag. 1.
18 GU L 293 del 31.10.2008, pag. 1.
19 COM(2006) 251 del 31.5.2006.
20 Risoluzione del Consiglio del 22 marzo 2007 su una strategia per una società dell'informazione sicura in Europa (GU C 68 del 24.3.2007, pag. 1).
21 COM(2009) 149 del 30.3.2009.
22 Risoluzione del Consiglio, del 18 dicembre 2009, su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione (GU C 321 del 29.12.2009, pag. 1).
23 COM (2010) 245 del 19.5.2010.

(7) Nel campo della sicurezza delle comunicazioni elettroniche e, più in generale, della sicurezza delle reti e dell'informazione, le misure relative al mercato interno presuppongono l'adozione di diverse soluzioni tecniche e organizzative da parte degli Stati membri e della Commissione. L'applicazione eterogenea di tali requisiti può portare a soluzioni inefficaci e creare ostacoli al mercato interno. Da ciò sorge la necessità di istituire un centro di competenze a livello europeo che fornisca orientamenti, consulenze e, se richiesto, assistenza in materia di sicurezza delle reti e dell'informazione, al quale possano rivolgersi gli Stati membri e le istituzioni europee. L'Agenzia può rispondere a queste esigenze creando e mantenendo un elevato livello di esperienza e assistendo gli Stati membri e la Commissione, e di conseguenza collaborando con la comunità degli operatori economici, al fine di aiutarli a soddisfare le prescrizioni giuridiche e normative in materia di sicurezza delle reti e dell'informazione, contribuendo in tal modo al corretto funzionamento del mercato interno.

(8) L'Agenzia dovrebbe svolgere i compiti che le sono conferiti dalla vigente legislazione dell'Unione nel settore delle comunicazioni elettroniche e contribuire, più in generale, ad aumentare il livello di sicurezza delle comunicazioni elettroniche anche fornendo competenze e assistenza e promuovendo lo scambio di buone pratiche.

(9) La 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)[24] impone inoltre ai fornitori delle reti pubbliche di comunicazioni elettroniche e dei servizi di comunicazione elettronica accessibili al pubblico di prendere i provvedimenti adeguati a proteggere la loro integrità e sicurezza e introdurre requisiti in materia di notifica delle violazioni della sicurezza e di perdita di integrità. Se del caso, le autorità nazionali di regolamentazione devono inoltre notificare all'Agenzia e trasmettere alla Commissione e all'Agenzia una relazione sintetica annuale sulle notifiche ricevute e le azioni intraprese. La direttiva 2002/21/CE prevede inoltre che l'Agenzia contribuisca ad armonizzare le misure di sicurezza tecniche ed organizzative appropriate, offrendo la sua consulenza.

(10) 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)[25] stabilisce che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi e impone inoltre la riservatezza delle comunicazioni nonché dei relativi dati sul traffico. La direttiva 2002/58/CE introduce requisiti in materia di informazione e notifica delle violazioni dei dati personali cui devono attenersi i fornitori di servizi di comunicazioni elettroniche. La direttiva prevede inoltre che la Commissione consulti l'Agenzia per qualsiasi misura tecnica di attuazione che deve essere adottata relativamente alle circostanze o al formato delle prescrizioni in materia di informazione e notifica e le relative procedure applicabili. La 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,

---

[24] GU L 108 del 24.4.2002, pag. 33.
[25] GU L 201 del 31.7.2002, pag. 37.

nonché alla libera circolazione di tali dati[26] fa obbligo agli Stati membri di disporre che il responsabile del trattamento attui misure tecniche e organizzative appropriate per proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta la trasmissione di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

(11) Occorre che l'Agenzia contribuisca ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nell'Unione e a sviluppare una cultura in materia a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al corretto funzionamento del mercato interno.

(12) È opportuno stabilire una serie di compiti che definiscano in che modo l'Agenzia deve raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione. Occorre che tra i compiti dell'Agenzia rientri la raccolta di informazioni e dati che consentano di svolgere analisi dei rischi in materia di sicurezza e resilienza delle comunicazioni elettroniche e dei relativi servizi e infrastrutture e di valutare, in cooperazione con gli Stati membri, lo stato della sicurezza delle reti e dell'informazione in Europa. Occorre che l'Agenzia assicuri il coordinamento con gli Stati membri e rafforzi la cooperazione tra le parti interessate in Europa, in particolare facendo partecipare alle proprie attività gli organismi nazionali competenti e gli esperti del settore privato nel campo della sicurezza delle reti e dell'informazione. L'Agenzia dovrebbe fornire assistenza alla Commissione e agli Stati membri nel loro dialogo con l'industria, per affrontare i problemi inerenti la sicurezza nei prodotti hardware e software, contribuendo così ad attuare un approccio collaborativo alla sicurezza delle reti e dell'informazione.

(13) È opportuno che l'Agenzia operi come punto di riferimento e si assicuri la fiducia degli interessati grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni diffuse, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei compiti che le sono assegnati. L'Agenzia dovrebbe basarsi sugli sforzi prodotti a livello nazionale e di Unione e svolgere pertanto i propri compiti in piena collaborazione con gli Stati membri mantenendo contatti con il settore e altri soggetti interessati. È opportuno inoltre che l'Agenzia si avvalga dei contributi derivanti dalla cooperazione con il settore privato, che svolge un ruolo importante nel garantire la sicurezza delle comunicazioni elettroniche e dei relativi servizi e infrastrutture.

(14) La Commissione ha lanciato un partenariato pubblico-privato europeo per la resilienza, che costituisce un quadro flessibile di gestione della resilienza delle infrastrutture TIC in tutta Europa. È necessario che l'Agenzia svolga un ruolo di facilitatore nell'ambito del partenariato, riunendo parti interessate del settore privato e di quello pubblico per discutere le priorità della strategia pubblica, le dimensioni economiche e commerciali delle problematiche e delle misure a favore della resilienza delle infrastrutture TIC e per individuare le responsabilità delle parti interessate.

---

[26] GU L 281 del 23.11.1995, pag. 31.

(15) Occorre che l'Agenzia, di propria iniziativa o su richiesta della Commissione, fornisca consulenze alla Commissione tramite pareri e analisi tecniche e socioeconomiche per assisterla nell'elaborazione di politiche nel settore della sicurezza delle reti e dell'informazione. L'Agenzia dovrebbe inoltre assistere, su loro richiesta, gli Stati membri e le istituzioni e gli organismi europei nel loro impegno a mettere a punto strategie e capacità nel campo della sicurezza.

(16) È opportuno che l'Agenzia assista gli Stati membri e le istituzioni europee nel loro impegno a costruire e consolidare la capacità e la preparazione transfrontaliere per prevenire, rilevare, mitigare e reagire ai problemi e agli incidenti legati alla sicurezza delle reti e dell'informazione; in questo ambito, l'Agenzia dovrebbe facilitare la cooperazione tra gli Stati membri e tra questi e la Commissione. A tale scopo, l'Agenzia dovrebbe sostenere attivamente gli Stati membri nel loro impegno costante a migliorare la capacità di reazione nonché organizzare e realizzare esercitazioni a livello nazionale ed europeo relative alla sicurezza.

(17) La direttiva 95/46/CE disciplina il trattamento dei dati personali effettuato ai sensi del presente regolamento.

(18) Per meglio comprendere le difficoltà del settore della sicurezza delle reti e dell'informazione, l'Agenzia deve analizzare i rischi attuali e quelli emergenti. A tale scopo, è opportuno che raccolga le informazioni pertinenti, in cooperazione con gli Stati membri e, se del caso, con istituti di statistica. L'Agenzia dovrebbe inoltre assistere gli Stati membri e le istituzioni e gli organi europei nel loro impegno a raccogliere, analizzare e diffondere i dati relativi alla sicurezza delle reti e dell'informazione.

(19) Nello svolgimento delle attività di monitoraggio nell'Unione, occorre che l'Agenzia agevoli la cooperazione tra l'Unione e gli Stati membri nella valutazione dello stato della sicurezza in Europa e contribuisca alle valutazioni in cooperazione con gli Stati membri.

(20) È necessario che l'Agenzia faciliti la cooperazione tra gli enti pubblici competenti degli Stati membri, in particolare sostenendo la messa a punto e lo scambio di buone pratiche e di standard in materia di programmi educativi e di strategie per la sensibilizzazione. Uno scambio più intenso di informazioni tra gli Stati membri favorirà queste azioni. L'Agenzia dovrebbe inoltre sostenere la cooperazione tra le parti interessate del settore pubblico e di quello privato a livello di Unione, in parte promuovendo la condivisione di informazioni, campagne di sensibilizzazione e programmi di istruzione e formazione.

(21) Strategie efficaci in materia di sicurezza dovrebbero basarsi su metodi validi di valutazione dei rischi, sia nel settore pubblico che in quello privato. Sono utilizzati metodi e procedure a diversi livelli, senza una prassi comune per un'applicazione efficace. La promozione e lo sviluppo delle migliori pratiche per la valutazione dei rischi e per soluzioni interoperabili per la loro gestione all'interno delle organizzazioni del settore pubblico e privato aumenteranno il livello di sicurezza delle reti e dei sistemi di informazione in Europa. A tale scopo, l'Agenzia dovrebbe sostenere la cooperazione tra le parti interessate pubbliche e private a livello di Unione, facilitando il loro impegno nella definizione e nella diffusione di standard in materia di gestione dei rischi e di sicurezza misurabile di prodotti, sistemi, reti e servizi elettronici.

(22) È opportuno che nell'assolvimento dei propri compiti l'Agenzia si avvalga delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione.

(23) Ove indicato e utile per il conseguimento delle proprie finalità, obiettivi e compiti, è opportuno che l'Agenzia condivida esperienze e informazioni generali con gli organismi e le agenzie istituiti ai sensi del diritto dell'Unione europea che si occupano della sicurezza delle reti e dell'informazione.

(24) Nelle relazioni con gli organismi preposti all'applicazione delle norme in relazione agli aspetti della criminalità informatica inerenti la sicurezza, l'Agenzia si avvale dei canali di informazione e delle reti esistenti, come i punti di contatto indicati nella proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi informatici, che abroga la decisione quadro 2005/222/JHA o la task-force di Europol composta dai capi delle unità specializzate nella lotta alla criminalità ad alta tecnologia.

(25) Per conseguire appieno i propri obiettivi occorre che l'Agenzia instauri dei rapporti con gli organismi incaricati del rispetto delle norme e quelli preposti alla tutela della vita privata per mettere in rilievo e affrontare in maniera adeguata gli aspetti della sicurezza delle reti e dell'informazione nella lotta contro la criminalità informatica. I rappresentanti di queste autorità dovrebbero diventare parti in causa a pieno titolo dell'Agenzia e dovrebbero essere rappresentate nel gruppo permanente di parti interessate dell'Agenzia.

(26) I problemi di sicurezza delle reti e dell'informazione sono questioni globali. È necessaria una più stretta cooperazione internazionale per migliorare gli standard di sicurezza e lo scambio di informazioni e per promuovere un approccio comune globale alle questioni inerenti la sicurezza delle reti e dell'informazione. A questo scopo l'Agenzia dovrebbe sostenere la cooperazione con i paesi terzi e le organizzazioni internazionali in collaborazione, se del caso, con il Servizio europeo per l'azione esterna (SEAE).

(27) L'assolvimento dei compiti dell'Agenzia non dovrebbe interferire con le competenze né costituire pregiudizio, ostacolo o sovrapposizione alle pertinenti competenze e mansioni assegnate ai seguenti soggetti: le autorità di regolamentazione nazionali, come indicato nelle direttive relative alle reti e ai servizi di comunicazione elettronica; l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC) istituito dal regolamento (CE) n. 1211/2009 del Parlamento europeo e del Consiglio[27]; il Comitato per le comunicazioni di cui alla direttiva 2002/21/CE; gli organismi europei di normalizzazione, gli organismi nazionali di normalizzazione; il comitato permanente di cui alla 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 regole relative ai servizi della società dell'informazione[28]; le autorità di controllo degli Stati membri che si occupano della alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

---

27 GU L 337 del 18.12.2009, pag. 1.

28 GU L 204 del 21.7.1998, pag. 37.

(28) Per assicurare che l'Agenzia sia efficace, è opportuno che gli Stati membri e la Commissione siano rappresentati in seno al consiglio di amministrazione, che dovrebbe definire l'orientamento generale delle azioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe essere dotato dei necessari poteri di stabilire il bilancio, verificarne l'esecuzione, adottare le regole finanziarie necessarie, istituire procedure di lavoro trasparenti per l'adozione delle decisioni dell'Agenzia, approvarne il programma di lavoro, adottare il proprio regolamento interno e quello dell'Agenzia, nonché nominare e decidere in merito all'estensione o alla conclusione del mandato del direttore esecutivo. Il consiglio di amministrazione dovrebbe poter istituire organismi di lavoro che lo assistano nello svolgimento delle sue funzioni, ad esempio redigendo le bozze delle decisioni del consiglio di amministrazione o monitorandone l'attuazione.

(29) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale nonché alla competenza e all'esperienza acquisita in materia di sicurezza delle reti e dell'informazione e svolga le proprie funzioni relativamente all'organizzazione e al funzionamento interno dell'Agenzia in completa indipendenza. A tal fine e previa consultazione dei servizi della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le azioni necessarie per garantire che il programma venga adeguatamente eseguito. Dovrebbe inoltre predisporre ogni anno un progetto di relazione generale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio.

(30) È opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Nell'istituire i gruppi di lavoro ad hoc, il direttore esecutivo dovrebbe cercare contributi e avvalersi dell'esperienza esterna pertinente necessaria per consentire all'Agenzia di avere accesso alle informazioni più aggiornate per poter rispondere alle sfide nel settore della sicurezza poste dallo sviluppo della società dell'informazione. L'Agenzia dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, il settore privato, le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione. Se necessario, l'Agenzia può invitare a titolo individuale degli esperti di riconosciuta competenza nel campo a partecipare alle attività dei gruppi di lavoro, caso per caso. Le loro spese dovrebbero essere sostenute dall'Agenzia a norma del suo regolamento interno e conformemente al regolamento finanziario vigente.

(31) È opportuno che l'Agenzia disponga di un gruppo permanente di parti interessate come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e le altri parti interessate. Il gruppo permanente di parti interessate, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per tutte le parti interessate e sottoporle all'attenzione dell'Agenzia. Il direttore esecutivo può, ove opportuno e in funzione dell'ordine del giorno delle riunioni, invitare rappresentanti del Parlamento europeo e di altri organi competenti a partecipare alle riunioni del gruppo.

(32) L'Agenzia opera nel rispetto del principio di sussidiarietà, che garantisce un adeguato livello di coordinazione tra gli Stati membri su questioni inerenti la sicurezza delle reti e dell'informazione e che aumenta l'efficacia delle strategie nazionali, alle quali apporta valore aggiunto, e del principio di proporzionalità, non andando oltre quanto necessario a raggiungere gli obiettivi definiti nel presente regolamento.

(33) Occorre che l'Agenzia applichi la legislazione UE pertinente in materia di accesso del pubblico ai documenti quale definita dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[29] e di tutela delle persone fisiche in relazione al trattamento dei dati personali quale definita dal 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[30].

(34) Nell'ambito della sua sfera d'azione e dei suoi obiettivi e nell'assolvimento dei suoi compiti, è opportuno che l'Agenzia si conformi in particolare alle disposizioni applicabili alle istituzioni europee e alla legislazione nazionale in materia di documenti sensibili. Il consiglio di amministrazione dovrebbe avere il potere di prendere una decisione che consenta all'Agenzia di trattare informazioni riservate.

(35) Per garantire all'Agenzia piena autonomia e indipendenza, si ritiene necessario dotarla di un bilancio autonomo le cui entrate siano essenzialmente costituite da contributi dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. Lo Stato membro ospitante, o qualsiasi altro Stato membro, dovrebbe essere autorizzato a contribuire alle entrate dell'Agenzia versando contributi volontari. La procedura di bilancio dell'UE resta tuttavia applicabile a qualsiasi sovvenzione a carico del bilancio generale delle Unione europea. Inoltre, la revisione contabile dovrebbe essere svolta dalla Corte dei conti.

(36) È opportuno che l'Agenzia succeda all'ENISA istituita con il regolamento n. 460/2004. Nel quadro della decisione presa dai rappresentanti degli Stati membri, riuniti in seno al Consiglio europeo del 13 dicembre 2003, lo Stato membro ospitante dovrebbe mantenere e sviluppare le attuali modalità pratiche applicate per garantire un funzionamento corretto ed efficiente dell'Agenzia, in particolare per quanto riguarda la cooperazione dell'Agenzia con la Commissione, gli Stati membri e gli organi nazionali competenti, altre istituzioni e organismi dell'UE, nonché le parti interessate pubbliche e private di tutta Europa e l'assistenza che l'Agenzia fornisce a tutti questi soggetti.

(37) L'Agenzia dovrebbe essere istituita per un periodo limitato. Il suo operato dovrebbe essere valutato in rapporto all'efficacia nel conseguimento degli obiettivi fissati e le sue pratiche di lavoro, per determinare se tali obiettivi continuano ad essere validi e, in base a quanto accertato, per determinare l'eventuale necessità di estendere ulteriormente la durata del suo funzionamento,

---

[29] 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 (GU L 145 del 31.5.2001, pag. 43).

[30] 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 (GU L 8 del 12.1.2001, pag. 1).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

SEZIONE 1 AMBITO D'APPLICAZIONE, OBIETTIVI E COMPITI

Articolo 1
Oggetto e campo di applicazione

1. Il presente regolamento istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (in seguito: "l'Agenzia") al fine di assicurare un elevato ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito dell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al corretto funzionamento del mercato interno.

2. Gli obiettivi e i compiti dell'Agenzia lasciano impregiudicate le competenze degli Stati membri per quanto riguarda la sicurezza delle reti e dell'informazione e comunque le attività nel settore della pubblica sicurezza, della difesa, della sicurezza dello Stato (compreso il benessere economico dello Stato laddove le questioni riguardano problemi attinenti alla sicurezza dello Stato) e le attività dello Stato nell'ambito del diritto penale.

3. Ai fini del presente regolamento, si intende per "*sicurezza delle reti e dell'informazione*" la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei relativi servizi forniti o accessibili tramite tale rete o sistema.

Articolo 2
Obiettivi

1. L'Agenzia assiste la Commissione e gli Stati membri al fine di aiutarli a soddisfare le prescrizioni giuridiche e normative in materia di sicurezza delle reti e dell'informazione previste dalla normativa europea vigente e futura, contribuendo in tal modo al corretto funzionamento del mercato interno.

2. L'Agenzia rafforza la capacità e la preparazione dell'Unione e degli Stati membri per prevenire, rilevare e reagire ai problemi e agli incidenti legati alla sicurezza delle reti e dell'informazione.

3. L'Agenzia sviluppa e mantiene un elevato livello di competenza, che impiega per stimolare un'ampia cooperazione tra attori del settore pubblico e del settore privato.

Articolo 3
Compiti

1. Per raggiungere gli obiettivi di cui all'articolo 1, l'Agenzia svolge i seguenti compiti:

a) assiste la Commissione, su richiesta di questa o di propria iniziativa, nell'elaborazione di politiche in materia di sicurezza delle reti e dell'informazione, fornendole consulenze, pareri e

analisi tecniche e socioeconomiche e svolgendo attività preparatorie all'elaborazione e all'aggiornamento della normativa UE nel settore;

b) facilita la cooperazione tra Stati membri e tra questi e la Commissione nell'impegno a prevenire, rilevare e reagire, a livello transnazionale, agli incidenti legati alla sicurezza delle reti e dell'informazione;

c) assiste gli Stati membri e le istituzioni e gli organi europei nel loro impegno a raccogliere, analizzare e divulgare i dati relativi alla sicurezza delle reti e dell'informazione;

d) valuta periodicamente, in cooperazione con gli Stati membri e le istituzioni europee, lo stato della sicurezza delle reti e dell'informazione in Europa;

e) facilita la cooperazione tra gli enti pubblici competenti in Europa, in particolare sostenendo la messa a punto e lo scambio di buone pratiche e di standard;

f) assiste l'Unione e gli Stati membri nella promozione del ricorso a buone pratiche e norme di gestione dei rischi e di sicurezza per prodotti, sistemi e servizi elettronici;

g) sostiene la cooperazione tra le parti interessate del settore pubblico e di quello privato a livello di Unione, tra l'altro promuovendo la condivisione di informazioni e la sensibilizzazione e aiutandole nell'impegno a definire e adottare norme in materia di gestione dei rischi e di sicurezza dei prodotti, delle reti e dei servizi elettronici;

h) facilita il dialogo e lo scambio di buone pratiche tra le parti interessate pubbliche e private in materia di sicurezza delle reti e dell'informazione, inclusi aspetti inerenti la lotta contro la criminalità informatica; assiste la Commissione nell'elaborazione di politiche che tengano conto degli aspetti inerenti la sicurezza delle reti e dell'informazione nella lotta contro la criminalità informatica;

i) assiste, su loro richiesta, gli Stati membri e le istituzioni e gli organismi europei nel loro impegno a mettere a punto capacità di rilevazione, analisi e reazione nel campo della sicurezza delle reti e dell'informazione;

j) sostiene il dialogo e la cooperazione con i paesi terzi e le organizzazioni internazionali, se del caso in collaborazione con la SEAE, per promuovere la cooperazione internazionale e un approccio comune globale alle questioni relative alla sicurezza delle reti e dell'informazione;

k) svolge i compiti attribuitile da atti legislativi dell'Unione.

SEZIONE 2 ORGANIZZAZIONE

Articolo 4
Organi dell'Agenzia

L'agenzia è composta da:

a) un consiglio di amministrazione;

b) un direttore esecutivo con relativo personale; nonché,

c) un gruppo permanente di parti interessate.

Articolo 5
Consiglio di amministrazione

1. Il consiglio di amministrazione definisce gli orientamenti generali del funzionamento dell'Agenzia e assicura che l'Agenzia operi secondo i principi di cui al presente regolamento. Assicura inoltre la coerenza del lavoro dell'Agenzia con le attività svolte dagli Stati membri nonché a livello di Unione.

2. Il consiglio di amministrazione adotta il proprio regolamento interno in accordo con i pertinenti servizi della Commissione.

3. Il consiglio di amministrazione adotta il regolamento interno dell'Agenzia in accordo con i pertinenti servizi della Commissione. Il regolamento è pubblicato.

4. Il consiglio di amministrazione nomina il direttore esecutivo ai sensi dell'articolo 10, paragrafo 2, e può sollevarlo dall'incarico. Il consiglio di amministrazione esercita l'autorità disciplinare sul direttore esecutivo.

5. Il consiglio di amministrazione adotta il programma di lavoro dell'Agenzia conformemente all'articolo 13, paragrafo 3, e la relazione generale sulle attività dell'Agenzia per l'anno precedente secondo quanto previsto all'articolo 14, paragrafo 2.

6. Il consiglio di amministrazione adotta le regole finanziarie applicabili all'Agenzia. Queste possono discostarsi dal regolamento (CE, Euratom) n. 2343/2002 della Commissione, del 19 novembre 2002, che reca regolamento finanziario quadro degli organismi di cui all'articolo 185 del regolamento (CE, Euratom) n. 1605/2002 del Consiglio che stabilisce il regolamento finanziario applicabile al bilancio generale delle Comunità europee[31], solo se lo richiedono le esigenze specifiche di funzionamento dell'Agenzia e previo accordo della Commissione.

7. Il consiglio di amministrazione, di concerto con la Commissione, adotta le modalità di applicazione adeguate, a norma dell'articolo 110 dello statuto dei funzionari.

8. Il consiglio di amministrazione può istituire organismi di lavoro, composti da membri del consiglio medesimo, che lo assistano nello svolgimento delle sue funzioni, compresi la stesura delle sue decisioni e il monitoraggio della relativa attuazione.

9. Il consiglio di amministrazione può adottare un piano pluriennale di politica del personale, previa consultazione dei servizi della Commissione e dopo averne debitamente informato l'autorità di bilancio.

[31] GU L 357 del 31.12.2002, pag. 72.

Articolo 6

Composizione del consiglio di amministrazione

1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro, tre rappresentanti nominati dalla Commissione, nonché tre rappresentanti privi del diritto di voto, designati dalla Commissione, ciascuno dei quali in rappresentanza di uno dei seguenti gruppi:

a) industria della tecnologia dell'informazione e della comunicazione;

b) gruppi di consumatori;

c) esperti universitari in materia di sicurezza delle reti e dell'informazione.

2. I membri del consiglio di amministrazione e i rispettivi supplenti sono nominati in base al grado di esperienza e perizia appropriate nel settore della sicurezza delle reti e dell'informazione.

3. Il mandato dei rappresentanti dei gruppi di cui al paragrafo 1, lettere a), b) e c), è di quattro anni e può essere rinnovato una volta. Se un rappresentante termina la propria partecipazione al rispettivo gruppo di interesse, la Commissione nomina un sostituto.

Articolo 7

Presidente del consiglio di amministrazione

Il consiglio di amministrazione elegge tra i propri membri un presidente e un vicepresidente con mandato di tre anni, rinnovabile. Il vicepresidente sostituisce *ex officio* il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Articolo 8

Riunioni

1. Il consiglio di amministrazione si riunisce su convocazione del presidente.

2. Il consiglio di amministrazione si riunisce in seduta ordinaria due volte l'anno. Si riunisce inoltre in seduta straordinaria su convocazione del presidente o su richiesta di almeno un terzo dei suoi membri aventi diritto di voto.

3. Il direttore esecutivo partecipa alle riunioni del consiglio d'amministrazione, senza diritto di voto.

Articolo 9

Modalità di voto

1. Il consiglio di amministrazione delibera a maggioranza dei suoi membri aventi diritto di voto.

2. La maggioranza di due terzi di tutti i membri aventi diritto di voto è necessaria per l'adozione del regolamento interno del consiglio di amministrazione, del regolamento interno

dell'Agenzia, del bilancio, del programma di lavoro annuale e per la nomina, la proroga del mandato e la revoca del direttore esecutivo.

Articolo 10
Il direttore esecutivo

1. L'Agenzia è diretta dal suo direttore esecutivo che è indipendente nell'espletamento delle sue funzioni.

2. Il direttore esecutivo è nominato e revocato dal consiglio di amministrazione. La nomina è effettuata da un elenco di candidati proposti dalla Commissione per un periodo di cinque anni, in base al merito e a capacità amministrative e manageriali documentate, nonché sulla base di competenze ed esperienze specifiche. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione può essere invitato a fare una dichiarazione presso la competente commissione del Parlamento europeo ed a rispondere alle domande rivolte dai membri di quest'ultima.

3. Durante i nove mesi che precedono questa scadenza, la Commissione procede a una valutazione, che riguarda, in particolare:

– i risultati ottenuti dal direttore esecutivo;

– i compiti e le esigenze dell'Agenzia per gli anni successivi.

4. Il consiglio di amministrazione, deliberando su proposta della Commissione, tenendo conto della relazione di valutazione e solo nei casi in cui ciò possa essere giustificato dai doveri e dalle esigenze dell'Agenzia, può prorogare il mandato del direttore esecutivo per un periodo non superiore a tre anni.

5. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo. Entro un mese prima della proroga del suo mandato, il direttore esecutivo può essere invitato a fare una dichiarazione davanti alla competente commissione del Parlamento europeo e a rispondere alle domande rivolte dai membri di quest'ultima.

6. Se il mandato non è rinnovato, il direttore esecutivo rimane in carica fino alla nomina del suo successore.

7. Il direttore esecutivo è responsabile di:

a) provvedere all'amministrazione corrente dell'Agenzia;

b) attuare il programma di lavoro e le decisioni del consiglio di amministrazione;

c) assicurare che l'Agenzia svolga le proprie attività secondo le esigenze di coloro che fruiscono dei suoi servizi, con particolare riguardo all'adeguatezza dei servizi forniti;

d) tutte le questioni specifiche inerenti il personale, garantendo che siano conformi agli orientamenti e alle decisioni generali del consiglio di amministrazione;

e) sviluppare e mantenere i contatti con le istituzioni e gli organismi europei;

f) sviluppare e mantenere i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con le parti interessate;

g) altri compiti che gli sono attribuiti dal presente regolamento.

8. In base alle esigenze e nell'ambito degli obiettivi e dei compiti dell'Agenzia, il direttore esecutivo può istituire dei gruppi di lavoro ad hoc composti da esperti. Il consiglio di amministrazione ne è informato in anticipo. Le procedure relative in particolare alla composizione, alla nomina degli esperti da parte del direttore esecutivo e al lavoro dei gruppi di lavoro ad hoc vengono specificate nel regolamento interno dell'Agenzia.

9. Il direttore esecutivo mette a disposizione del consiglio di amministrazione personale di supporto e altre risorse, secondo le necessità.

Articolo 11
Gruppo permanente di parti interessate

1. Il consiglio di amministrazione istituisce il gruppo permanente di parti interessate, su proposta del direttore esecutivo, composto da esperti che rappresentano i soggetti interessati, quali l'industria delle tecnologie dell'informazione e della comunicazione, le organizzazioni dei consumatori, gli esperti universitari in materia di sicurezza delle reti e dell'informazione e gli organismi incaricati del rispetto delle norme e quelli preposti alla tutela della privacy.

2. Le modalità inerenti in particolare al numero, alla composizione, alla nomina dei membri da parte del consiglio di amministrazione, alla proposta del direttore esecutivo e al funzionamento del gruppo sono specificate nel regolamento interno dell'Agenzia e rese pubbliche.

3. Il gruppo è presieduto dal direttore esecutivo.

4. Il mandato dei membri è di due anni e mezzo. I membri del consiglio di amministrazione non possono essere membri del gruppo. Il personale della Commissione può presenziare alle riunioni del gruppo e partecipare alle sue attività.

5. Il gruppo fornisce consulenza all'Agenzia per lo svolgimento delle sue attività. In particolare, il gruppo consiglia il direttore esecutivo ai fini della stesura della proposta relativa ai programmi di lavoro dell'Agenzia e nell'assicurare la comunicazione con le parti interessate su tutte le questioni inerenti al programma di lavoro.

SEZIONE 3 FUNZIONAMENTO

Articolo 12
Programma di lavoro

1. L'Agenzia svolge la sua attività secondo quanto previsto dal suo programma di lavoro, che deve contenere tutte le attività programmate. L'esistenza del programma di lavoro non pregiudica la possibilità che l'Agenzia svolga anche attività non programmate che rientrano nei suoi obiettivi e compiti e nei limiti finanziari stabiliti. Il direttore esecutivo informa il consiglio di amministrazione delle attività dell'agenzia non previste nel programma di lavoro.

2. Il direttore esecutivo è responsabile dell'elaborazione del progetto di programma di lavoro dell'Agenzia, previa consultazione dei servizi della Commissione. Entro il 15 marzo di ogni anno il direttore esecutivo trasmette al consiglio di amministrazione il progetto di programma di lavoro per l'anno successivo.

3. Entro il 30 novembre di ogni anno il consiglio di amministrazione, dopo aver consultato i servizi della Commissione, adotta il programma di lavoro dell'Agenzia per l'anno successivo. Il programma di lavoro comprende prospettive pluriennali. Il consiglio di amministrazione provvede a che tale programma sia coerente con gli obiettivi dell'Agenzia nonché con le priorità legislative e strategiche della Comunità nel campo della sicurezza delle reti e dell'informazione.

4. Il programma di lavoro è organizzato secondo il principio della gestione basata sull'attività (ABM, *Activity-Based Management*). Il programma di lavoro è conforme allo stato di previsione delle entrate e delle spese dell'Agenzia e al bilancio dell'Agenzia per lo stesso anno finanziario.

5. Il direttore esecutivo, previa adozione in sede di consiglio di amministrazione, trasmette il programma di lavoro al Parlamento europeo, al Consiglio, alla Commissione e agli Stati membri e ne dispone la pubblicazione.

Articolo 13
Relazione generale

1. Ogni anno, il direttore esecutivo trasmette al consiglio di amministrazione un progetto di relazione generale che tratta tutte le attività svolte dall'Agenzia nell'anno precedente.

2. Entro il 31 marzo di ogni anno il consiglio di amministrazione adotta la relazione generale sulle attività dell'Agenzia per l'anno precedente.

3. Il direttore esecutivo, previa adozione in sede di consiglio di amministrazione, trasmette la relazione generale dell'Agenzia al Parlamento europeo, al Consiglio, alla Commissione, alla Corte dei conti, al Comitato economico e sociale europeo e al Comitato delle regioni e ne dispone la pubblicazione.

Articolo 14
Richieste all'Agenzia

1. Le richieste di consulenze e assistenza nell'ambito degli obiettivi e dei compiti dell'Agenzia sono inoltrate al direttore esecutivo e corredate di una documentazione informativa che illustra la questione da esaminare. Il direttore esecutivo informa il consiglio di amministrazione in merito delle richieste ricevute e, a tempo debito, del seguito dato alle richieste. Qualora respinga una richiesta, l'Agenzia deve motivare il proprio rifiuto.

2. Le richieste di cui al paragrafo 1 possono provenire:

a) dal Parlamento europeo;

b) dal Consiglio;

c) dalla Commissione;

d) da un qualsiasi organismo competente designato da uno Stato membro come autorità nazionale di regolamentazione definita all'articolo 2 della direttiva 2002/21/CE.

3. Le modalità pratiche di applicazione dei paragrafi 1 e 2, con particolare riguardo alla presentazione, alla definizione delle priorità e al seguito da dare alle richieste rivolte all'Agenzia, come pure all'informazione del consiglio di amministrazione in merito ad esse, sono definite dal consiglio di amministrazione nel regolamento interno dell'Agenzia.

Articolo 15
Dichiarazione d'interesse

1. Il direttore esecutivo, come pure i funzionari comandati dagli Stati membri a titolo temporaneo, rendono una dichiarazione scritta di impegni e una dichiarazione scritta con la quale indicano l'assenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza.

2. Gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano a ogni riunione qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del giorno e si astengono dal partecipare alle discussioni inerenti tali punti.

Articolo 16
Trasparenza

1. L'Agenzia si impegna a svolgere le proprie attività con un livello elevato di trasparenza e nel rispetto degli articoli 13 e 14.

2. Essa provvede a che il pubblico e le parti interessate dispongano di informazioni obiettive, affidabili e facilmente accessibili, in particolare riguardanti, eventualmente, i risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese dal direttore esecutivo e dai funzionari comandati dagli Stati membri a titolo temporaneo, nonché le dichiarazioni di interessi rese dagli esperti in relazione ai punti all'ordine del giorno delle riunioni dei gruppi di lavoro ad hoc.

3. Il consiglio di amministrazione, su proposta del direttore esecutivo, può autorizzare altre parti interessate a presenziare come osservatori allo svolgimento di alcune attività dell'Agenzia.

4. L'Agenzia inserisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di trasparenza di cui ai paragrafi 1 e 2.

Articolo 17
Riservatezza

1. Fatto salvo l'articolo 14, l'Agenzia non rivela a terzi le informazioni da essa trattate o ricevute per le quali è stato richiesto un trattamento riservato.

2. I membri del consiglio di amministrazione, il direttore esecutivo, i membri del gruppo permanente di parti interessate, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'Agenzia, compresi i funzionari comandati dagli Stati membri a titolo temporaneo, restano soggetti agli obblighi di riservatezza di cui all'articolo 339 del trattato anche dopo la cessazione delle proprie funzioni.

3. L'Agenzia inserisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione delle regole di riservatezza di cui ai paragrafi 1 e 2.

4. Il consiglio di amministrazione può decidere di consentire all'Agenzia di trattare informazioni riservate. In questo caso, il consiglio di amministrazione, in accordo con i pertinenti servizi della Commissione, adotta un regolamento interno che applica i principi di sicurezza enunciati nella decisione 2001/844/CE, CECA, Euratom della Commissione, del 29 novembre 2001, che modifica il regolamento interno della Commissione[32] e che segnatamente disciplinano lo scambio, il trattamento e la conservazione di informazioni classificate.

Articolo 18
Accesso ai documenti

1. Ai documenti detenuti dall'Agenzia si applica il regolamento (CE) n. 1049/2001.

2. Entro sei mesi dall'istituzione dell'Agenzia, il consiglio di amministrazione adotta disposizioni per l'attuazione del regolamento (CE) n. 1049/2001.

3. Le decisioni adottate dall'Agenzia a norma dell'articolo 8 del regolamento (CE) n. 1049/2001 possono essere impugnate mediante denuncia presentata al mediatore europeo o mediante ricorso dinanzi alla Corte di giustizia dell'Unione europea, a norma rispettivamente degli articoli 228 e 263 del trattato.

SEZIONE 4 DISPOSIZIONI FINANZIARIE

Articolo 19
Adozione del bilancio

1. Le entrate dell'Agenzia sono costituite da un contributo proveniente dal bilancio dell'Unione europea, dal contributo dei paesi terzi che partecipano alle sue attività, come stabilito dall'articolo 29, e dai contributi degli Stati membri.

2. Le spese dell'Agenzia comprendono le spese amministrative, tecniche, infrastrutturali, di esercizio e relative al personale, nonché quelle conseguenti a contratti stipulati con terzi.

3. Entro il 1° marzo di ogni anno il direttore esecutivo redige un progetto di stato di previsione delle entrate e delle spese dell'Agenzia per l'esercizio finanziario successivo e lo trasmette al consiglio di amministrazione, corredato di un progetto di tabella dell'organico.

---

[32] GU L 317 del 3.12.2001, pag. 1.

4. Le entrate e le spese devono risultare in pareggio.

5. Ogni anno il consiglio di amministrazione, sulla base di un progetto di stato di previsione delle entrate e delle spese redatto dal direttore esecutivo, adotta lo stato di previsione delle entrate e delle spese dell'Agenzia per l'esercizio finanziario successivo.

6. Il consiglio di amministrazione trasmette entro il 31 marzo lo stato di previsione, accompagnato da un progetto di tabella dell'organico e un progetto di programma di lavoro, alla Commissione e agli Stati con cui l'Unione europea ha concluso accordi a norma dell'articolo 24.

7. La Commissione trasmette lo stato di previsione al Parlamento europeo e al Consiglio (l'"autorità di bilancio") insieme al progetto di bilancio dell'Unione europea.

8. Sulla base dello stato di previsione, la Commissione iscrive le stime per quanto concerne la tabella dell'organico e l'importo della sovvenzione a carico del bilancio generale nel progetto di bilancio generale dell'Unione europea che essa sottopone all'autorità di bilancio conformemente all'articolo 314 del trattato.

9. L'autorità di bilancio autorizza gli stanziamenti a titolo della sovvenzione destinata all'Agenzia.

10. L'autorità di bilancio adotta la tabella dell'organico per l'Agenzia.

11. Insieme al programma di lavoro, il consiglio di amministrazione adotta il bilancio dell'Agenzia. Esso diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione europea. Se del caso, il consiglio di amministrazione modifica il bilancio e il piano di lavoro dell'Agenzia per conformarli al bilancio generale dell'Unione europea. Il consiglio di amministrazione lo trasmette senza indugio alla Commissione e all'autorità di bilancio.

Articolo 20
Lotta antifrode

1. Nella lotta contro la frode, la corruzione ed altre attività illegali si applicano senza limitazioni le disposizioni del regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio, del 25 maggio 1999, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF)[33].

2. L'Agenzia aderisce all'accordo interistituzionale del 25 maggio 1999 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione delle Comunità europee relativo alle indagini interne svolte dall'Ufficio europeo per la lotta antifrode (OLAF)[34] e adotta immediatamente le disposizioni corrispondenti valide per l'insieme dei collaboratori dell'Agenzia.

[33] GU L 136 del 31.5.1999, pag. 1.
[34] GU L 136 del 31.5.1999, pag. 15.

Articolo 21
Esecuzione del bilancio

1. Il direttore esecutivo esegue il bilancio dell'Agenzia.

2. Il revisore contabile interno della Commissione esercita nei confronti dell'Agenzia le stesse competenze di cui dispone nei confronti dei servizi della Commissione.

3. Entro il 1° marzo successivo alla chiusura dell'esercizio il contabile dell'Agenzia trasmette al contabile della Commissione i conti provvisori insieme a una relazione sulla gestione finanziaria e di bilancio dell'esercizio. Il contabile della Commissione procede al consolidamento dei conti provvisori delle istituzioni e degli organismi decentrati conformemente all'articolo 128 del regolamento (CE, Euratom) n. 1605/2002 del Consiglio, del 25 giugno 2002, che stabilisce il regolamento finanziario applicabile al bilancio generale delle Comunità europee[35] (in prosieguo: "regolamento finanziario generale").

4. Entro il 31 marzo successivo alla chiusura dell'esercizio, il contabile della Commissione trasmette i conti provvisori dell'Agenzia, insieme alla relazione sulla gestione finanziaria e di bilancio dell'esercizio, alla Corte dei conti. La relazione sulla gestione finanziaria e di bilancio dell'esercizio è trasmessa anche all'autorità di bilancio.

5. Al ricevimento delle osservazioni formulate dalla Corte dei conti in merito ai conti provvisori dell'Agenzia, ai sensi dell'articolo 129 del regolamento finanziario generale, il direttore esecutivo stabilisce i conti definitivi dell'Agenzia, sotto la propria responsabilità, e li trasmette per parere al consiglio di amministrazione.

6. Il consiglio di amministrazione esprime un parere sui conti definitivi dell'Agenzia.

7. Entro il 1° luglio successivo alla chiusura dell'esercizio finanziario, il direttore esecutivo trasmette i conti definitivi, corredati del parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.

8. Il direttore esecutivo pubblica i conti definitivi.

9. Il direttore esecutivo invia alla Corte dei conti entro il 30 settembre una risposta alle osservazioni da essa formulate e ne trasmette copia al consiglio di amministrazione.

10. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo e conformemente all'articolo 146, paragrafo 3, del regolamento finanziario generale, tutte le informazioni necessarie al corretto svolgimento della procedura di scarico per l'esercizio in oggetto.

11. Il Parlamento europeo, agendo su raccomandazione del Consiglio, dà discarico al direttore esecutivo, entro il 30 aprile dell'anno N+2, dell'esecuzione del bilancio dell'esercizio N.

---

35 GU L 248 del 16.9.2002, pag. 1.

SEZIONE 5 DISPOSIZIONI GENERALI

Articolo 22
Natura giuridica

1. L'Agenzia è un organismo dell'Unione. Essa ha personalità giuridica.

2. In ciascuno degli Stati membri l'Agenzia ha la più ampia capacità giuridica riconosciuta alle persone giuridiche dalle rispettive legislazioni. In particolare, può acquisire e alienare beni mobili e immobili e stare in giudizio.

3. L'Agenzia è rappresentata dal proprio direttore esecutivo.

Articolo 23
Personale

1. Il personale dell'Agenzia, compreso il direttore esecutivo, è soggetto alle norme e ai regolamenti che si applicano ai funzionari e agli altri agenti dell'Unione europea.

2. Il consiglio di amministrazione esercita, relativamente al direttore esecutivo, le competenze conferite all'autorità investita del potere di nomina dallo Statuto dei funzionari e all'autorità abilitata a stipulare i contratti dal regime.

3. Il direttore esecutivo esercita, relativamente al personale dell'Agenzia, le competenze conferite all'autorità investita del potere di nomina dallo Statuto dei funzionari e all'autorità abilitata a stipulare contratti dal regime.

4. L'Agenzia può avvalersi di esperti nazionali distaccati degli Stati membri. L'Agenzia inserisce nel proprio regolamento interno le disposizioni pratiche per l'attuazione di questa disposizione.

Articolo 24
Privilegi e immunità

All'Agenzia e al suo personale si applica il protocollo sui privilegi e sulle immunità delle Comunità europee.

Articolo 25
Responsabilità

1. La responsabilità contrattuale dell'Agenzia è disciplinata dalla normativa applicabile al contratto di cui trattasi.

La Corte di giustizia dell'Unione europea è competente a giudicare in virtù di clausole compromissorie contenute in un contratto concluso dall'Agenzia.

2. In materia di responsabilità extracontrattuale, l'Agenzia è obbligata, secondo i principi generali comuni agli ordinamenti degli Stati membri, al risarcimento dei danni cagionati da essa o dai suoi agenti nell'esercizio delle loro funzioni.

La Corte di giustizia è competente a conoscere delle controversie relative al risarcimento di tali danni.

3. La responsabilità personale degli agenti nei confronti dell'Agenzia è disciplinata dalle disposizioni pertinenti che si applicano al personale dell'Agenzia.

Articolo 26
Lingue

1. All'Agenzia si applicano le disposizioni previste nel regolamento n. 1 del 15 aprile 1958 che stabilisce il regime linguistico della Comunità economica europea[36]. Gli Stati membri e gli altri organismi da essi designati possono rivolgersi all'Agenzia e ottenere la risposta nella lingua dell'Unione di loro scelta.

2. I servizi di traduzione necessari per il funzionamento dell'Agenzia vengono forniti dal Centro di traduzione per gli organismi dell'Unione europea.

Articolo 27
Protezione dei dati di carattere personale

Per il trattamento dei dati relativi agli individui, l'Agenzia è soggetta alle disposizioni del regolamento (CE) n. 45/2001.

Articolo 28
Partecipazione di paesi terzi

1. Alle attività dell'Agenzia possono partecipare i paesi terzi che hanno concluso con l'Unione europea accordi in virtù dei quali hanno adottato e applicano la normativa UE nella materia disciplinata dal presente regolamento.

2. In forza delle pertinenti disposizioni di tali accordi sono concordate soluzioni organizzative relative in particolare alla natura, alla portata e alle modalità di partecipazione di tali paesi alle attività dell'Agenzia, comprese disposizioni riguardanti la partecipazione alle iniziative intraprese dall'Agenzia, i contributi finanziari e il personale.

[36] GU 17 del 6.10.1958, pag. 385. Regolamento modificato da ultimo dal trattato di adesione del 1994.

SEZIONE 6 DISPOSIZIONI FINALI

Articolo 29
Clausola di riesame

1. Entro tre anni dalla data di istituzione di cui all'articolo 34, la Commissione, tenendo conto dei pareri di tutti i soggetti interessati, procede a una valutazione sulla base del mandato concordato con il consiglio di amministrazione. La valutazione esamina l'impatto e l'efficacia dell'Agenzia ai fini del raggiungimento degli obiettivi di cui all'articolo 2 e dell'efficacia delle pratiche operative dell'Agenzia. La Commissione esegue la valutazione in particolare per determinare se l'Agenzia è ancora uno strumento efficace e se la durata dell'Agenzia debba essere ulteriormente prorogata oltre il periodo di cui all'articolo 34.

2. Le risultanze della valutazione sono trasmesse dalla Commissione al Parlamento europeo e al Consiglio e sono rese pubbliche.

3. La valutazione è trasmessa al consiglio di amministrazione, che presenta alla Commissione raccomandazioni in merito alle modifiche da apportare al presente regolamento, all'Agenzia ed ai suoi metodi di lavoro. Il consiglio di amministrazione e il direttore esecutivo dovrebbero tenere conto dei risultati della valutazione in sede di pianificazione pluriennale delle attività dell'Agenzia.

Articolo 30
Cooperazione dello Stato membro ospitante

Lo Stato membro in cui ha sede l'Agenzia garantisce le migliori condizioni possibili per un funzionamento corretto ed efficace dell'Agenzia.

Articolo 31
Controllo amministrativo

L'operato dell'Agenzia è sottoposto al controllo del mediatore, a norma delle disposizioni dell'articolo 228 del trattato.

Articolo 32
Abrogazione e sostituzione

1. Il regolamento (CE) n. 460/2004 è abrogato.

I riferimenti al regolamento (CE) n. 460/2004 e all'ENISA si intendono fatti al presente regolamento e all'Agenzia.

2. L'Agenzia sostituisce l'Agenzia istituita dal regolamento (CE) n. 460/2004 per quanto riguarda diritti di proprietà, accordi, obblighi giuridici, contratti di lavoro, impegni finanziari e responsabilità.

Articolo 33
Durata

L'Agenzia è istituita il […] per un periodo di cinque anni.

Articolo 34
Entrata in vigore

Il presente regolamento entra in vigore il giorno successivo alla data di pubblicazione nella *Gazzetta ufficiale dell'Unione europea* e si applica a decorrere dal 14 marzo 2012, oppure dal giorno successivo alla data di pubblicazione, a seconda di quale sia la data posteriore.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a […],

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

SCHEDA FINANZIARIA LEGISLATIVA PER PROPOSTE

1. CONTESTO DELLA PROPOSTA/ INIZIATIVA

1.1. Denominazione della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

1.2. Politica interessata nella struttura ABM/ABB[37]

Società dell'informazione e media.

Quadro normativo per l'agenda digitale.

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. Obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

Coerenza degli approcci normativi – fornire orientamenti e consulenze alla Commissione e agli Stati membri per l'aggiornamento e la definizione di un quadro normativo globale nel campo della sicurezza delle reti e dell'informazione.

Prevenzione, rilevamento e reazione – migliorare la preparazione contribuendo alla capacità europea di allarme tempestivo e di reazione in caso di incidenti e alla messa a punto di esercitazioni e piani di emergenza paneuropei.

Promuovere la conoscenza per i responsabili politici – fornire assistenza e consulenza alla Commissione e agli Stati membri per raggiungere un elevato livello di conoscenza, in tutta l'Unione, in materia di sicurezza delle reti e dell'informazione e della sua applicazione alle parti interessate del settore. Sono compresi anche la creazione, l'analisi e la diffusione dei dati relativi all'economia e all'impatto delle violazioni della sicurezza, gli elementi che favoriscono gli investimenti nelle misure relative alla sicurezza delle reti e dell'informazione, l'identificazione dei rischi e gli indicatori dello stato della sicurezza nell'Unione, ecc.

Responsabilizzazione delle parti interessate – sviluppare una cultura della sicurezza e della gestione dei rischi favorendo la condivisione di informazioni e la cooperazione tra le

[37] ABM: Activity Based Management – ABB: Activity Based Budgeting.

[38] Secondo la definizione di cui all'articolo 49, paragrafo 6, lettera a) o b), del regolamento finanziario.

parti sia del settore pubblico che di quello privato, anche a diretto vantaggio dei cittadini, e favorire il diffondersi di una cultura in materia di sicurezza delle reti e dell'informazione.

Proteggere l'Europa dalle minacce internazionali – raggiungere un elevato livello di cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere un approccio comune alla sicurezza su scala mondiale e incoraggiare iniziative internazionali di alto livello in Europa.

Verso una collaborazione ai fini dell'attuazione – facilitare la collaborazione nell'attuazione delle politiche in materia di sicurezza delle reti e dell'informazione.

Lotta contro la criminalità informatica – integrare gli aspetti relativi alla sicurezza delle reti e dell'informazione della lotta alla criminalità informatica nelle discussioni e nello scambio di buone pratiche tra parti pubbliche e private, in particolare tramite la cooperazione con le autorità del secondo e terzo pilastro (non più esistenti), ad es. con Europol.

1.4.2. Obiettivi specifici e attività ABM/ABB interessate

Obiettivo specifico

Potenziare la sicurezza delle reti e dell'informazione, sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico, nonché individuare le sfide cui saranno confrontate le reti future e Internet.

Attività AMB/ABB interessate

Politica delle comunicazioni elettroniche e della sicurezza delle reti

1.4.3. Risultati ed effetti previsti

Si prevede che l'iniziativa abbia i seguenti impatti sull'economia:

- maggiore disponibilità di informazioni sulle sfide attuali e future in questo settore e sui rischi per la sicurezza e la resilienza;

- non duplicazione degli sforzi nella raccolta di informazioni rilevanti relative ai rischi, alle minacce e alle vulnerabilità in ciascuno Stato membro;

- più elevato livello di informazione dei responsabili politici quando prendono decisioni;

- migliore qualità delle disposizioni in materia di sicurezza delle reti e dell'informazione negli Stati membri grazie alla diffusione di buone pratiche;

- economie di scala nella reazione agli incidenti a livello di UE;

- maggiori investimenti stimolati da obiettivi strategici e standard comuni per la sicurezza e la resilienza a livello di UE;

- minori rischi operativi per le imprese grazie ad un più elevato livello di sicurezza e resilienza;

- maggiore coerenza degli strumenti per la lotta alla criminalità informatica;

Si prevede che l'iniziativa abbia i seguenti impatti sulla società:

- maggiore fiducia degli utenti nei sistemi e nei servizi della società dell'informazione;

- maggiore fiducia nel funzionamento del mercato interno dell'UE grazie a una migliore tutela dei consumatori;

- maggiore scambio di informazioni e conoscenze con i paesi terzi;

- migliore tutela dei diritti umani fondamentali nell'Unione grazie alla parità di tutela dei dati personali e della riservatezza dei cittadini dell'UE.

Gli effetti previsti sull'ambiente sono trascurabili:

- minore impatto delle emissioni di CO_2 grazie, ad esempio, ai minori spostamenti derivanti dal maggiore ricorso all'uso di sistemi e servizi TIC e minore consumo di energia grazie alle economie di scala nell'attuazione degli obblighi in materia di sicurezza.

1.4.4. Indicatori di risultato e di incidenza

Per ogni obiettivo si applicano i seguenti indicatori di monitoraggio:

Coerenza degli approcci normativi:

- numero di Stati membri che si è avvalso delle raccomandazioni dell'Agenzia nell'ambito del processo decisionale;

- numero di studi volti a individuare carenze e incongruenze nel panorama delle norme applicabili alla sicurezza delle reti e dell'informazione;

- riduzione delle divergenze di approccio tra i diversi Stati membri.

Prevenzione, rilevazione e reazione:

- numero di formazioni organizzate nel campo della sicurezza delle reti e dell'informazione;

- disponibilità di un sistema di allarme tempestivo funzionante per i rischi emergenti e gli attacchi;

- numero di esercitazioni in materia di sicurezza delle reti e dell'informazione a livello di UE coordinate dall'Agenzia.

Promuovere la conoscenza per i responsabili politici:

- Numero di studi condotti per raccogliere informazioni in merito ai rischi attuali e previsti in relazione alla sicurezza delle reti e dell'informazione e tecnologie per la prevenzione dei rischi

- Numero di consultazioni con enti pubblici che si occupano di sicurezza delle reti e dell'informazione

- Disponibilità di un quadro europeo per l'organizzazione dei dati raccolti

Responsabilizzazione delle parti interessate:

- Numero di buone pratiche individuate per il settore

- Livello degli investimenti in misure di sicurezza da parte di privati

Proteggere l'Europa dalle minacce internazionali:

- Numero di conferenze/riunioni tra Stati membri per definire obiettivi comuni in materia

- Numero di riunioni tra esperti europei e internazionali in materia di sicurezza delle reti e dell'informazione

Verso una collaborazione ai fini dell'attuazione:

- Numero di valutazioni della conformità normativa

- Numero di pratiche in materia di sicurezza delle reti e dell'informazione diffuse in tutta l'UE

Lotta contro la criminalità informatica:

- Regolarità delle interazioni tra agenzie attinenti ai precedenti secondo e terzo pilastro

- Numero di casi in cui è stata fornita assistenza durante indagini penali.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità dell'azione nel breve e lungo termine

L'ENISA è stata istituita nel 2004 per affrontare le minacce alla sicurezza delle reti e dell'informazione e le violazioni che potrebbero derivarne. Da allora le sfide sono cambiate con l'evolvere della tecnologia e del mercato e sono state al centro di ulteriori riflessioni e dibattiti, grazie ai quali oggi è possibile descrivere in modo aggiornato e più dettagliato i problemi specifici che sono stati identificati e come questi risentono del costante variare delle questioni inerenti la sicurezza.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

I problemi legati alla sicurezza delle reti e dell'informazione superano i confini nazionali, pertanto non possono essere affrontati in maniera efficace solo a livello nazionale. Allo stesso tempo, nei vari Stati membri le autorità pubbliche affrontano la questione in modo molto diverso. Queste differenze possono costituire un enorme ostacolo all'attuazione di meccanismi adeguati per potenziare la sicurezza delle reti e dell'informazione in tutta l'Unione europea. Per via dell'interconnessione delle infrastrutture delle TIC, l'eventuale inadeguatezza delle misure adottate in alcuni Stati membri si ripercuote fortemente sull'efficacia delle misure adottate a livello nazionale in altri Stati membri, pregiudicata

anche dalla mancanza di una sistematica cooperazione transfrontaliera. Misure di sicurezza insufficienti all'origine di un incidente legato alle reti e all'informazione in uno Stato membro possono causare interruzioni dei servizi anche in altri Stati membri.

Inoltre, il moltiplicarsi delle prescrizioni in materia di sicurezza comporta costi per le imprese che sono attive a livello dell'Unione e causano frammentazione e mancanza di competitività nel mercato interno europeo.

Mentre la dipendenza dalle reti e dai sistemi di informazione è in aumento, la capacità di reagire agli incidenti sembra insufficiente.

Gli attuali sistemi nazionali di allarme tempestivo e di intervento in caso di incidenti presentano gravi carenze. I processi e le pratiche applicati per monitorare e notificare gli incidenti a danno della sicurezza delle reti sono però molto diversi da uno Stato membro all'altro. In alcuni paesi i processi non sono formalizzati mentre in altri non esiste un'autorità competente a ricevere e trattare le notifiche sugli incidenti. Non esistono sistemi europei, di conseguenza la fornitura dei servizi di base potrebbe subire turbative gravi per via di incidenti legati alla sicurezza delle reti e dell'informazione e occorre quindi approntare modalità di reazione adeguate. La comunicazione della Commissione sulla protezione delle infrastrutture critiche informatizzate e di comunicazione ha sottolineato inoltre la necessità di una capacità di allarme tempestivo e di reazione in caso di incidenti a livello europeo, eventualmente supportata da esercitazioni su scala europea.

Occorrono chiaramente strumenti strategici volti a individuare attivamente i rischi e le vulnerabilità legate alla sicurezza delle reti e dell'informazione, a istituire adeguati meccanismi di reazione (ad esempio individuando e diffondendo buone pratiche) e a garantire che tali meccanismi di risposta siano conosciuti e utilizzati da tutte le parti interessate.

1.5.3. Principali insegnamenti tratti da esperienze simili

Si vedano i punti 1.5.1 e 1.5.2

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

Questa iniziativa è pienamente coerente con il dibattito generale in materia di sicurezza delle reti e dell'informazione e con altre iniziative strategiche incentrate sul futuro del settore. Si tratta di uno dei principali elementi dell'Agenda digitale europea, a sua volta un'iniziativa faro della strategia "Europa 2020".

1.6. Durata dell'azione e incidenza finanziaria

☑ Proposta/iniziativa a **durata limitata**

– ☑ Il punto iniziale della proroga quinquennale è il 14.3.2012 o il giorno di entrata in vigore del nuovo regolamento, se successivo.

– ☑ Incidenza finanziaria dal 2012 al 2017

☐ Proposta/iniziativa a **durata illimitata**

– Attuazione con un periodo di avviamento dal AAAA al AAAA

– seguito da un funzionamento a ritmo regolare.

1.7. Modalità di gestione previste[39]

☐ **Gestione centralizzata diretta** da parte della Commissione

☑ **Gestione centralizzata indiretta** con delega delle funzioni di esecuzione a:

– ☐ agenzie esecutive

– ☑ organismi istituiti dall'Unione europea[40]

– ☐ organismi pubblici nazionali/organismi con funzioni di servizio pubblico

– ☐ persone incaricate di attuare azioni specifiche di cui al titolo V del trattato UE, 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 (***specificare***)

---

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.html

40 A norma dell'articolo 185 del regolamento finanziario.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di controllo e di comunicazione

Il direttore esecutivo è responsabile del controllo e della valutazione effettivi delle realizzazioni dell'Agenzia rispetto agli obiettivi fissati, e riferisce annualmente al consiglio di amministrazione.

Il direttore esecutivo redige una relazione generale riguardante tutte le attività svolte dall'Agenzia nel corso dell'anno precedente, confrontando in particolare i risultati ottenuti con gli obiettivi del programma di lavoro annuale. Una volta adottata dal consiglio di amministrazione, la relazione viene trasmessa al Parlamento europeo, al Consiglio, alla Commissione, alla Corte dei Conti, al Comitato economico e sociale europeo e al Comitato delle regioni, e pubblicata.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi identificati

Dalla sua istituzione nel 2004 l'ENISA è stata oggetto di valutazioni esterne ed interne.

Ai sensi dell'articolo 25 del regolamento che istituisce l'ENISA, la prima tappa di questo processo è stata una valutazione indipendente dell'Agenzia realizzata da un gruppo di esperti esterni nel 2006/2007. La relazione elaborata dal gruppo di esperti esterni[41] ha confermato la validità delle ragioni strategiche che avevano motivato l'istituzione dell'ENISA e delle sue finalità originali, ed è servita a definire alcune delle questioni che occorreva affrontare.

Nel marzo 2007 la Commissione ha riferito in merito alla valutazione al consiglio di amministrazione, che ha successivamente formulato le sue raccomandazioni sul futuro dell'Agenzia e sulle modifiche da apportare al regolamento ENISA[42].

Nel giugno 2007 la Commissione ha presentato la sua valutazione dei risultati della valutazione esterna e delle raccomandazioni del consiglio di amministrazione in una comunicazione al Parlamento europeo e al Consiglio[43]. Nella comunicazione si afferma che occorre decidere se prorogare il mandato dell'Agenzia o sostituire l'ENISA con un altro meccanismo, ad esempio un forum permanente delle parti interessate o una rete di organizzazioni operanti nel settore della sicurezza. La comunicazione ha anche lanciato una consultazione pubblica sull'argomento, sollecitando le proposte e le reazioni delle parti interessate europee con un elenco di domande volte a guidare l'ulteriore dibattito[44].

---

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 Ai sensi dell'articolo 25 del regolamento ENISA. Il testo integrale del documento adottato dal consiglio di amministrazione dell'ENISA, contenente tra l'altro anche le riflessioni del consiglio, è disponibile sul seguente sito Web: http://enisa.europa.eu/pages/03_02.htm.

43 Comunicazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), COM (2007) 285 definitivo dell'1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:IT:NOT.

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

2.2.2. Modalità di controllo previste

Si vedano i punti 2.1 e 2.2.1.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Il controllo dei pagamenti per tutti i servizi o studi necessari viene effettuato dal personale dell'Agenzia prima del pagamento stesso, tenendo conto degli obblighi contrattuali, dei principi economici e delle prassi finanziarie o di sana gestione. Disposizioni antifrode (sorveglianza, obbligo di presentare relazioni, ecc.) saranno inserite in tutti gli accordi e contratti stipulati tra l'Agenzia e i beneficiari dei pagamenti.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/ INIZIATIVA*

3.1. Rubriche del quadro finanziario pluriennale e linee di bilancio di spesa interessate

- Linee di bilancio di spesa esistenti

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Partecipazione			
	Numero / Descrizione	SD/SND (45)	di paesi EFTA[46]	di paesi candidati[47]	di paesi terzi	ai sensi dell'articolo 18, paragrafo 1, lettera a bis), del regolamento finanziario
1.a Competitività per la crescita e l'occupazione	09 02 03 01 Agenzia europea per la sicurezza delle reti e dell'informazione – Sovvenzione ai titoli 1 e 2	SD	SÌ	NO	NO	NO
	09 02 03 02 Agenzia europea per la sicurezza delle reti e dell'informazione – Sovvenzione al titolo 3	SD	SÌ	NO	NO	NO
5 Spese amministrative	09 01 01 Spese relative al personale in attività di servizio del settore «Società dell'informazione e media»	SND	NO	NO	NO	NO
	09 01 02 11 Altre spese di gestione	SND	NO	NO	NO	NO

* L'incidenza finanziaria prevista della proposta per il periodo successivo all'attuale periodo di programmazione finanziaria (2007-2013) non rientra nella presente scheda finanziaria legislativa. Sulla base della proposta della Commissione del regolamento che fissa il quadro finanziario pluriennale dopo il 2013 e tenendo conto delle conclusioni della valutazione di impatto, la Commissione presenterà una scheda finanziaria legislativa modificata.

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

46 EFTA: Associazione europea di libero scambio.

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

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

milioni di EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale:	1.a	Competitività per la crescita e l'occupazione

ENISA			1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	**TOTALE 14 mar 2012-13 mar 2017**
Stanziamenti operativi										
09 02 03 02 Agenzia europea per la sicurezza delle reti e dell'informazione – Sovvenzione al titolo 3	Impegni	(1)	0,454	1,976	2,470	--	--	--	--	--
	Pagamenti	(2)	0,454	1,976	2,470	--	--	--	--	--
Stanziamenti amministrativi										
09 02 03 01 Agenzia europea per la sicurezza delle reti e dell'informazione – Sovvenzione ai titoli 1 e 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTALE degli stanziamenti per la RUBRICA 1a	Impegni	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Pagamenti	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTALE degli stanziamenti operativi	Impegni	(4)	0,454	1,976	2,470	--	--	--	--	--
	Pagamenti	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTALE degli stanziamenti per la RUBRICA 1.a del programma quadro pluriennale	Impegni	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Pagamenti	=5+6	1,747	6,673	8,590	--	--	--	--	--

milioni di EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale:	5	Spese amministrative

		1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	Totale
Risorse umane		0,085	0,342	0,427	--	--	--	--	--
Altre spese amministrative		0,002	0,013	0,015	--	--	--	--	--
TOTALE DG INFSO	Stanziamenti	0,087	0,355	0,442	--	--	--	--	--

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Impegni totali = pagamenti totali)	0,087	0,355	0,442	--	--	--	--	--

		1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	Totale
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	1,834	7,028	9,032	--	--	--	--	--
	Pagamenti	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Incidenza prevista sugli stanziamenti operativi

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

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

Stanziamenti di impegno in milioni di EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩	1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	**TOTALE 14 mar 2012- 13 mar 2017**
Coerenza degli approcci normativi:	0,114	0,494	0,620	--	--	--	--	--
Prevenzione, mitigazione e reazione	0,114	0,494	0,620	--	--	--	--	--
Promuovere la conoscenza per i responsabili politici	0,068	0,297	0,370	--	--	--	--	--
Responsabilizzazione delle parti interessate	0,050	0,218	0,270	--	--	--	--	--
Proteggere l'Europa dalle minacce internazionali	0,023	0,099	0,120	--	--	--	--	--
Verso una collaborazione ai fini dell'attuazione	0,064	0,276	0,340	--	--	--	--	--
Lotta contro la criminalità informatica	0,023	0,098	0,120	--	--	--	--	--
COSTO TOTALE	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa[48]

3.2.3.1. Sintesi

– ☐ La proposta/iniziativa non comporta l'utilizzazione di stanziamenti di natura amministrativa

– ☑ La proposta/iniziativa comporta l'utilizzazione di stanziamenti di natura amministrativa, come spiegato di seguito:

a) Spesa amministrativa per la rubrica 5 del quadro finanziario pluriennale

milioni di EUR (al terzo decimale)

RUBRICA 5 del quadro finanziario pluriennale	1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	**TOTALE 14 mar 2012-13 mar 2017**
Risorse umane	0,085	0,342	0,427	--	--	--	--	--
Altre spese amministrative	0,002	0,013	0,015	--	--	--	--	--
TOTALE	0,087	0,355	0,442	--	--	--	--	--

b) Spesa amministrativa relativa all'ENISA - finanziata dalla linea di bilancio "09.020301 Sicurezza delle reti e dell'informazione: Titolo 1 – Personale e Titolo 2 – Funzionamento dell'agenzia".

milioni di EUR (al terzo decimale)

	1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	**TOTALE 14 mar 2012-13 mar 2017**
Titolo 1 – Risorse umane - Personale	1,153	4,329	5,607	--	--	--	--	--
Altre spese di natura amministrativa – Titolo 2 – Funzionamento dell'Agenzia	0,140	0,368	0,513	--	--	--	--	--

[48] L'allegato della scheda finanziaria legislativa non è compilato perché non è applicabile alla proposta in oggetto.

TOTALE	**1,293**	**4,697**	**6,120**	--	--	--	--	--

3.2.3.2. Fabbisogno previsto di risorse umane

Ogni anno la tabella dell'organico dell'Agenzia è illustrata e motivata in un documento chiamato "Piano di politica del personale" che deve essere trasmesso all'autorità di bilancio.

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

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

a) Risorse umane nei servizi della Commissione

	1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017
Posti della tabella dell'organico (funzionari e agenti temporanei)							
XX 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)	3,5	3,5	3,5	--	--	--	--
TOTALE	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Risorse umane dell'ENISA

		1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017
Posti della tabella nell'organico dell'ENISA (in equivalenti a tempo pieno)								
Funzionari o agenti temporanei	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTALE Funzionari o agenti temporanei		44	47	47	--	--	--	--
Altro personale (in equivalenti a tempo pieno)								
Agenti contrattuali		13	14	14	--	--	--	--
Esperti nazionali distaccati		5	5	5	--	--	--	--
Totale altro personale		18	19	19	--	--	--	--
TOTALE		**62**	**66**	**66**	--	--	--	--

Descrizione dei compiti che devono essere svolti dal personale dell'Agenzia:

Funzionari e agenti temporanei	L'Agenzia continuerà: – a svolgere funzioni consultive e di coordinamento relative alla **raccolta e all'analisi di dati** sulla sicurezza dell'informazione. Oggi sia organizzazioni private che enti pubblici con diverse finalità raccolgono dati relativi agli incidenti nel settore delle TI e altri dati pertinenti alla sicurezza dell'informazione. Non esiste però un'entità centrale a livello europeo che possa raccogliere e analizzare in modo esauriente i dati e fornire pareri e consulenze a sostegno dell'impegno strategico dell'Unione in materia di sicurezza delle reti e dell'informazione; – a fungere da **centro di competenze** al quale possono rivolgersi sia gli Stati membri che le istituzioni europee per ottenere **pareri e consulenze su questioni tecniche** legate alla sicurezza; – a contribuire ad **un'ampia collaborazione fra diversi soggetti** nel campo della sicurezza dell'informazione, ad esempio fornendo assistenza nelle attività di controllo a sostegno di un commercio elettronico sicuro. Una tale collaborazione rappresenta un prerequisito essenziale del funzionamento sicuro delle reti e dei sistemi di informazione in Europa. Sono necessari la partecipazione e l'impegno di tutti i soggetti interessati; – a contribuire ad un approccio coordinato alla società dell'informazione, fornendo **assistenza agli Stati membri**, ad esempio, nella **promozione della valutazione dei rischi** e nelle azioni di sensibilizzazione; – a garantire **l'interoperabilità delle reti e dei sistemi di informazione** quando gli Stati membri **applicano** requisiti tecnici che influiscono sulla sicurezza; – a individuare le esigenze di **normalizzazione** e a valutare le norme di sicurezza e i regimi di certificazione, promuovendone l'uso più ampio possibile a sostegno della legislazione europea; – a sostenere la **cooperazione internazionale** in questo settore, sempre più necessaria in quanto le questioni di sicurezza delle reti e dell'informazione sono caratterizzate da una dimensione mondiale.
Personale esterno	Vedere sopra.

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

– ☑ La proposta/iniziativa è compatibile con la programmazione finanziaria in vigore.

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

– ☐ La proposta/iniziativa richiede l'attivazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[49].

Il finanziamento dell'UE dopo il 2013 sarà esaminato nell'ambito di un dibattito che coinvolgerà tutta la Commissione e verterà sulle proposte relative al periodo post-2013. Questo significa che, una volta presentata la proposta per il quadro finanziario pluriennale successivo, la Commissione presenta una scheda finanziaria legislativa modificata che tiene conto delle conclusioni della valutazione di impatto.

3.2.5. Partecipazione di terzi al finanziamento

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

– ☑ La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Stanziamenti di impegno in milioni di EUR (al terzo decimale)

	1° gen – 13 mar 2012	14 mar – 31 dic 2012	2013	2014	2015	2016	1° gen – 13 mar 2017	**TOTALE 14 mar 2012- 13 mar 2017**
EFTA	0,042	0,160	0,206	--	--	--	--	--

3.3. Incidenza prevista sulle entrate

– ☑ La proposta/iniziativa non incide finanziariamente sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

  – ☐ sulle risorse proprie

  – ☐ sulle entrate varie

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