Consiglio dell'Unione europea

Bruxelles, 1º marzo 2018
(OR. en)

12183/2/17
REV 2

Fascicolo interistituzionale: 2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139
CSC 276
CSCI 68

PROPOSTA

n. doc. Comm.:	COM(2017) 477 final/3
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

Si trasmette in allegato, per le delegazioni, il documento COM(2017) 477 final/3.

All.: COM(2017) 477 final/3

COMMISSIONE
EUROPEA

Bruxelles, 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2014

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

(Testo rilevante ai fini del SEE)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

L'Unione europea ha adottato una serie di provvedimenti per diventare più resiliente e migliorare la sua preparazione in materia di cibersicurezza. La prima strategia dell'Unione europea per la cibersicurezza[1], adottata nel 2013, definisce obiettivi strategici e azioni concrete per raggiungere la resilienza, ridurre la criminalità informatica, sviluppare una politica e le capacità di ciberdifesa, sviluppare le risorse industriali e tecnologiche in materia e instaurare una politica internazionale coerente dell'Unione europea sul ciberspazio. In tale contesto, sono stati conseguiti da allora importanti sviluppi, compreso in particolare l'avvio del secondo mandato dell'Agenzia dell'Unione europea per la sicurezza delle reti e dei sistemi informativi (ENISA)[2] e l'adozione della **direttiva sulla sicurezza delle reti e dei sistemi informativi**[3] ("direttiva NIS"), che costituiscono la base della presente proposta.

Inoltre, nel 2016 la Commissione ha adottato una comunicazione intitolata **"Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza"**[4], in cui annunciava ulteriori misure per intensificare la cooperazione, lo scambio di informazioni e di conoscenze e aumentare la resilienza e la preparazione dell'UE, prendendo anche in considerazione l'eventualità di possibili incidenti informatici su vasta scala e di una crisi della cibersicurezza a livello paneuropeo. In tale contesto, la Commissione aveva annunciato che avrebbe effettuato **una valutazione** e una **revisione** del regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio relativo all'ENISA e che abroga il regolamento (CE) n. 460/2004 ("regolamento ENISA"). Il processo di valutazione avrebbe potuto sfociare in un'eventuale riforma dell'Agenzia e in un rafforzamento delle sue competenze e capacità per assistere gli Stati membri in modo sostenibile. La riforma avrebbe pertanto dato un taglio più operativo e un ruolo centrale per quanto riguarda la resilienza in materia di cibersicurezza e il nuovo mandato dell'Agenzia avrebbe rispecchiato le sue nuove responsabilità in forza della direttiva NIS.

La direttiva NIS costituisce un primo passo fondamentale per promuovere una cultura della gestione del rischio, introducendo requisiti di sicurezza obbligatori per i principali operatori economici, in particolare gli operatori che forniscono servizi essenziali (operatori di servizi essenziali — OES) e i fornitori di alcuni dei principali servizi digitali (fornitori di servizi digitali — DSP). Considerando fondamentali i requisiti di sicurezza per salvaguardare i benefici della crescente digitalizzazione della società, e data la rapida proliferazione di dispositivi connessi (internet degli oggetti - IoT), la comunicazione del 2016 avanza anche l'idea di instaurare un quadro per la certificazione della sicurezza di prodotti e servizi TIC, al

---

1 Comunicazione congiunta della Commissione europea e del Servizio europeo per l'azione esterna - "Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro" (JOIN(2013) 1 final).

2 Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

3 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

4 Comunicazione della Commissione "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" (COM(2016) 0410 final).

fine di accrescere la fiducia e la sicurezza nel mercato unico digitale. La certificazione della cibersicurezza delle TIC è particolarmente importante alla luce del maggiore utilizzo delle tecnologie che richiedono un livello elevato di sicurezza informatica, come le automobili connesse e automatizzate, la sanità elettronica e i sistemi di controllo per l'automazione industriale (IACS).

Tali misure e annunci di natura strategica sono stati ulteriormente rafforzati dalle **conclusioni del Consiglio** del 2016, che riconoscevano che "le vulnerabilità e le minacce informatiche continuano a evolversi e a intensificarsi. Ciò richiederà una cooperazione costante e più stretta, in particolare nella gestione degli incidenti transfrontalieri e su vasta scala in materia di cibersicurezza". Le conclusioni ribadivano che il regolamento ENISA costituisce uno degli "elementi centrali di un quadro dell'UE in materia di resilienza informatica"[5] e invitavano la Commissione a prendere ulteriori iniziative per affrontare la questione della certificazione a livello europeo.

L'introduzione di un sistema di certificazione richiederebbe l'istituzione di un adeguato sistema di governance a livello di UE, che dovrebbe anche comprendere una solida competenza fornita da un'agenzia dell'UE indipendente. A questo proposito, la presente proposta individua in ENISA il naturale organismo a livello dell'UE competente in materia di cibersicurezza, che dovrebbe assumere il ruolo di riunire le autorità nazionali competenti in materia di certificazione e coordinarne il lavoro.

Nella sua comunicazione sulla **revisione intermedia della strategia per il mercato unico digitale del maggio 2017**, la Commissione ha ulteriormente precisato che avrebbe rivisto il mandato dell'ENISA entro settembre 2017, per definirne il ruolo nel mutato ecosistema della cibersicurezza ed elaborare misure relative a norme tecniche, certificazioni ed etichettature in materia di sicurezza informatica, per rendere più sicuri i sistemi basati sulle TIC, oggetti connessi inclusi[6]. Le **conclusioni del Consiglio europeo** del giugno 2017[7] hanno accolto con favore l'intenzione della Commissione di riesaminare la strategia per la cibersicurezza nel mese di settembre e di proporre ulteriori azioni mirate entro la fine dell'anno.

La proposta di regolamento prevede una serie completa di misure che costituiscono lo sviluppo di precedenti azioni e promuove obiettivi specifici che si rafforzano reciprocamente:

- accrescere le **capacità e la preparazione** degli Stati membri e delle imprese;
- migliorare **la cooperazione e il coordinamento** tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE;
- aumentare **le capacità a livello dell'UE per integrare l'azione degli Stati membri**, in particolare in caso di crisi informatiche transfrontaliere.
- intensificare la **consapevolezza** di cittadini e imprese sulle questioni riguardanti la cibersicurezza;

[5] "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" - conclusioni del Consiglio del 15 novembre 2016.

[6] Comunicazione della Commissione sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale (COM/2017/0228 final).

[7] Riunione del Consiglio europeo (22 e 23 giugno 2017) – Conclusioni, EUCO 8/17.

- migliorare, in generale, la **trasparenza dell'affidabilità in termini di cibersicurezza** [8] dei prodotti e dei servizi TIC, al fine di rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale; e
- evitare la **frammentazione dei sistemi di certificazione** nell'UE e i relativi requisiti di sicurezza e criteri di valutazione nei vari Stati membri e settori di attività.

La seguente parte della relazione espone in modo più dettagliato le motivazioni dell'iniziativa per quanto riguarda le azioni proposte per l'ENISA e la certificazione della cibersicurezza.

[8] Per trasparenza dell'affidabilità in termini di cibersicurezza si intende il fatto di fornire agli utenti informazioni sufficienti sulle caratteristiche di cibersicurezza per permettere loro di stabilire oggettivamente il livello di sicurezza di un determinato prodotto, servizio o processo nel settore delle TIC.

ENISA

L'ENISA è un centro di competenze incaricato di migliorare la sicurezza delle reti e dell'informazione nell'Unione e di sostenere lo sviluppo delle capacità degli Stati membri.

L'ENISA è stata istituita nel 2004[9] per contribuire all'obiettivo generale di garantire un livello elevato di sicurezza delle reti e dell'informazione nell'ambito dell'UE. Nel 2013 il regolamento (UE) n. 526/2013 ha definito il nuovo mandato dell'Agenzia per un periodo di sette anni, fino al 2020. L'Agenzia ha sede in Grecia, e segnatamente la sede amministrativa a Heraklion (Creta) e il centro operativo ad Atene.

Rispetto alle altre agenzie dell'UE, l'ENISA è un'agenzia piccola, dotata di bilancio modesto e un organico poco numeroso e il cui mandato è a tempo determinato.

L'ENISA sostiene le istituzioni europee, gli Stati membri e le imprese **nell'affrontare, risolvere e in particolare prevenire i problemi di sicurezza delle reti e dell'informazione**. A tal fine effettua una serie di attività nei cinque settori individuati nella sua strategia[10]:

- Competenza: fornire informazioni e competenze sulle principali questioni relative alla sicurezza delle reti e dell'informazione.
- Politica: sostenere l'elaborazione e l'attuazione delle politiche dell'Unione.
- Capacità: contribuire allo sviluppo delle capacità in tutta l'Unione (ad esempio attraverso attività di formazione, raccomandazioni, attività di sensibilizzazione).
- Comunità: promuovere la comunità della sicurezza delle reti e delle informazioni (ad esempio sostegno alle squadre di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (*Computer Emergency Response Teams* - CERT), coordinamento delle esercitazioni paneuropee di cibersicurezza).
- Facilitazione: ad esempio collaborazione con i portatori d'interessi e avvio di relazioni internazionali.

Nel corso dei negoziati relativi alla direttiva NIS, i colegislatori dell'UE hanno deciso di attribuire importanti funzioni all'ENISA nell'applicazione della presente direttiva. In particolare, l'Agenzia assicura le funzioni di segretariato della rete di CSIRT (istituita per promuovere una collaborazione operativa rapida ed efficace tra Stati membri in relazione a specifici incidenti connessi alla cibersicurezza e alla condivisione delle informazioni sui rischi), ed è inoltre chiamata ad assistere il gruppo di cooperazione nell'esecuzione dei suoi compiti. Inoltre, la direttiva dispone che l'ENISA assista gli Stati membri e la Commissione mettendo loro a disposizione le proprie competenze e consulenze e agevolando lo scambio di migliori pratiche.

Conformemente al regolamento che istituisce l'ENISA, la Commissione ha proceduto a una valutazione dell'Agenzia, comprendente uno studio indipendente e una consultazione pubblica. La valutazione ha riguardato la pertinenza, l'impatto, l'efficacia, l'efficienza, la

---

9 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).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

coerenza e il valore aggiunto UE dell'Agenzia sotto il profilo delle sue prestazioni, della sua governance, dell'organizzazione interna e dei nuovi metodi di lavoro, nel corso del periodo 2013-2016.

Le prestazioni complessive dell'ENISA sono state valutate positivamente dalla maggioranza degli intervistati[11] (74%) che hanno partecipato alla consultazione pubblica. Una maggioranza di intervistati ritiene, inoltre, che l'ENISA stia realizzando i suoi diversi obiettivi (almeno il 63% per ciascuno degli obiettivi). I servizi e i prodotti dell'ENISA sono periodicamente (a cadenza mensile o più frequente) utilizzati da quasi la metà degli intervistati (46%) e sono apprezzati per la loro provenienza da un organismo a livello dell'UE (83%) e per la loro qualità (62%).

Tuttavia, la grande maggioranza (88%) degli intervistati ritiene che gli attuali strumenti e meccanismi disponibili a livello dell'UE siano insufficienti o solo parzialmente adeguati per affrontare le attuali sfide in materia di cibersicurezza. La grande maggioranza dei partecipanti (98%) è del parere che un organismo dell'UE dovrebbe tenere conto di queste esigenze, e il 99% pensa che l'ENISA sia l'organizzazione adatta a tal proposito. Inoltre, il 67,5% dei partecipanti ha espresso l'opinione che l'ENISA potesse svolgere un ruolo nella creazione di un quadro armonizzato per la certificazione della sicurezza di prodotti e servizi informatici.

La valutazione complessiva (basata non solo sulla consultazione pubblica, ma anche su una serie di interviste individuali, altre indagini mirate e seminari) ha raggiunto le seguenti conclusioni:

- gli obiettivi dell'ENISA continuano ad essere pertinenti. In un contesto di rapida evoluzione tecnologica e minacce in costante evoluzione e alla luce dei crescenti rischi di sicurezza informatica a livello mondiale, vi è una chiara necessità nell'UE di promuovere e rafforzare ulteriormente le competenze tecniche di alto livello nelle questioni riguardanti la cibersicurezza. È necessario rafforzare la capacità degli Stati membri di capire e di rispondere alle minacce e i portatori d'interessi dovranno cooperare nei vari settori tematici e a livello interistituzionale.
- Nonostante la dotazione di bilancio limitata, l'Agenzia è stata efficiente dal punto di vista operativo nell'uso delle sue risorse e nell'esecuzione dei suoi compiti. L'ubicazione suddivisa tra Atene e Heraklion, tuttavia, ha anche generato costi amministrativi supplementari.
- In termini di efficacia, l'ENISA ha parzialmente raggiunto i suoi obiettivi. L'Agenzia ha contribuito positivamente a migliorare la sicurezza delle reti e dell'informazione in Europa, sostenendo la creazione di capacità in 28 Stati membri[12], rafforzando la

11 Hanno risposto alla consultazione 90 portatori di interessi provenienti da 19 Stati membri (88 risposte e 2 documenti di sintesi), comprese le autorità nazionali di 15 Stati membri e 8 organizzazioni ombrello che rappresentano un numero significativo di imprese europee.

12 I partecipanti che hanno risposto alla consultazione pubblica sono stati invitati a formulare osservazioni sui principali risultati conseguiti - a loro giudizio - dall'ENISA nel periodo 2013-2016. Partecipanti rientranti in tutte le categorie (55 in totale, di cui 13 da autorità nazionali, 20 dal settore privato e 22 «altri») hanno ritenuto che i principali risultati conseguiti dall'ENISA fossero: 1) il coordinamento delle esercitazioni in materia di sicurezza informatica; 2) il sostegno fornito ai CERT/CSIRT attraverso azioni di formazione e seminari per promuovere lo scambio di informazioni e il coordinamento; 3) le pubblicazioni dell'ENISA (orientamenti e raccomandazioni, relazioni sugli scenari di minaccia, strategie per la segnalazione di incidenti e la gestione delle crisi, ecc.) che sono state considerate utili per creare e aggiornare i quadri nazionali in materia di sicurezza, nonché come riferimento ai responsabili politici e agli operatori nel settore della sicurezza informatica; 4) l'assistenza fornita nella

cooperazione fra gli Stati membri e i portatori d'interessi in materia di sicurezza delle reti e dell'informazione e fornendo consulenza, facilitando la creazione di comunità e sostenendo lo sviluppo delle politiche. Complessivamente, l'ENISA si è diligentemente concentrata sull'attuazione del suo programma di lavoro e ha agito da partner affidabile per i suoi portatori d'interessi, in un settore di cui solo recentemente è stata riconosciuta la forte rilevanza transfrontaliera.

- L'ENISA ha certamente influito positivamente - almeno in certa misura - sulla sicurezza delle reti e dell'informazione, ma non è pienamente riuscita ad acquisire una reputazione solida né una visibilità sufficiente per essere riconosciuta come "il" centro di competenza in Europa. La spiegazione va trovata nell'ampio mandato dell'ENISA, che non è stata dotata di risorse sufficienti in relazione ai suoi compiti. Inoltre, l'ENISA rimane l'unica agenzia dell'Unione europea con un mandato a tempo determinato, il che ne limita la capacità di elaborare una visione a lungo termine e assistere i portatori d'interessi in modo sostenibile. Tale situazione non è conforme alle disposizioni della direttiva NIS che affida a ENISA compiti senza alcuna data di scadenza. Infine, dalla valutazione emerge che tale efficacia limitata può essere in parte spiegata con la forte dipendenza dalle competenze esterne rispetto a quelle interne e con le difficoltà incontrate nel reclutare e trattenere personale specializzato.
- Da ultimo, ma non meno importante, la valutazione ha concluso che il valore aggiunto dell'ENISA risiede principalmente nella capacità dell'Agenzia di intensificare la cooperazione soprattutto tra gli Stati membri, e in particolare con le pertinenti comunità della sicurezza delle reti e dell'informazione (in particolare tra i CSIRT). Nessun altro organismo sostiene - a livello dell'UE - una comunità così ampia di portatori d'interessi nel settore della sicurezza delle reti e dell'informazione. Tuttavia, dovendo dare rigide priorità alle sue attività, il programma di lavoro dell'ENISA è per lo più orientato alle esigenze degli Stati membri. Di conseguenza, non si occupa adeguatamente delle esigenze di altri operatori, in particolare dell'industria. Il mandato ha inoltre indotto l'Agenzia a rispondere alle esigenze dei suoi principali portatori d'interessi, impedendole in tal modo di conseguire un impatto più ampio. Pertanto, il valore aggiunto fornito dall'Agenzia varia a seconda delle esigenze divergenti dei suoi portatori d'interessi e della misura in cui l'Agenzia è stata in grado di soddisfarle (ad esempio, gli Stati membri grandi vs i piccoli Stati membri, gli Stati membri vs le imprese).

In sintesi, i risultati delle consultazioni e la valutazione dei portatori d'interessi suggeriscono che le risorse e il mandato dell'ENISA devono essere adattati affinché l'Agenzia possa svolgere un ruolo adeguato per rispondere alle sfide presenti e future.

Alla luce di tali risultati, la presente proposta esamina l'attuale mandato dell'ENISA e stabilisce una serie rinnovata di compiti e funzioni al fine di sostenere, in modo efficace ed efficiente, gli sforzi degli Stati membri, delle istituzioni dell'UE e degli altri portatori d'interessi volti a garantire un ciberspazio sicuro all'interno dell'Unione europea. Il nuovo mandato proposto intende conferire all'Agenzia un ruolo più forte e centrale, in particolare anche aiutando gli Stati membri ad attuare la direttiva NIS e contrastare più attivamente le particolari minacce (capacità operativa) e diventando un centro specializzato volto a sostenere

---

promozione della sicurezza delle reti e dell'informazione; 5) gli sforzi per sensibilizzare maggiormente alla cibersicurezza attraverso il mese della sicurezza informatica.

gli Stati membri e la Commissione in materia di certificazione della cibersicurezza. Nel quadro della presente proposta:

- all'ENISA sarebbe conferito un mandato permanente e l'Agenzia disporrebbe in tal modo di una base stabile per il futuro. Il mandato, gli obiettivi e i compiti continueranno ad essere oggetto di revisione periodica.
- Il mandato proposto definisce più precisamente il ruolo dell'ENISA in quanto agenzia dell'UE per la sicurezza informatica e come punto di riferimento nell'ecosistema della cibersicurezza dell'UE, in stretta collaborazione con tutti gli altri organismi pertinenti di tale ecosistema.
- L'organizzazione e la governance dell'Agenzia, che sono state giudicate positivamente nel corso della valutazione, sarebbero leggermente rivedute, in particolare al fine di garantire che le esigenze della più ampia comunità dei portatori d'interessi siano rispecchiate più adeguatamente nei lavori dell'Agenzia.
- Il campo di applicazione proposto per il mandato è ben delineato, sono rafforzati quei settori in cui l'Agenzia ha dimostrato un chiaro valore aggiunto e sono integrati nuovi settori in cui è necessario un sostegno alla luce delle nuove priorità politiche e dei nuovi strumenti, in particolare la direttiva NIS, il riesame della strategia dell'UE per la cibersicurezza, il prossimo programma di cibersicurezza dell'UE per la cooperazione in caso di crisi informatica e la certificazione della sicurezza delle TIC:
    - **sviluppo e attuazione delle politiche dell'UE:** l'ENISA avrebbe il compito di contribuire attivamente alla formulazione della politica in materia di sicurezza delle reti e dell'informazione, nonché allo sviluppo di altre iniziative politiche che presentano elementi di cibersicurezza in diversi settori (ad esempio, energia, trasporti, finanza). A tal fine, avrebbe un forte ruolo consultivo che potrà svolgere fornendo pareri indipendenti e lavori preparatori per l'elaborazione e l'aggiornamento delle politiche e della legislazione. L'ENISA potrebbe sostenere anche la politica e la normativa dell'UE in materia di comunicazioni elettroniche, identità elettronica e servizi fiduciari, al fine di promuovere un livello più elevato di sicurezza informatica. In fase di attuazione, in particolare nel contesto del gruppo di collaborazione NIS, l'ENISA assisterebbe gli Stati membri nel conseguire un approccio coerente per l'attuazione transfrontaliera e transettoriale della direttiva NIS, nonché di altre pertinenti normative e politiche. Al fine di sostenere il riesame periodico delle politiche e delle leggi in materia di sicurezza informatica, l'ENISA approntterebbe anche relazioni periodiche sullo stato di attuazione del quadro giuridico dell'UE.
    - **Rafforzamento delle capacità:** l'ENISA contribuirebbe a migliorare le capacità e le competenze delle autorità pubbliche nazionali e dell'UE, anche in materia di risposta agli incidenti e di vigilanza delle relative misure di regolamentazione della sicurezza informatica. L'Agenzia dovrebbe inoltre contribuire alla creazione di centri di condivisione e di analisi delle informazioni (ISAC) in vari settori proponendo migliori pratiche e orientamenti sugli strumenti e le procedure disponibili, nonché affrontando in maniera adeguata le questioni regolamentari relative alla condivisione di informazioni.
    - **Condivisione di conoscenze e informazioni, sensibilizzazione:** l'ENISA diventerebbe il polo d'informazione dell'UE. Ciò implicherebbe la promozione

e la condivisione delle migliori pratiche e di iniziative in tutta l'UE, mettendo in comune le informazioni in materia di cibersicurezza provenienti dalle istituzioni, agenzie e organismi dell'UE e nazionali. L'Agenzia dovrebbe inoltre fornire consulenza, orientamenti e migliori pratiche sulla sicurezza delle infrastrutture critiche. Dopo il verificarsi di significativi incidenti informatici transfrontalieri di sicurezza, l'ENISA dovrebbe inoltre elaborare relazioni al fine di fornire orientamenti alle imprese e ai cittadini in tutta l'UE. Questo compito comporterebbe anche l'organizzazione periodica di attività di sensibilizzazione, di concerto con le autorità degli Stati membri.

- **Compiti connessi al mercato (normazione, certificazione della cibersicurezza):** l'ENISA dovrebbe svolgere una serie di compiti, segnatamente a sostegno del mercato interno e costituire un "osservatorio del mercato della cibersicurezza", analizzando le tendenze pertinenti nel mercato della sicurezza informatica per migliorare l'incontro tra domanda e offerta, e sostenendo lo sviluppo delle politiche dell'UE nei settori della normazione e della certificazione della cibersicurezza delle TIC. Per quanto riguarda la normazione, faciliterebbe la definizione e l'adozione di norme tecniche in materia di sicurezza informatica. L'ENISA dovrebbe inoltre eseguire i compiti previsti nel contesto del futuro quadro per la certificazione (cfr. infra).

- **Ricerca e innovazione:** l'ENISA dovrebbe apportare le sue conoscenze consigliando le autorità nazionali e dell'UE sulla definizione delle priorità in materia di ricerca e sviluppo, anche nel contesto dell'accordo di partenariato pubblico-privato contrattuale sulla cibersicurezza (cPPP). La consulenza dell'ENISA sulla ricerca sarebbe di sostegno al nuovo Centro europeo di ricerca e di competenza sulla cibersicurezza nell'ambito del prossimo quadro finanziario pluriennale. L'ENISA potrebbe anche essere coinvolta, su richiesta della Commissione, nell'attuazione di programmi di finanziamento dell'UE in materia di ricerca e innovazione.

- **Cooperazione operativa e gestione delle crisi:** questo filone di lavoro consisterebbe nel rafforzare le esistenti capacità operative di prevenzione, in particolare aggiornando le esercitazioni paneuropee in questo settore (Cyber Europe), che sarebbero organizzate su base annuale, e nell'assumere un ruolo di sostegno alla cooperazione operativa in veste di segretariato della rete di CSIRT (come da disposizioni della direttiva NIS), garantendo, tra l'altro, il buon funzionamento delle infrastrutture informatiche e dei canali di comunicazione della rete di CSIRT. In tale contesto, sarebbe necessario instaurare una cooperazione strutturata con la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) e altri organi competenti dell'UE. Inoltre, una cooperazione strutturata con la CERT-UE, che comporti una stretta vicinanza geografica, dovrebbe tradursi in una funzione di assistenza tecnica in caso di incidenti rilevanti e di sostegno all'analisi degli incidenti. Su loro richiesta, gli Stati membri riceverebbero assistenza nel trattamento degli incidenti e sostegno all'analisi delle vulnerabilità, degli artefatti e degli incidenti al fine di rafforzare la loro capacità di risposta e di prevenzione.

- L'ENISA svolgerebbe un ruolo anche nel **programma di cibersicurezza dell'UE**, presentato come elemento del presente pacchetto legislativo, che formula la raccomandazione della Commissione agli Stati membri per una

risposta coordinata a livello dell'UE agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala[13]. L'ENISA avrebbe il compito di facilitare la cooperazione tra i singoli Stati membri che affrontano interventi di emergenza mediante l'analisi e l'aggregazione delle relazioni nazionali sulla situazione basate su informazioni messe a disposizione dell'Agenzia, su base volontaria, dagli Stati membri e da altri soggetti.

- **Certificazione della cibersicurezza di prodotti e servizi TIC**

Per creare e preservare la fiducia e la sicurezza, i prodotti e i servizi TIC devono incorporare direttamente gli elementi di sicurezza fin dagli stadi iniziali della loro progettazione e sviluppo tecnico (sicurezza fin dalla progettazione). Inoltre, clienti e utenti devono poter conoscere il livello di affidabilità della sicurezza dei prodotti e dei servizi che utilizzano o acquistano.

La certificazione, che consiste nella valutazione formale dei prodotti, servizi e processi da parte di un organismo indipendente e accreditato rispetto a una serie definita di criteri standard e nel rilascio di un certificato di conformità, svolge un ruolo importante nel rafforzare la fiducia e la sicurezza di prodotti e servizi. Mentre le valutazioni della sicurezza riguardano gli aspetti tecnici, la certificazione serve a informare e rassicurare gli acquirenti e gli utenti in merito alle caratteristiche di sicurezza dei prodotti e servizi TIC che acquistano o utilizzano. Come già indicato, ciò è particolarmente significativo per i nuovi sistemi che fanno ampio uso delle tecnologie digitali e richiedono un livello elevato di sicurezza, come ad esempio le automobili connesse e automatizzate, la sanità elettronica, i sistemi di controllo per l'automazione industriale (IACS)[14] o le reti elettriche intelligenti.

Attualmente, il panorama della certificazione della cibersicurezza dei prodotti e dei servizi TIC nell'UE è piuttosto frammentato. Esistono diverse iniziative internazionali, quali i cosiddetti criteri comuni (CC) per la valutazione della sicurezza delle tecnologie d'informazione (ISO 15408), che costituiscono una norma tecnica internazionale per la valutazione della sicurezza informatica. Essa si basa sulla valutazione da parte di terzi e prevede sette livelli di valutazione dell'affidabilità (*Evaluation Assurance Level* - EAL). I CC e l'associata Metodologia comune per la valutazione della sicurezza delle tecnologie d'informazione (CEM) costituiscono la base tecnica per un accordo internazionale, l'Accordo di riconoscimento dei criteri comuni (CCRA), che garantisce che i certificati basati sui CC sono riconosciuti da tutti i firmatari del CCRA. Tuttavia, nell'attuale versione del CCRA godono di reciproco riconoscimento solo valutazioni fino all'EAL 2. Inoltre, solo 13 Stati membri hanno firmato l'accordo.

Le autorità di certificazione di 12 Stati membri hanno concluso un accordo di reciproco riconoscimento dei certificati rilasciati in conformità con l'accordo sulla base dei criteri

---

13 Il programma si applicherà agli incidenti connessi alla cibersicurezza dalle conseguenze negative più ampie di quanto uno Stato membro possa gestire da solo o riguardanti due o più Stati membri con un impatto talmente ampio e significativo o una rilevanza politica tale da richiedere un coordinamento e una reazione tempestiva a livello politico dell'Unione.

14 La DG JRC ha pubblicato una relazione che propone una prima serie di prescrizioni europee comuni e orientamenti di massima relativi alla certificazione in materia di cibersicurezza dei componenti degli IACS. La relazione è disponibile al seguente indirizzo: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf.

comuni[15]. Inoltre, negli Stati membri esistono o sono in corso di introduzione svariate iniziative di certificazione delle TIC. Sebbene importanti, c'è il rischio che tali iniziative provochino la frammentazione del mercato unico e problemi di interoperabilità. Di conseguenza, per poter offrire il suo prodotto in più mercati, una società può essere costretta a sottoporsi a diverse procedure di certificazione in vari Stati membri. Per esempio, il fabbricante di un contatore intelligente che intenda vendere i propri prodotti in tre Stati membri, ad esempio Germania, Francia e Regno Unito, deve attualmente conformarsi a tre diversi sistemi di certificazione: la *Commercial Product Assurance* (CPA) nel Regno Unito, la *Certification de Sécurité de Premier Niveau* in Francia (CSPN) e uno specifico profilo di protezione sulla base di criteri comuni in Germania.

Tale situazione comporta un aumento dei costi e rappresenta un considerevole onere amministrativo per le imprese che operano in più Stati membri. Benché possano variare sensibilmente a seconda del prodotto/servizio interessato, del livello di affidabilità richiesto e/o di altri componenti, i costi di certificazione tendono in generale, ad essere piuttosto elevati per le imprese. Ad esempio, per il certificato *Smart Meter Gateway* del BSI, l'istituto federale tedesco per la sicurezza informatica, il costo è superiore a 1 milione di EUR (il certificato attesta il livello più elevato di prova e di affidabilità e riguarda non solo il prodotto, ma tutta la relativa infrastruttura), mentre i costi per la certificazione dei contatori intelligenti nel Regno Unito e in Francia ammontano a circa 150 000 EUR.

I principali portatori d'interessi del settore pubblico e privato riconoscono che, in assenza di un sistema di certificazione della cibersicurezza a livello di UE, in molti casi, le imprese devono essere certificate in ciascuno Stato membro, il che genera una frammentazione del mercato. Ancor più importante è il fatto che, in mancanza di una legislazione volta all'armonizzazione nell'Unione per i prodotti e i servizi TIC, le differenze tra gli Stati membri in termini di norme tecniche e prassi per la certificazione della cibersicurezza potrebbero creare in pratica 28 distinti mercati della sicurezza nell'UE, ciascuno con propri requisiti tecnici, metodi di prova e procedure di certificazione della cibersicurezza. Tali approcci divergenti a livello nazionale sono tali da provocare – in mancanza di misure adeguate a livello UE – un notevole passo indietro nella realizzazione del mercato unico digitale, rallentando o prevenendo gli effetti positivi connessi in termini di crescita e di occupazione.

Sulla base di quanto precede, la proposta di regolamento istituisce un quadro europeo di certificazione della cibersicurezza (il "**quadro**") per i prodotti e i servizi TIC e precisa le funzioni essenziali e i compiti dell'ENISA nel settore della certificazione della cibersicurezza. La presente proposta introduce un quadro complessivo di regole che disciplinano i sistemi europei di certificazione della cibersicurezza. La proposta non istituisce sistemi di certificazione direttamente operativi, ma crea piuttosto un "quadro" per l'istituzione di specifici sistemi di certificazione per determinati prodotti/servizi TIC ("sistemi europei di certificazione della cibersicurezza"). La creazione di sistemi di certificazione della cibersicurezza conformi al quadro generale significherà che i certificati rilasciati nell'ambito di tali sistemi saranno validi e riconosciuti in tutti gli Stati membri e permetterà di affrontare l'attuale frammentazione del mercato.

---

[15] Il Gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (SOG-IS) comprende 12 Stati membri, più la Norvegia, e ha messo a punto alcuni profili di protezione su un numero limitato di prodotti, quali la firma digitale, il tachigrafo digitale e le smart card. I partecipanti lavorano insieme per coordinare la normazione dei profili di protezione basati sui CC e coordinarne lo sviluppo. Gli Stati membri spesso fanno richiesta della certificazione rilasciata dal SOG-IS per gare di appalto pubbliche nazionali.

L'obiettivo generale di un sistema europeo di certificazione della cibersicurezza è di attestare che i prodotti e servizi TIC certificati sulla base di tale sistema rispettano precisi requisiti di sicurezza informatica. Si potrebbe trattare, ad esempio, della loro capacità di protezione dei dati (dati memorizzati, trasmessi o altrimenti trattati) dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati e dalla distruzione e dalla perdita accidentale o dall'alterazione. I sistemi di certificazione della cibersicurezza dell'UE farebbero riferimento alle norme tecniche esistenti in relazione ai requisiti tecnici e alle procedure di valutazione che i prodotti devono rispettare e non svilupperebbero proprie norme tecniche[16]. Ad esempio, una certificazione a livello UE per i prodotti quali le "smart card", che attualmente viene verificata rispetto alle norme tecniche internazionali in materia di CC nell'ambito del sistema multilaterale SOG-IS (sopra descritto), renderebbe tale regime valido in tutta l'UE.

Oltre a definire una serie specifica di obiettivi di sicurezza da prendere in considerazione all'atto della progettazione di uno specifico sistema europeo di certificazione della cibersicurezza, la proposta dispone quale debba essere il contenuto minimo di tali sistemi. Essi dovranno definire, tra l'altro, una serie di elementi specifici che stabiliscono il campo di applicazione e l'oggetto della certificazione della cibersicurezza. Ciò include l'identificazione delle categorie di prodotti e servizi contemplati, l'indicazione dettagliata dei requisiti di sicurezza informatica (ad esempio con riferimento alle pertinenti norme o specifiche tecniche), i criteri e i metodi di valutazione specifici e il livello di affidabilità che intendono assicurare (ossia: di base, significativo o elevato).

I sistemi europei di certificazione della cibersicurezza saranno preparati dall'ENISA, con l'assistenza, la consulenza e la stretta collaborazione del Gruppo europeo per la certificazione della cibersicurezza (cfr. infra) e adottati dalla Commissione mediante atti di esecuzione. Quando sia rilevata la necessità di un sistema di certificazione della cibersicurezza, la Commissione chiederà all'ENISA di predisporre un sistema per specifici prodotti o servizi TIC. L'ENISA lavorerà a tal fine di concerto con le autorità nazionali di controllo della certificazione rappresentate in seno al gruppo. Gli Stati membri e il gruppo possono suggerire alla Commissione di chiedere all'ENISA di preparare un sistema particolare.

La certificazione può rivelarsi un processo molto costoso, con un possibile conseguente aumento dei prezzi per i clienti e i consumatori. La necessità di certificazione può anche variare significativamente a seconda del contesto specifico di uso dei prodotti e dei servizi e del rapido ritmo dell'evoluzione tecnologica. Il ricorso alla certificazione europea della cibersicurezza dovrebbe pertanto avere carattere facoltativo, salvo se altrimenti previsto nella legislazione dell'Unione che stabilisce requisiti di sicurezza dei prodotti e servizi TIC.

Al fine di garantire l'armonizzazione ed evitare la frammentazione, le procedure o i sistemi nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza cesseranno di applicarsi a decorrere dalla data stabilita nell'atto di esecuzione che adotta il sistema. Gli Stati membri dovrebbero inoltre astenersi dall'introdurre nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza.

Una volta adottato un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i prestatori di servizi TIC potranno presentare domanda di certificazione per i

[16] Nel caso di norme tecniche europee, tale verifica è effettuata dalle organizzazioni europee di normazione e approvata dalla Commissione europea mediante pubblicazione nella *Gazzetta ufficiale* (cfr. regolamento n. 1025/2012).

rispettivi prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Detti organismi di valutazione della conformità dovranno essere accreditati da un organismo di accreditamento se soddisfano determinati requisiti. L'accreditamento è concesso per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento revocano l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

In base alla proposta, i compiti di controllo, di vigilanza e di esecuzione spettano agli Stati membri. Gli Stati membri dovranno prevedere un'autorità di controllo della certificazione. L'autorità in questione è incaricata di vigilare sulla conformità degli organismi di valutazione della conformità, così come dei certificati rilasciati da organismi di valutazione della conformità stabiliti nel loro territorio, rispetto ai requisiti stabiliti dal presente regolamento e ai pertinenti sistemi europei di certificazione della cibersicurezza. Le autorità nazionali di controllo della certificazione saranno competenti a trattare i reclami presentati da persone fisiche o giuridiche in relazione ai certificati rilasciati da organismi di valutazione della conformità stabiliti nel loro territorio. Esse esamineranno - nella misura opportuna - l'oggetto del reclamo e informeranno il reclamante dei progressi e dell'esito del loro esame entro un periodo di tempo ragionevole. Inoltre, coopereranno con altre autorità di controllo della certificazione o altre autorità pubbliche, ad esempio mediante lo scambio di informazioni su eventuali casi di non conformità dei prodotti e dei servizi TIC con le disposizioni del presente regolamento o con specifici sistemi europei di certificazione della cibersicurezza.

Infine, la proposta istituisce il Gruppo europeo per la certificazione della cibersicurezza (in seguito: il "gruppo"), che sarà composto da autorità nazionali di controllo della certificazione di tutti gli Stati membri. Il principale compito del gruppo è consigliare la Commissione sulle questioni concernenti la politica di certificazione della cibersicurezza e collaborare con l'ENISA per lo sviluppo di progetti di sistemi europei di certificazione della cibersicurezza. L'ENISA assisterà la Commissione assicurando il segretariato del gruppo e tenendo aggiornato un inventario pubblico dei sistemi approvati nell'ambito del quadro europeo di certificazione della cibersicurezza. L'ENISA manterrà contatti con gli organismi di normazione per garantire che le norme tecniche applicate nell'ambito dei sistemi approvati siano adeguate e per individuare le aree che necessitano di norme tecniche in materia di sicurezza informatica.

Il quadro europeo di certificazione della cibersicurezza ("quadro") offrirà diversi vantaggi ai cittadini e alle imprese. In particolare:

- La creazione di sistemi di certificazione della cibersicurezza di specifici prodotti o servizi a livello dell'UE fornirà uno "sportello unico" alle imprese per la certificazione della cibersicurezza nell'UE. Tali imprese potranno certificare i loro prodotti una sola volta e ottenere un certificato valido in tutti gli Stati membri. Non saranno tenuti a certificare nuovamente i loro prodotti presso diversi organismi nazionali di certificazione. Ciò consentirà di ridurre notevolmente i costi per le imprese, facilitare le operazioni transfrontaliere e, in ultima analisi, ridurre ed evitare la frammentazione del mercato interno per quanto riguarda i prodotti in questione.
- Il quadro stabilisce che i sistemi europei di certificazione della cibersicurezza prevalgono sui sistemi nazionali: in base a tale norma, l'adozione di un sistema europeo di certificazione della cibersicurezza sostituisce tutti gli attuali sistemi nazionali paralleli per gli stessi prodotti o servizi TIC a un dato livello di affidabilità.

Ciò apporterà maggiore chiarezza, riducendo l'attuale proliferazione di sistemi nazionali di certificazione della cibersicurezza che si sovrappongono e sono a volte contraddittori.

- La proposta sostiene e integra l'attuazione della direttiva NIS, dotando le imprese che ne sono soggette di uno strumento molto utile per dimostrare la conformità con le disposizioni di detta direttiva in tutta l'Unione. Nello sviluppo di nuovi sistemi di certificazione della cibersicurezza, l'ENISA e la Commissione continueranno a prestare particolare attenzione alla necessità di garantire che le disposizioni della direttiva NIS trovino riscontro nei sistemi di certificazione della cibersicurezza.
- La proposta mira a sostenere e agevolare lo sviluppo di una politica europea in materia di sicurezza informatica, armonizzando le condizioni e i requisiti sostanziali per la certificazione della cibersicurezza dei prodotti e dei servizi TIC nell'UE. I sistemi europei di certificazione della cibersicurezza faranno riferimento a norme tecniche o criteri di valutazione e metodologie di prova comuni. Ciò contribuirà in misura significativa, sia pure indiretta, all'adozione di soluzioni comuni in materia di sicurezza nell'UE, contribuendo altresì a rimuovere gli ostacoli al mercato interno.
- Il quadro è concepito in modo tale da assicurare la necessaria flessibilità per la cibersicurezza dei sistemi di certificazione. A seconda delle specifiche necessità di cibersicurezza, un prodotto o un servizio può essere certificato ad un livello più o meno elevato di sicurezza. I sistemi europei di certificazione della cibersicurezza saranno progettati tenendo in mente tale flessibilità e garantiranno quindi diversi livelli di affidabilità (ossia di base, sostanziale o elevato), in modo da poter essere utilizzati per scopi differenti o in contesti diversi.
- Tutti questi elementi renderanno più attraente la certificazione della cibersicurezza per le imprese come efficace strumento per comunicare il livello di affidabilità della cibersicurezza di prodotti o servizi TIC. Man mano che la certificazione della cibersicurezza diventerà meno costosa, più efficace e più interessante dal punto di vista commerciale, le imprese avranno maggiori incentivi a certificare i loro prodotti contro i rischi relativi alla cibersicurezza, contribuendo in tal modo alla diffusione delle migliori pratiche in materia di sicurezza informatica nella progettazione di prodotti e servizi TIC (cibersicurezza fin dalla progettazione).

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

A norma della direttiva NIS, gli operatori dei settori che sono fondamentali per la nostra economia e la nostra società, quali l'energia, i trasporti, l'acqua, i servizi bancari, le infrastrutture dei mercati finanziari, l'assistenza sanitaria e le infrastrutture digitali, così come i fornitori di servizi digitali (ad esempio, i motori di ricerca, i servizi di *cloud computing* e i mercati online) sono tenuti a prendere misure per gestire adeguatamente i rischi di sicurezza. Le nuove disposizioni della presente proposta integrano – assicurandone la coerenza – le disposizioni della direttiva NIS, al fine di conseguire una maggiore resilienza informatica dell'UE attraverso un più alto livello di capacità, cooperazione, sensibilizzazione e gestione dei rischi informatici.

Inoltre, le norme in materia di certificazione della cibersicurezza costituiscono uno strumento essenziale per le imprese soggette alla direttiva NIS, che potranno certificare i loro prodotti e servizi TIC contro i rischi relativi alla cibersicurezza sulla base di sistemi di certificazione della cibersicurezza validi e riconosciuti in tutta l'UE. Esse saranno inoltre complementari ai

requisiti di sicurezza di cui al regolamento eIDAS[17] e alla direttiva sulle apparecchiature radio[18].

- **Coerenza con le altre normative dell'Unione**

Il regolamento (UE) 2016/679 (il regolamento generale sulla protezione dei dati, "**RGPD**")[19] stabilisce le disposizioni volte a predisporre meccanismi di certificazione e sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti dei dati da parte di responsabili del trattamento e incaricati del trattamento. Il presente regolamento si applica fatta salva la certificazione delle operazioni di trattamento dei dati, anche nel caso in cui tali operazioni siano incorporate nei prodotti e servizi, a norma del regolamento generale sulla protezione dei dati.

Il regolamento proposto garantirà la compatibilità con il regolamento (CE) n. 765/2008 relativo all'accreditamento e alla vigilanza del mercato[20], facendo riferimento alle norme di tale quadro normativo per gli organismi nazionali di accreditamento e gli organismi di valutazione della conformità. Per quanto riguarda le autorità di controllo, il regolamento proposto impone agli Stati membri di designare autorità nazionali di controllo della certificazione con responsabilità in materia di vigilanza, monitoraggio e applicazione delle norme. Tali organismi continueranno a essere distinti dagli organismi di valutazione della conformità, secondo quanto prescritto dal regolamento (CE) n. 765/2008.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La base giuridica per l'azione dell'UE è l'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che concerne il ravvicinamento delle legislazioni degli Stati membri al fine di conseguire gli obiettivi dell'articolo 26 TFUE, ossia il corretto funzionamento del mercato interno.

La base giuridica del mercato interno, su cui si fonda l'istituzione dell'ENISA, è stata confermata dalla Corte di giustizia nella causa C-217/04 (*Regno Unito/Parlamento europeo e Consiglio*) ed è stata ulteriormente confermata dal regolamento del 2013 che stabilisce il mandato attuale dell'Agenzia. Inoltre, le attività intese a conseguire gli obiettivi di intensificare la cooperazione e il coordinamento tra gli Stati membri e quelli che aggiungono capacità a livello dell'UE per integrare l'azione degli Stati membri rientrano nella categoria della "cooperazione operativa". Questo aspetto è specificamente individuato dalla direttiva NIS (la cui base giuridica è l'articolo 114 del TFUE) come obiettivo da perseguire nel quadro della rete di CSIRT di cui "l'ENISA assicura il segretariato e sostiene attivamente la

---

17 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

18 Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE.

19 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

20 Regolamento (CE) n. 765/2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

cooperazione" (articolo 12, paragrafo 2). In particolare, l'articolo 12, paragrafo 3, lettera f), individua ulteriori forme di cooperazione operativa come compito della rete di CSIRT, anche in relazione a: i) categorie di rischi e di incidenti; ii) preallarmi; iii) assistenza reciproca; e iv) principi e modalità di coordinamento, quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri.

- L'attuale frammentazione dei sistemi di certificazione per i prodotti e i servizi TIC risulta anche dall'assenza di un quadro comune giuridicamente vincolante e di un efficace processo applicabile a tutti gli Stati membri. Ciò impedisce la creazione di un mercato interno per i prodotti e i servizi TIC e ostacola la competitività dell'industria europea in questo settore. La presente proposta mira ad affrontare l'attuale frammentazione e i relativi ostacoli al mercato interno creando un quadro comune per la creazione di sistemi di certificazione della cibersicurezza, validi in tutta l'UE.

Sussidiarietà (per la competenza non esclusiva)

Il principio di sussidiarietà impone di valutare la necessità e il valore aggiunto dell'azione dell'UE. Il rispetto del principio di sussidiarietà in questo settore è già stato riconosciuto all'atto dell'adozione dell'attuale regolamento ENISA[21].

La sicurezza informatica è una questione di interesse comune dell'Unione. Le interdipendenze tra le reti e i sistemi di informazione sono tali che i singoli soggetti (pubblici e privati, compresi i cittadini) molto spesso non possono affrontare le minacce, la gestione dei rischi e le possibili conseguenze degli incidenti informatici in modo isolato. Da un lato, le interdipendenze in tutti gli Stati membri, anche per quanto riguarda il funzionamento delle infrastrutture critiche (energia, trasporti, risorse idriche, solo per citarne alcune) rendono l'intervento pubblico a livello europeo non soltanto utile, ma anche necessario. Dall'altro, l'intervento dell'UE può apportare un positivo effetto di ricaduta dovuto alla condivisione di buone pratiche tra gli Stati membri, il che può tradursi in una maggiore sicurezza informatica dell'Unione.

In sintesi, nel contesto attuale e guardando al futuro, sembra che per **aumentare la ciberresilienza collettiva** dell'Unione non saranno sufficienti le **azioni individuali da parte degli Stati membri dell'UE e un approccio frammentario alla sicurezza informatica**.

L'azione dell'UE è ritenuta necessaria anche per affrontare la frammentazione degli attuali sistemi di certificazione della cibersicurezza. Ciò consentirebbe ai fabbricanti di beneficiare pienamente di un mercato interno, con significativi risparmi per quanto riguarda le prove e i costi di riprogettazione. L'attuale accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi d'informazione (SOG-IS) ha, ad esempio, conseguito risultati importanti in questo senso, ma ha anche messo in evidenza importanti limiti che ne ostacolano la capacità di fornire soluzioni sostenibili a lungo termine per realizzare il pieno potenziale del mercato interno.

Il valore aggiunto dell'azione a livello dell'Unione, in particolare al fine di migliorare la cooperazione tra gli Stati membri, ma anche tra le comunità della sicurezza delle reti e

[21] Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

dell'informazione, è stato riconosciuto nelle conclusioni del Consiglio[22] del 2016 e si evince anche chiaramente dalla valutazione dell'ENISA.

- **Proporzionalità**

La misura proposta non va al di là di quanto è strettamente necessario per raggiungere i suoi obiettivi politici. Inoltre, la portata dell'intervento dell'UE non osta a ulteriori azioni nazionali in materia di questioni di sicurezza nazionale. L'azione dell'UE è pertanto giustificata in termini di sussidiarietà e proporzionalità.

- **Scelta dell'atto giuridico**

La presente proposta rivede il regolamento (UE) n. 526/2013 che stabilisce l'attuale mandato e i compiti dell'ENISA. Inoltre, dato il ruolo importante dell'ENISA nella creazione e gestione di un quadro di certificazione della cibersicurezza dell'UE, è opportuno che il suo nuovo mandato e il citato quadro siano istituiti nell'ambito di un unico strumento giuridico, segnatamente lo strumento del regolamento.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

Valutazioni ex post/Vaglio di adeguatezza della legislazione vigente

Sulla base della tabella di marcia per la valutazione[23], la Commissione ha esaminato **la pertinenza, l'impatto, l'efficacia, l'efficienza, la coerenza e il valore aggiunto** dell'Agenzia sotto il profilo delle sue prestazioni, della governance, dell'organizzazione interna e dei nuovi metodi di lavoro, nel corso del periodo 2013-2016. I risultati principali possono essere riassunti come segue (per maggiori informazioni cfr. il pertinente documento di lavoro dei servizi della Commissione, che accompagna la valutazione d'impatto).

- **Pertinenza:** in un contesto di sviluppi tecnologici e di evoluzione delle minacce e tenendo conto del forte bisogno di maggiore sicurezza informatica nell'UE, gli obiettivi dell'ENISA si rivelano pertinenti. In effetti, gli Stati membri e gli organismi dell'UE si affidano alla sua notevole competenza in materia di cibersicurezza. È necessario inoltre rafforzare la capacità degli Stati membri di capire e di rispondere meglio alle minacce e i portatori d'interessi dovranno cooperare nei vari settori tematici e a livello interistituzionale. La sicurezza informatica continua ad essere una priorità politica fondamentale dell'UE alla quale l'ENISA dovrebbe far fronte; tuttavia, l'istituzione dell'ENISA come agenzia dell'Unione europea con un mandato a tempo determinato: i) non consente una pianificazione sostenibile e a lungo termine dell'assistenza da fornire agli Stati membri e alle istituzioni dell'UE; ii) può portare a una situazione di vuoto giuridico, in quanto le disposizioni della direttiva NIS affidano all'ENISA compiti di natura permanente[24]; iii) non è coerente con una concezione che colleghi l'ENISA a un ecosistema di cibersicurezza dell'UE.

---

22 "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" – conclusioni del Consiglio del 15 novembre 2016.

23 http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

24 Riferimento agli articoli 7, 9, 11, 12 e 19 della direttiva sulla sicurezza delle reti e dell'informazione (direttiva NIS).

- **Efficacia**: l'ENISA ha complessivamente raggiunto i propri obiettivi e attuato i propri compiti. L'Agenzia ha contribuito alla maggiore sicurezza delle reti e dell'informazione in Europa svolgendo le sue attività principali (sviluppo delle capacità, messa a disposizione di competenze, creazione di comunità e sostegno alle politiche). Tuttavia, in ciascuna di tali attività si sono ravvisati margini di miglioramento. Dalla valutazione emerge che l'ENISA ha di fatto creato forti relazioni basate sulla fiducia con alcuni dei portatori d'interessi, in particolare con gli Stati membri e le comunità di CSIRT. Gli interventi nell'ambito del potenziamento delle capacità sono stati considerati efficaci, in particolare per gli Stati membri dotati di minori risorse. Le azioni volte a stimolare un'ampia cooperazione sono state uno dei punti salienti, e i portatori d'interessi concordano maggioritariamente sul ruolo positivo che l'ENISA svolge nel mettere in contatto le persone. Tuttavia, l'ENISA ha incontrato difficoltà a conseguire un impatto significativo nel vasto campo della sicurezza delle reti e dell'informazione, anche a causa della disponibilità alquanto limitata di risorse umane e finanziarie a fronte di un mandato molto ampio. La valutazione ha inoltre concluso che l'ENISA ha parzialmente soddisfatto l'obiettivo di apportare competenze specializzate, risultato collegato alla difficoltà di reclutare esperti (cfr. anche il paragrafo relativo all'efficienza).
- **Efficienza**: nonostante la sua limitata dotazione di bilancio – tra le più modeste se confrontata ad altre agenzie dell'UE – l'Agenzia è riuscita a contribuire a obiettivi mirati, dimostrando un'efficienza generale nell'uso delle sue risorse. La valutazione ha concluso che i processi erano complessivamente efficienti e una chiara definizione delle responsabilità all'interno dell'organizzazione ha portato a una buona esecuzione dei lavori. Una delle sfide principali sotto il profilo dell'efficacia dell'Agenzia riguarda la difficoltà dell'ENISA a reclutare e trattenere esperti altamente qualificati. Secondo le conclusioni, ciò può essere spiegato con una combinazione di fattori, tra cui la difficoltà di ordine generale in tutto il settore pubblico a competere con il settore privato nel tentativo di assumere esperti altamente specializzati, il tipo di contratto (a tempo determinato) che l'Agenzia poteva per lo più offrire e il livello piuttosto modesto di attrattiva collegato alla sede dell'ENISA, ad esempio a motivo della difficoltà di trovare lavoro dei coniugi. Una sede suddivisa tra Atene e Heraklion ha richiesto sforzi supplementari di coordinamento e ha generato costi aggiuntivi, ma il trasferimento ad Atene, nel 2013, del centro operativo ha aumentato l'efficienza operativa dell'Agenzia.
- **Coerenza**: le attività dell'ENISA sono state generalmente coerenti con le politiche e le attività dei suoi portatori d'interessi, a livello nazionale e dell'Unione europea, ma è necessario adottare un approccio più coordinato alla sicurezza informatica a livello dell'UE. Il potenziale di cooperazione tra l'ENISA e gli altri organismi dell'Unione europea non è stato interamente sfruttato. L'evoluzione del quadro giuridico e dello scenario politico dell'UE rende oggi l'attuale mandato meno coerente.
- **Valore aggiunto europeo**: il valore aggiunto dell'ENISA consiste principalmente nella capacità dell'Agenzia di rafforzare la cooperazione, soprattutto tra gli Stati membri, ma anche con le comunità della sicurezza delle reti e dell'informazione. Nessun altro organismo sostiene – a livello dell'UE – la cooperazione di una comunità così ampia di portatori d'interessi nel settore della sicurezza delle reti e dell'informazione. Il valore aggiunto offerto dall'Agenzia varia in funzione delle diverse esigenze e risorse dei suoi portatori d'interessi (ad esempio, grandi e piccoli Stati membri; Stati membri e imprese) e della necessità dell'Agenzia di dare priorità alle sue attività in base al programma di lavoro. La valutazione ha concluso che

un'eventuale chiusura dell'ENISA sarebbe un'occasione persa per tutti gli Stati membri, poiché non sarebbe più possibile garantire il medesimo livello di creazione di comunità e di cooperazione tra gli Stati membri nel settore della sicurezza informatica. Senza un'agenzia dell'UE centralizzata, il quadro sarebbe più frammentato e il vuoto lasciato dall'ENISA sarebbe progressivamente colmato da forme di cooperazione bilaterale o regionale.

Per quanto riguarda specificamente le azioni passate e future dell'ENISA, le principali tendenze che emergono dalla consultazione del 2017 sono le seguenti[25]:

- Le prestazioni complessive dell'ENISA nel periodo dal 2013 al 2016 sono state valutate positivamente dalla maggioranza degli intervistati (74%). Una maggioranza di intervistati ritiene, inoltre, che l'ENISA stia realizzando i suoi diversi obiettivi (almeno il 63% per ciascuno degli obiettivi). I servizi e i prodotti dell'ENISA sono periodicamente (a cadenza mensile o più frequente) utilizzati da quasi la metà degli intervistati (46%) e sono apprezzati per il fatto che provengono da un organismo a livello dell'UE (83%) e per la loro qualità (62%).
- Gli intervistati hanno messo in luce una serie di carenze e sfide per il futuro della sicurezza informatica nell'UE, in particolare le cinque principali (in un elenco che ne comprendeva 16) sono state le seguenti: la cooperazione tra gli Stati membri; la capacità di prevenire, individuare e risolvere gli attacchi informatici su larga scala; la cooperazione tra gli Stati membri nelle questioni relative alla sicurezza informatica; la cooperazione e lo scambio di informazioni tra i diversi portatori d'interessi, compresa la cooperazione pubblico-privato; la protezione delle infrastrutture critiche dagli attacchi informatici.
- La grande maggioranza (88%) degli intervistati ritiene che gli attuali strumenti e meccanismi disponibili a livello dell'UE siano insufficienti o solo parzialmente adeguati per affrontare tali sfide. Il 98% dei partecipanti ritiene che un organismo dell'UE dovrebbe soddisfare queste esigenze, e il 99% reputa che l'ENISA sia l'organizzazione giusta a tale proposito.

Consultazioni dei portatori di interessi

- La Commissione ha organizzato una consultazione pubblica per la revisione dell'ENISA tra il 12 aprile e il 5 luglio 2016 e ha ricevuto 421 risposte[26]. In base ai risultati, il 67,5% dei partecipanti ha espresso l'opinione che l'ENISA potesse svolgere un ruolo nella creazione di un quadro armonizzato per la certificazione della sicurezza di prodotti e servizi informatici.

---

25 Hanno risposto alla consultazione 90 portatori di interessi provenienti da 19 Stati membri (88 risposte e 2 documenti di sintesi), comprese le autorità nazionali di 15 Stati membri, tra cui Francia, Italia, Irlanda e Grecia, e 8 organizzazioni ombrello che rappresentano un numero significativo di organizzazioni europee, ad esempio la Federazione bancaria europea, *Digital Europe* (che rappresenta il settore della tecnologia digitale in Europa), *European Telecommunications Network Operators' Association* (ETNO). La consultazione pubblica dell'ENISA è stata integrata da numerose altre fonti, compresi: i) interviste approfondite con circa 50 soggetti chiave nella comunità della cibersicurezza; ii) sondaggi effettuati nei confronti della rete di CSIRT; iii) sondaggi effettuati nei confronti del consiglio di amministrazione dell'ENISA, del comitato esecutivo, del gruppo permanente di parti interessate.

26 Sono pervenuti 162 contributi da cittadini, 33 dalla società civile e dalle organizzazioni dei consumatori; 186 dal settore e 40 dalle autorità pubbliche, comprese le competenti autorità responsabili dell'applicazione della direttiva sulla vita privata elettronica.

I risultati della consultazione sul cPPP[27] sulla cibersicurezza del 2016 concernente la sezione sulla certificazione mostrano che:

- il 50,4% (121 su 240) dei partecipanti ha risposto di non sapere se i sistemi di certificazione nazionali sono reciprocamente riconosciuti in tutti gli Stati membri dell'UE. Il 25,8% (62 su 240) ha risposto "No", mentre il 23,8% (57 su 240) ha risposto "Sì".
- Il 37,9% dei partecipanti (91 su 240) ritiene che i sistemi di certificazione esistenti non soddisfano le esigenze dell'industria europea. Per contro, il 17,5% (42 su 240) – soprattutto imprese globali che operano sul mercato europeo – ha espresso parere opposto.
- Il 49,6% (119 su 240) degli intervistati afferma che non è facile dimostrare l'equivalenza tra le norme tecniche, i sistemi di certificazione e le etichette. Il 37,9% (91 su 240) ha risposto "Non so", mentre il 12,5% (30 su 240) ha risposto "Sì".

Assunzione e uso di perizie

La Commissione si è basata sulle seguenti consulenze.

- Studio sulla valutazione dell'ENISA (Ramboll/Carsa 2017; n. SMART 2016/0077);
- Studio sulla certificazione della sicurezza ed etichettatura delle TIC – Raccolta di elementi di prova e valutazione d'impatto (PriceWaterhouseCoopers 2017; n. SMART 2016/0029).

Valutazione d'impatto

- La relazione sulla valutazione d'impatto di questa iniziativa ha individuato i seguenti principali problemi:
- frammentazione delle politiche e degli approcci alla cibersicurezza in tutti gli Stati membri;
- dispersione di risorse e frammentazione degli approcci alla cibersicurezza tra istituzioni, agenzie e organismi dell'UE; e
- insufficiente consapevolezza e informazione dei cittadini e delle imprese, insieme con la crescente diffusione di molteplici sistemi di certificazione nazionali e settoriali.

La relazione ha valutato le seguenti opzioni per quanto riguarda il mandato dell'ENISA:

- il mantenimento dello status quo, vale a dire la proroga di un mandato ancora limitato nel tempo (opzione di base);
- il termine dell'attuale mandato dell'ENISA senza rinnovo e la chiusura dell'ENISA (nessun intervento);
- una "ENISA riformata"; e
- un'agenzia per la sicurezza informatica dell'UE dotata di piena capacità operativa.

[27] Hanno risposto alla sezione relativa alla certificazione 240 portatori di interessi provenienti da amministrazioni pubbliche nazionali, grandi imprese, PMI, microimprese e organismi di ricerca..

La relazione ha valutato le seguenti opzioni per quanto riguarda la certificazione della cibersicurezza:

- nessun intervento (opzione di base);
- misure non legislative (non vincolanti);
- un atto legislativo dell'UE volto a instaurare un sistema obbligatorio per tutti gli Stati membri sulla base del sistema SOG-IS; e
- un quadro generale di certificazione della cibersicurezza delle TIC.

L'analisi ha portato alla conclusione che una "ENISA riformata" in combinazione con un quadro generale di certificazione della cibersicurezza dell'UE nel settore delle TIC è l'opzione prescelta.

L'opzione prescelta è stata considerata la più efficace per raggiungere gli obiettivi individuati dall'UE: aumentare le capacità di cibersicurezza, la preparazione, la cooperazione, la consapevolezza e la trasparenza ed evitare la frammentazione del mercato. È stata anche ritenuta l'opzione più coerente con le priorità della strategia dell'Unione europea per la cibersicurezza e le relative politiche (ad esempio la direttiva NIS) e la strategia per il mercato unico digitale. Inoltre, dal processo di consultazione è emerso che l'opzione prescelta gode del sostegno della maggioranza dei portatori d'interessi. L'analisi svolta nella valutazione d'impatto ha anche dimostrato che l'opzione prescelta permetterebbe di conseguire gli obiettivi con un impiego ragionevole di risorse.

Il comitato per il controllo normativo della Commissione aveva inizialmente espresso parere negativo il 24 luglio, e poi un parere positivo il 25 agosto 2017 a seguito della presentazione di una nuova valutazione. La relazione sulla valutazione d'impatto riportava ulteriori prove a sostegno, le conclusioni finali della valutazione dell'ENISA e precisazioni supplementari sulle opzioni politiche e il loro impatto. L'allegato 1 della relazione finale sulla valutazione d'impatto riassume in che modo sono state affrontate le osservazioni espresse dal consiglio di amministrazione nel secondo parere. In particolare, la relazione è stata aggiornata per presentare in modo più dettagliato il contesto della cibersicurezza dell'UE, comprese le misure che figurano nella comunicazione congiunta dal titolo "Resilienza, difesa e deterrenza: verso una cibersicurezza forte per l'UE" (JOIN(2017) 450), e che hanno un ruolo importante per l'ENISA: il programma di cibersicurezza dell'UE e il centro europeo di ricerca e di competenza sulla cibersicurezza, al quale l'Agenzia fornirebbe consulenza circa le esigenze di ricerca dell'UE.

La relazione illustra in che modo la riforma dell'Agenzia, compresi i nuovi compiti, le migliori condizioni di lavoro e la struttura di cooperazione con gli organismi dell'UE nel settore, potrebbe migliorare la propria attrattiva come datore di lavoro e contribuirebbe ad affrontare i problemi connessi all'assunzione di esperti. L'allegato 6 della relazione presenta inoltre una nuova stima dei costi connessi alle opzioni strategiche per l'ENISA. Per quanto riguarda il tema della certificazione, la relazione è stata modificata per fornire una spiegazione più dettagliata, compresa la presentazione grafica, dell'opzione prescelta, così come stime dei costi sostenuti dagli Stati membri e dalla Commissione in relazione al nuovo quadro di certificazione. Le motivazioni per la scelta dell'ENISA come soggetto fondamentale nel quadro sono state ulteriormente spiegate sulla base della sua competenza nel settore e del fatto che è la sola agenzia a livello dell'UE in materia di sicurezza informatica. Infine, le sezioni riguardanti la certificazione sono state rivedute per chiarire gli aspetti relativi alla differenza tra l'attuale sistema SOG-IS e i benefici connessi alle diverse opzioni e per precisare che il tipo di prodotti e servizi TIC contemplati da un sistema europeo di certificazione sarà definito dal sistema stesso.

Efficienza normativa e semplificazione

Non applicabile

Impatto sui diritti fondamentali

La sicurezza informatica svolge un ruolo fondamentale nel proteggere la vita privata e i dati personali dei cittadini conformemente agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In caso di incidenti informatici la vita privata e la protezione dei dati personali sono chiaramente esposti. La sicurezza informatica è pertanto una condizione necessaria per il rispetto della vita privata e della riservatezza dei dati personali. In tale prospettiva, nell'obiettivo di rafforzare la sicurezza informatica in Europa, la proposta prevede un importante complemento della legislazione vigente a tutela del diritto fondamentale al rispetto della vita privata e dei dati personali. La sicurezza informatica è anche fondamentale per tutelare la riservatezza delle nostre comunicazioni elettroniche e, pertanto, per l'esercizio della libertà di espressione e di informazione, e di altri diritti correlati, quali la libertà di pensiero, di coscienza e di religione.

4. INCIDENZA SUL BILANCIO

Cfr. scheda finanziaria

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La Commissione monitorerà l'applicazione del regolamento e ogni cinque anni presenterà una relazione di valutazione al Parlamento europeo, al Consiglio e al Comitato economico e sociale. Queste relazioni saranno rese pubbliche e illustreranno in dettaglio l'effettiva applicazione del regolamento.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

Il titolo I del regolamento contiene le disposizioni generali: l'oggetto (articolo 1), le definizioni (articolo 2), compresi i riferimenti alle pertinenti definizioni provenienti da altri strumenti dell'UE, come la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS), il regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93, e il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio sulla normazione europea.

Il titolo II del regolamento contiene le disposizioni fondamentali relative all'ENISA, l'Agenzia dell'UE per la cibersicurezza.

Il capo I di tale titolo illustra il mandato (articolo 3), gli obiettivi (articolo 4) e i compiti dell'Agenzia (articoli da 5 a 11).

Il capo II illustra l'organizzazione dell'ENISA e comprende disposizioni fondamentali sulla sua struttura (articolo 12). Esso tratta la composizione, le modalità di voto e le funzioni del consiglio di amministrazione (sezione 1, articoli da 13 a 17), del comitato esecutivo (sezione

2, articolo 18) e del direttore esecutivo (sezione 3, articolo 19). Contiene inoltre disposizioni sulla composizione e il ruolo del gruppo permanente dei portatori d'interessi (sezione 4, articolo 20). Per ultimo, ma non meno importante, la sezione 5 di tale capo stabilisce in dettaglio le norme operative per l'Agenzia, anche in relazione alla programmazione delle sue operazioni, al conflitto di interessi, alla trasparenza, alla riservatezza e all'accesso ai documenti (articoli da 21 a 25).

Il capo III riguarda la formazione e la struttura del bilancio dell'Agenzia (articoli 26 e 27), nonché le regole che ne disciplinano l'esecuzione (articoli 28 e 29). Esso contiene anche le disposizioni per facilitare la lotta contro la frode, la corruzione e altre attività illecite (articolo 30).

Il capo IV verte sul personale dell'Agenzia e comprende disposizioni generali relative allo statuto dei funzionari e al regime applicabile agli altri agenti e le regole che disciplinano i privilegi e le immunità (articolo 31 e 32). Esso illustra altresì le regole di reclutamento e nomina del direttore esecutivo dell'agenzia (articolo 33). Da ultimo, ma non meno importante, include le disposizioni per l'impiego di esperti nazionali distaccati o di altro personale non assunto dall'Agenzia (articolo 34).

Infine, il capo V contiene le disposizioni generali relative all'Agenzia. Esso delinea lo status giuridico (articolo 35) e include disposizioni che disciplinano le questioni di responsabilità, il regime linguistico, la protezione dei dati personali (articoli da 36 a 38), nonché le norme di sicurezza in materia di protezione delle informazioni classificate e delle informazioni sensibili non classificate (articolo 40). Esso descrive le regole che disciplinano la cooperazione dell'Agenzia con i paesi terzi e le organizzazioni internazionali (articolo 39). Da ultimo, ma non meno importante, contiene anche disposizioni concernenti la sede dell'Agenzia e le condizioni di esercizio, nonché il controllo amministrativo da parte del Mediatore (articoli 41 e 42).

Il titolo III del regolamento istituisce il quadro europeo di certificazione della cibersicurezza (il "**quadro**") per i prodotti e i servizi TIC in quanto *lex generalis* (articolo 1). Esso definisce l'obiettivo generale dei sistemi europei di certificazione della cibersicurezza, vale a dire attestare che i prodotti e i servizi TIC sono conformi a determinati requisiti di sicurezza informatica per quanto riguarda la loro capacità di resistere, a un determinato livello di affidabilità, ad azioni volte a compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le relative funzioni e servizi (articolo 43). Inoltre, esso elenca gli obiettivi di sicurezza che i sistemi europei di certificazione della cibersicurezza si prefiggono (articolo 45), come, tra l'altro, la capacità di proteggere i dati dall'accesso o dalla divulgazione, dalla distruzione o dall'alterazione accidentali o non autorizzati, nonché il contenuto (cioè gli elementi) dei sistemi europei di certificazione della cibersicurezza, quali, ad esempio, la definizione del loro ambito di applicazione, gli obiettivi in materia di sicurezza, i criteri di valutazione, ecc. (articolo 47).

Il titolo III stabilisce inoltre i principali effetti giuridici dei sistemi europei di certificazione della cibersicurezza, vale a dire: i) l'obbligo di attuare il sistema a livello nazionale e il carattere volontario della certificazione; ii) l'effetto invalidante dei sistemi europei di certificazione della cibersicurezza sui sistemi nazionali per gli stessi prodotti o servizi (articoli 48 e 49).

Il titolo stabilisce inoltre la procedura per l'adozione dei sistemi europei di certificazione della cibersicurezza e i rispettivi ruoli della Commissione, dell'ENISA e del gruppo europeo per la certificazione della cibersicurezza – (il "gruppo") (articolo 44). Infine, il titolo stabilisce le disposizioni che disciplinano gli organismi di valutazione della conformità, compresi i loro

requisiti, le competenze e i compiti, le autorità nazionali di controllo della certificazione e le sanzioni.

Il gruppo è istituito nel citato titolo come un organo fondamentale composto da rappresentanti delle autorità nazionali di controllo della certificazione la cui funzione principale è collaborare con l'ENISA nell'elaborazione dei sistemi europei di certificazione della cibersicurezza e fornire consulenza alla Commissione su questioni generali o specifiche riguardanti la politica di certificazione della cibersicurezza.

Il titolo IV del regolamento contiene le disposizioni finali che descrivono l'esercizio della delega, i requisiti in materia di valutazione, abrogazione e sostituzione, così come l'entrata in vigore.

2017/0225 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[28],

visto il parere del Comitato delle regioni[29],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Le reti e i sistemi informativi e le reti e i servizi di telecomunicazione svolgono un ruolo essenziale per la società e sono diventati i pilastri della crescita economica. Le tecnologie dell'informazione e della comunicazione sono alla base dei sistemi complessi su cui poggiano le attività della società, che fanno funzionare le nostre economie in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e che, in particolare, contribuiscono al funzionamento del mercato interno.

(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, imprese e amministrazioni pubbliche di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'internet degli oggetti (IoT) nel prossimo decennio dovrebbero essere disponibili in tutta l'UE milioni, se non miliardi, di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi siano connessi a internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti aziendali e individuali dispongano di informazioni insufficienti sulle caratteristiche dei prodotti e dei servizi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali.

(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle

[28] GU C , , pag. .
[29] GU C , , pag. .

minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche).

(4) Gli attacchi informatici sono in aumento e la maggiore vulnerabilità dell'economia e della società connesse alle minacce e agli attacchi informatici impone un rafforzamento delle difese. Tuttavia, mentre gli attacchi informatici hanno spesso una dimensione transfrontaliera, le risposte politiche delle autorità incaricate della cibersicurezza e le competenze in materia di applicazione della legge sono prevalentemente nazionali. Gli incidenti informatici su vasta scala possono ostacolare la prestazione di servizi essenziali su tutto il territorio dell'UE. Ciò richiede capacità effettive di risposta e di gestione delle crisi a livello di UE, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca. Inoltre, una valutazione periodica dello stato della cibersicurezza e della resilienza nell'Unione, che sia basata su dati affidabili a livello di Unione e su previsioni sistematiche degli sviluppi, delle sfide e delle minacce futuri, sia a livello di Unione sia a livello mondiale, è quindi importante per i responsabili delle politiche, il settore e gli utenti.

(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

(6) Nel 2004 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 460/2004[30] che istituisce l'ENISA 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 amministrazioni pubbliche. Nel 2008 il Parlamento europeo e il Consiglio hanno adottato il

[30] 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).

regolamento (CE) n. 1007/2008[31] che ha prorogato il mandato dell'Agenzia fino a marzo 2012. Il regolamento (CE) n. 580/2011[32] ha prorogato ulteriormente il mandato dell'Agenzia fino al 13 settembre 2013. Nel 2013 il Parlamento europeo e il Consiglio hanno adottato il regolamento (CE) n. 526/2013[33] relativo all'ENISA e che abroga il regolamento (CE) n. 460/2004, che ha prorogato il mandato dell'agenzia fino a giugno 2020.

(7) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la strategia dell'UE per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi per la cibersicurezza. Nell'ambito dei suoi sforzi volti a proteggere maggiormente gli europei durante la navigazione online, nel 2016 l'Unione ha adottato il primo atto legislativo nel settore della cibersicurezza, la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("direttiva NIS"). La direttiva NIS ha stabilito obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, l'acqua, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di cloud computing e mercati online). All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza.

(8) È noto che, dall'adozione della strategia dell'UE per la cibersicurezza del 2013 e dall'ultima revisione del mandato dell'Agenzia, il contesto politico generale è cambiato in modo significativo, anche in relazione a un contesto globale più incerto e meno sicuro. In tale contesto e nel quadro della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama delle minacce, per far fronte al quale l'attuale mandato non è sufficiente, come riconosciuto dalla valutazione dell'Agenzia.

(9) L'Agenzia istituita dal presente regolamento dovrebbe succedere all'ENISA, istituita con il regolamento (UE) n. 526/2013. L'Agenzia dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli atti legislativi dell'UE nel settore della cibersicurezza, anche fornendo consulenze e pareri e fungendo da centro di informazioni e conoscenze dell'Unione. Dovrebbe promuovere lo scambio di buone

---

31 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).

32 Regolamento (UE) n. 580/2011 del Parlamento europeo e del Consiglio, dell'8 giugno 2011, 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 165 del 24.6.2011, pag. 3).

33 Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).

pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornendo suggerimenti strategici alla Commissione europea e agli Stati membri, fungendo da punto di riferimento per iniziative politiche settoriali dell'Unione sulle questioni di cibersicurezza, promuovendo la cooperazione operativa tra gli Stati membri e tra questi ultimi e le istituzioni, le agenzie e gli organismi dell'UE.

(10) Nel quadro della decisione 2004/97/CE, Euratom, adottata nella riunione del Consiglio europeo del 13 dicembre 2003, i rappresentanti degli Stati membri hanno deciso che la sede dell'ENISA sarebbe stata in Grecia, in una città designata dal governo greco. Lo Stato membro ospitante dovrebbe garantire le migliori condizioni possibili per il corretto ed efficace funzionamento dell'Agenzia. Per uno svolgimento adeguato ed efficiente dei suoi compiti, per l'assunzione e il mantenimento del personale e per una maggiore efficacia delle attività relative alla creazione di una rete di contatti, è imprescindibile che l'Agenzia sia ubicata in una sede adeguata che garantisca, tra l'altro, collegamenti e infrastrutture di trasporto appropriati per i coniugi e i figli del personale. Le disposizioni necessarie dovrebbero essere fissate in un accordo concluso tra l'Agenzia e lo Stato membro ospitante previa approvazione del consiglio di amministrazione dell'Agenzia.

(11) Tenuto conto delle crescenti sfide in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'Agenzia dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale europeo.

(12) È opportuno che l'Agenzia sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza, alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'Agenzia dovrebbe contribuire in modo proattivo agli sforzi nazionali e dell'Unione, collaborando pienamente con istituzioni, organi, uffici e agenzie dell'Unione e con gli Stati membri. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione del settore privato e di altri portatori d'interessi. 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.

(13) L'Agenzia dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza, anche per quanto riguarda la protezione delle infrastrutture critiche e la ciberresilienza. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza.

(14) Il compito di base dell'Agenzia è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva NIS, che è essenziale ai fini del rafforzamento della ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.

(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la

preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.

(16) L'Agenzia dovrebbe assistere il gruppo di cooperazione istituito dalla direttiva NIS nell'esecuzione dei suoi compiti, in particolare mettendo a disposizione competenze, fornendo consulenze e agevolando lo scambio di migliori pratiche, specialmente per quanto riguarda l'individuazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti.

(17) Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, in particolare per sostenere la protezione delle infrastrutture critiche, l'Agenzia dovrebbe agevolare la creazione di centri settoriali di condivisione e di analisi delle informazioni (ISAC) fornendo migliori pratiche e orientamenti sugli strumenti disponibili, procedure e orientamenti su come affrontare le questioni normative relative alla condivisione delle informazioni.

(18) L'Agenzia dovrebbe aggregare e analizzare le relazioni nazionali dei CSIRT e della CERT-UE, definendo norme, lingua e terminologia comuni per lo scambio delle informazioni. Dovrebbe inoltre coinvolgere il settore privato, nel quadro della direttiva NIS che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo con la creazione della rete di CSIRT.

(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.

(20) Ai fini dello svolgimento dei suoi compiti operativi, l'Agenzia dovrebbe avvalersi delle competenze disponibili della CERT-UE attraverso una cooperazione strutturata, caratterizzata da una stretta vicinanza geografica. La cooperazione strutturata faciliterà le sinergie necessarie e il rafforzamento delle competenze dell'ENISA. Se del caso, dovrebbero essere conclusi appositi accordi tra le due organizzazioni per definire l'attuazione pratica di tale cooperazione.

(21) Conformemente ai suoi compiti operativi, l'Agenzia dovrebbe essere in grado di assistere gli Stati membri, ad esempio fornendo consulenza o assistenza tecnica o assicurando l'analisi di minacce e incidenti. Nella sua raccomandazione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, la Commissione raccomanda agli Stati membri di cooperare in buona fede e di condividere tra loro e con l'ENISA senza indebiti ritardi le informazioni su tali

incidenti e crisi. Tali informazioni dovrebbero aiutare ulteriormente l'ENISA nello svolgimento dei suoi compiti operativi.

(22) Nell'ambito della costante cooperazione a livello tecnico per sostenere la conoscenza situazionale dell'Unione, l'Agenzia dovrebbe elaborare periodicamente la relazione sulla situazione tecnica della cibersicurezza nell'UE in merito alle minacce e agli incidenti, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni trasmesse dai CSIRT degli Stati membri (su base volontaria) o dai punti di contatto unici istituiti dalla direttiva NIS, dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol, dalla CERT-UE e, ove necessario, dal Centro dell'UE di analisi dell'intelligence (INTCEN) presso il Servizio europeo per l'azione esterna (SEAE). La relazione dovrebbe essere messa a disposizione delle istanze competenti del Consiglio, della Commissione, dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e della rete di CSIRT.

(23) Le indagini tecniche ex post sugli incidenti aventi un impatto significativo in più Stati membri coadiuvate o avviate dall'Agenzia su richiesta o con l'accordo degli Stati membri interessati dovrebbero essere incentrate sulla prevenzione degli incidenti futuri ed essere effettuate senza arrecare pregiudizio agli eventuali procedimenti giudiziari o amministrativi finalizzati all'accertamento di colpe o responsabilità.

(24) Fatti salvi l'articolo 346 del trattato sul funzionamento dell'Unione europea o altri motivi di ordine pubblico, gli Stati membri interessati dovrebbero fornire le informazioni e l'assistenza necessarie all'Agenzia ai fini dell'indagine.

(25) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'Agenzia, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale.

(26) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni dell'Unione, l'Agenzia ha bisogno di analizzare i rischi attuali e quelli emergenti. A tal fine, in cooperazione con gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'Agenzia dovrebbe raccogliere le informazioni pertinenti, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'Agenzia dovrebbe inoltre assistere gli Stati membri e le istituzioni, le agenzie e gli organi dell'Unione nell'individuazione delle tendenze emergenti e nella prevenzione dei problemi connessi alla cibersicurezza attraverso l'analisi di minacce e incidenti.

(27) Al fine di aumentare la resilienza dell'Unione, l'Agenzia dovrebbe sviluppare l'eccellenza in materia di sicurezza delle infrastrutture di internet e delle infrastrutture critiche, fornendo consulenza, orientamenti e migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'Agenzia dovrebbe sviluppare e mantenere il "polo d'informazione" dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dalle agenzie e dagli organi dell'UE e nazionali.

(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a

promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

(29) Al fine di sostenere le imprese operanti nel settore della cibersicurezza, come pure gli utilizzatori delle soluzioni di cibersicurezza, l'Agenzia dovrebbe sviluppare e mantenere un "osservatorio del mercato" mediante l'esecuzione di analisi periodiche e la diffusione di informazioni sulle principali tendenze del mercato della cibersicurezza, sul versante sia della domanda che dell'offerta.

(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

(31) L'Agenzia, in quanto membro che svolge la funzione di segretariato della rete di CSIRT, dovrebbe sostenere i CSIRT degli Stati membri e la CERT-UE nella cooperazione operativa, così come in tutte le pertinenti funzioni della rete di CSIRT, secondo quanto stabilito dalla direttiva NIS. Inoltre, l'Agenzia dovrebbe promuovere e sostenere la cooperazione tra i CSIRT interessati in caso di incidenti, attacchi o perturbazioni delle reti o delle infrastrutture della cui gestione o protezione sono responsabili i CSIRT e nei quali siano o possano essere coinvolti almeno due CSIRT, tenendo debitamente conto delle procedure operative standard della rete di CSIRT.

(32) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti di cibersicurezza, l'Agenzia dovrebbe organizzare ogni anno esercitazioni di cibersicurezza a livello di Unione e, su loro richiesta, assistere le istituzioni, le agenzie e gli organi degli Stati membri e dell'UE nell'organizzazione delle esercitazioni.

(33) L'Agenzia dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'UE in questo campo. Essa dovrebbe promuovere la diffusione della certificazione della

cibersicurezza nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.

(34) Strategie efficaci in materia di cibersicurezza dovrebbero essere basate su buoni metodi di valutazione dei rischi, sia nel settore pubblico che in quello privato. I metodi di valutazione dei rischi sono utilizzati a diversi livelli, e non esiste una prassi comune per quanto riguarda le modalità per una loro applicazione efficiente. La promozione e lo sviluppo di migliori pratiche per la valutazione dei rischi e per soluzioni interoperabili per la loro gestione nelle organizzazioni del settore pubblico e del settore privato aumenteranno il livello di cibersicurezza nell'Unione. A tal fine, l'Agenzia dovrebbe sostenere la cooperazione tra i portatori di interessi a livello di Unione, facilitando il loro impegno nella definizione e nella diffusione di standard europei e internazionali in materia di gestione dei rischi e di sicurezza misurabile di prodotti elettronici, sistemi, reti e servizi che, insieme ai software, costituiscono le reti e i sistemi informativi.

(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria cibersicurezza. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di cibersicurezza. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti e servizi.

(36) L'Agenzia dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, agli organi, agli uffici e alle agenzie dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca nel settore della sicurezza delle reti e dell'informazione, in particolare per quanto riguarda la cibersicurezza.

(37) I problemi di cibersicurezza sono questioni globali. È necessaria una più stretta cooperazione internazionale per migliorare gli standard di sicurezza, anche definendo norme di comportamento comuni, condividendo le informazioni e promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'Agenzia dovrebbe sostenere una partecipazione e una cooperazione maggiori dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo, se del caso, le competenze e le analisi necessarie alle istituzioni, agli organi, agli uffici e alle agenzie dell'Unione competenti.

(38) L'Agenzia dovrebbe essere in grado di rispondere alle richieste specifiche di consulenza e di assistenza inoltrate dagli Stati membri e dalle istituzioni, dalle agenzie e dagli organi dell'UE che rientrano nei suoi obiettivi.

(39) È necessario applicare taluni principi per quanto riguarda la gestione dell'Agenzia al fine di rispettare la dichiarazione congiunta e l'approccio comune concordati nel luglio 2012 dal gruppo di lavoro interistituzionale sulle agenzie decentrate dell'Unione, con l'obiettivo di razionalizzare le attività delle agenzie e di migliorare la loro efficacia. La dichiarazione congiunta e l'approccio comune dovrebbero riflettersi, se del caso, nei

programmi di lavoro dell'Agenzia, nelle sue valutazioni e nelle sue prassi di informazione e amministrazione.

(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.

(41) Per garantire il funzionamento corretto ed efficace dell'Agenzia, la Commissione e gli Stati membri dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze ed esperienze professionali adeguate nelle aree funzionali. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori.

(42) 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 cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe inoltre redigere una relazione annuale 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. Inoltre, 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. Il direttore esecutivo 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, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

(43) Il comitato esecutivo dovrebbe contribuire al funzionamento efficace del consiglio di amministrazione. Nel quadro dei lavori preparatori relativi alle decisioni del consiglio di amministrazione, esso dovrebbe esaminare dettagliatamente le informazioni pertinenti, valutare le opzioni disponibili e fornire consulenza e soluzioni per la preparazione delle decisioni pertinenti del consiglio di amministrazione.

(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire

un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.

(45) L'Agenzia dovrebbe disporre di norme relative alla prevenzione e alla gestione dei conflitti di interessi. L'Agenzia dovrebbe applicare le disposizioni pertinenti dell'Unione in materia di accesso del pubblico ai documenti stabilite dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio[34]. Il trattamento dei dati personali da parte dell'Agenzia dovrebbe avvenire in conformità al 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[35]. È opportuno che l'Agenzia si conformi alle disposizioni applicabili alle istituzioni dell'Unione e alla legislazione nazionale in materia di gestione delle informazioni, in particolare delle informazioni sensibili non classificate e delle informazioni classificate dell'UE.

(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che essa sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del suo mandato. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della rendicontabilità, la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.

(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

(48) La certificazione della cibersicurezza riveste un ruolo importante nel rafforzare la sicurezza di prodotti e servizi TIC e nell'accrescere la fiducia negli stessi. Il mercato unico digitale, e in particolare l'economia dei dati e l'internet degli oggetti, possono prosperare solo se i cittadini sono convinti che tali prodotti e servizi offrono un determinato livello di affidabilità in termini di cibersicurezza. Le automobili connesse e automatizzate, i dispositivi medici elettronici, i sistemi di controllo per

---

34 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).

35 GU L 8 del 12.1.2001, pag. 1.

l'automazione industriale e le reti elettriche intelligenti sono solo alcuni esempi di settori in cui la certificazione è già ampiamente utilizzata o sarà probabilmente utilizzata in un prossimo futuro. La certificazione della cibersicurezza riveste un'importanza fondamentale anche nei settori disciplinati dalla direttiva NIS.

(49) Nella comunicazione del 2016 dal titolo "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" la Commissione ha sottolineato la necessità di prodotti e soluzioni di alta qualità, a costi contenuti e interoperabili. L'offerta di prodotti e servizi TIC nel mercato unico resta molto frammentata dal punto di vista geografico. La causa di tale frammentazione va ravvisata nel fatto che il settore della cibersicurezza in Europa si è sviluppato soprattutto in risposta alla domanda pubblica nazionale. Inoltre, l'assenza di soluzioni interoperabili (norme tecniche), di pratiche e di meccanismi UE di certificazione è un'altra delle lacune che influisce sul mercato unico della cibersicurezza. Ciò incide negativamente sulla competitività delle imprese europee a livello nazionale, europeo e mondiale e allo stesso tempo limita la gamma di tecnologie di cibersicurezza valide e utilizzabili a cui cittadini e imprese hanno accesso. Anche nella revisione intermedia dell'attuazione della strategia per il mercato unico digitale, la Commissione ha evidenziato la necessità di prodotti e sistemi connessi sicuri e ha dichiarato che la creazione di un quadro europeo di sicurezza delle TIC che definisca norme su come organizzare la certificazione della sicurezza delle TIC nell'Unione potrebbe sia preservare la fiducia nei confronti di internet sia permettere di affrontare l'attuale frammentazione del mercato della cibersicurezza.

(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo.

(51) In passato sono stati compiuti sforzi finalizzati al reciproco riconoscimento dei certificati in Europa. Il loro successo tuttavia è stato solo parziale. L'esempio più importante in tal senso è l'accordo sul reciproco riconoscimento (ARR) del gruppo di alti funzionari competente in materia di sicurezza dei sistemi di informazione (SOG-IS). Sebbene rappresenti il più importante modello di cooperazione e di riconoscimento reciproco nel campo della certificazione della sicurezza, l'ARR del SOG-IS presenta alcune carenze significative, che vanno ravvisate nei suoi costi elevati e nel suo campo di applicazione limitato. Finora sono stati sviluppati solo alcuni profili di protezione per i prodotti digitali, ad esempio la firma digitale, il tachigrafo digitale e le smart card. Un aspetto ancora più importante riguarda il fatto che il SOG-IS comprende solo una parte degli Stati membri dell'Unione. Ciò ha limitato l'efficacia dell'ARR del SOG-IS dal punto di vista del mercato interno.

(52) In considerazione di quanto precede, è necessario definire un quadro europeo di certificazione della cibersicurezza che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della cibersicurezza da sviluppare e che consenta di

riconoscere e utilizzare i certificati per i prodotti e servizi TIC in tutti gli Stati membri. Il quadro europeo dovrebbe avere un duplice obiettivo: da un lato dovrebbe contribuire ad aumentare la fiducia nei prodotti e nei servizi TIC che sono stati certificati in base a detti sistemi. Dall'altro lato dovrebbe evitare il proliferare di certificazioni nazionali della cibersicurezza confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi dovrebbero essere non discriminatori e basati su norme tecniche internazionali e/o dell'Unione, a meno che tali norme non siano inefficaci o inadeguate ai fini del conseguimento dei legittimi obiettivi dell'UE in tale ambito.

(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.

(54) Le disposizioni del presente regolamento dovrebbero lasciare impregiudicata la legislazione dell'Unione che prevede norme specifiche sulla certificazione di prodotti e servizi TIC. In particolare, il regolamento generale sulla protezione dei dati stabilisce disposizioni per l'istituzione di meccanismi di certificazione e sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali meccanismi di certificazione e sigilli e marchi di protezione dei dati dovrebbero consentire agli interessati di valutare rapidamente il livello di protezione dei dati dei prodotti e dei servizi. Il presente regolamento lascia impregiudicata la certificazione delle operazioni di trattamento dei dati, anche nel caso in cui tali operazioni siano integrate nei prodotti e nei servizi, nel quadro del regolamento generale sulla protezione dei dati.

(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti e i servizi TIC certificati nel loro ambito siano conformi ai requisiti specificati. Tali requisiti riguardano la capacità di resistere, a un determinato livello di affidabilità, alle azioni che mirano a compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti e servizi TIC. I prodotti e i servizi TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei prodotti e nei servizi TIC specifici dovrebbero quindi essere ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche.

(56) La Commissione dovrebbe avere la facoltà di incaricare l'ENISA di preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.

(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

(59) È necessario imporre a tutti gli Stati membri di designare un'autorità di controllo della certificazione della cibersicurezza per vigilare sulla conformità degli organismi di valutazione della conformità e dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio ai requisiti del presente regolamento e dei pertinenti sistemi di certificazione della cibersicurezza. Le autorità nazionali di controllo della certificazione dovrebbero trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio, svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Esse dovrebbero inoltre cooperare con le altre autorità nazionali di controllo della certificazione o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi di cibersicurezza.

(60) Al fine di garantire un'applicazione coerente del quadro europeo di certificazione della cibersicurezza, dovrebbe essere costituito un gruppo europeo per la certificazione della cibersicurezza (di seguito il "gruppo") costituito dalle autorità nazionali di controllo della certificazione. I compiti principali del gruppo dovrebbero essere consigliare e assistere la Commissione nelle attività volte ad assicurare un'attuazione e un'applicazione coerenti del quadro europeo di certificazione della cibersicurezza; assistere e cooperare strettamente con l'Agenzia nella preparazione delle proposte di sistemi di certificazione della cibersicurezza; raccomandare alla Commissione di incaricare l'Agenzia di preparare una proposta di sistema europeo di certificazione della cibersicurezza; adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

(61) Al fine di accrescere la consapevolezza e facilitare l'accettazione dei futuri sistemi di cibersicurezza dell'UE, la Commissione europea può emanare orientamenti generali o settoriali in materia di cibersicurezza, ad esempio orientamenti sulle buone pratiche o sul comportamento responsabile in tale ambito, sottolineando l'effetto positivo dell'utilizzo di prodotti e servizi TIC certificati.

(62) Il sostegno fornito dall'Agenzia nella certificazione della cibersicurezza dovrebbe comprendere anche i contatti con il Comitato per la sicurezza del Consiglio e con l'organismo nazionale competente relativamente all'approvazione crittografica dei prodotti da utilizzare nelle reti classificare.

(63) Al fine di specificare ulteriori criteri per l'accreditamento degli organismi di valutazione della conformità, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. Durante i lavori preparatori la Commissione dovrebbe svolgere adeguate consultazioni, anche a livello di esperti. Tali consultazioni dovrebbero essere condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016. In particolare, per assicurare pari opportunità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti in concomitanza con gli esperti degli Stati membri e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione che si occupano della preparazione degli atti delegati.

(64) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011.

(65) La procedura d'esame dovrebbe essere utilizzata per l'adozione degli atti di esecuzione sui sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC; sulle modalità di conduzione delle indagini da parte dell'Agenzia; sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di controllo della certificazione alla Commissione.

(66) L'operato dell'Agenzia dovrebbe essere valutato in maniera indipendente. La valutazione dovrebbe tenere conto del conseguimento degli obiettivi da parte dell'Agenzia, delle sue pratiche di lavoro e della pertinenza dei suoi compiti. Dovrebbe altresì valutare l'impatto, l'efficacia e l'efficienza del quadro europeo di certificazione della cibersicurezza.

(67) Il regolamento (UE) n. 526/2013 dovrebbe essere abrogato.

(68) Poiché gli obiettivi del presente regolamento non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto necessario per conseguire tali scopi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I
DISPOSIZIONI GENERALI

Articolo 1
Oggetto e ambito di applicazione

Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento:

(a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, l'Agenzia dell'UE per la cibersicurezza, di seguito denominata "l'Agenzia" e

(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti e dei servizi TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione.

Articolo 2
Definizioni

Ai fini del presente regolamento si intende per:

(1) "cibersicurezza", l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, i loro utenti e le persone interessate dalle minacce informatiche;

(2) "rete e sistema informativo", un sistema ai sensi dell'articolo 4, punto 1, della direttiva (UE) 2016/1148;

(3) "strategia nazionale per la sicurezza della rete e dei sistemi informativi", un quadro ai sensi dell'articolo 4, punto 3, della direttiva (UE) 2016/1148;

(4) "operatore di servizi essenziali", un soggetto pubblico o privato ai sensi dell'articolo 4, punto 4, della direttiva (UE) 2016/1148;

(5) "fornitore di servizio digitale", qualsiasi persona giuridica che fornisce un servizio digitale ai sensi dell'articolo 4, punto 6, della direttiva (UE) 2016/1148;

(6) "incidente", qualsiasi evento che corrisponda alla definizione di cui all'articolo 4, punto 7, della direttiva (UE) 2016/1148;

(7) "trattamento dell'incidente", qualsiasi procedura che corrisponda alla definizione di cui all'articolo 4, punto 8, della direttiva (UE) 2016/1148;

(8) "minaccia informatica", qualsiasi circostanza o evento che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

(11) "prodotto e servizio TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;

(12) "accreditamento", l'accreditamento quale definito all'articolo 2, punto 10, del regolamento (CE) n. 765/2008;

(13) "organismo nazionale di accreditamento", un organismo nazionale di accreditamento ai sensi dell'articolo 2, punto 11, del regolamento (CE) n. 765/2008;

(14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008;

(15) "organismo di valutazione della conformità", un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008;

(16) "norma tecnica", una norma tecnica ai sensi dell'articolo 2, punto 1, del regolamento (UE) n. 1025/2012.

TITOLO II
ENISA – l'Agenzia dell'UE per la cibersicurezza

CAPO I
MANDATO, OBIETTIVI E COMPITI

Articolo 3
Mandato

1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di contribuire a un elevato livello di cibersicurezza nell'Unione.
2. L'Agenzia svolge i compiti che le sono attribuiti dagli atti dell'Unione che stabiliscono le misure per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza.
3. Gli obiettivi e i compiti dell'Agenzia fanno salve le competenze degli Stati membri per quanto riguarda la cibersicurezza e, in ogni caso, fanno salve le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

Articolo 4
Obiettivi

1. L'Agenzia opera come centro di competenze nel settore della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.
2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza.
3. L'Agenzia sostiene lo sviluppo della capacità e la preparazione nell'Unione, assistendo l'Unione, gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo di abilità e competenze nel campo della cibersicurezza e nel conseguimento della ciberresilienza.
4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, su questioni relative alla cibersicurezza.
5. L'Agenzia rafforza le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.
6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei

servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.

7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

Articolo 5

Compiti relativi allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione

L'Agenzia contribuisce allo sviluppo e all'attuazione delle politiche e della normativa dell'Unione:

1. fornendo assistenza e consulenza, in particolare fornendo un parere indipendente e lavori preparatori, per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel settore della cibersicurezza, nonché delle iniziative legislative e politiche settoriali che presentano una correlazione con le questioni relative alla cibersicurezza;

2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

3. contribuendo ai lavori del gruppo di cooperazione di cui all'articolo 11 della direttiva (UE) 2016/1148, mettendo a disposizione le proprie competenze e fornendo assistenza;

4. sostenendo:

   (1) lo sviluppo e l'attuazione della politica dell'Unione nel settore dell'identificazione elettronica e dei servizi fiduciari, in particolare fornendo consulenza e orientamenti tecnici e agevolando lo scambio di migliori pratiche tra le autorità competenti;

   (2) la promozione di un livello di sicurezza più elevato delle comunicazioni elettroniche, anche fornendo competenze e consulenza e agevolando lo scambio delle migliori pratiche tra le autorità competenti;

5. sostenendo il riesame periodico delle attività politiche dell'Unione attraverso una relazione annuale sullo stato di attuazione del relativo quadro giuridico per quanto riguarda:

   (a) le notifiche degli incidenti degli Stati membri trasmesse dal punto di contatto unico al gruppo di cooperazione, a norma dell'articolo 10, paragrafo 3, della direttiva (UE) 2016/1148;

   (b) le notifiche di violazioni della sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari, trasmesse dagli organismi di vigilanza all'Agenzia, a norma dell'articolo 19, paragrafo 3, del regolamento (UE) n. 910/2014;

   (c) le notifiche di violazione della sicurezza trasmesse dalle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione

elettronica accessibili al pubblico, trasmesse dalle autorità competenti all'Agenzia, a norma dell'articolo 40 della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche].

Articolo 6

Compiti relativi allo sviluppo della capacità

1. L'Agenzia assiste:

(a) gli Stati membri nell'impegno a migliorare la prevenzione, la rilevazione e l'analisi di problemi e incidenti legati alla cibersicurezza, come pure la capacità di reazione agli stessi, fornendo loro le conoscenze e le competenze necessarie;

(b) le istituzioni, gli organismi, gli uffici e le agenzie dell'Unione nel loro impegno a migliorare la prevenzione, la rilevazione e l'analisi dei problemi e degli incidenti legati alla cibersicurezza, come pure la capacità di reazione agli stessi, tramite un sostegno adeguato alla squadra CERT delle istituzioni, delle agenzie e degli organismi dell'Unione (CERT-UE);

(c) gli Stati membri, su loro richiesta, nello sviluppo di gruppi di intervento nazionali per la sicurezza informatica in caso di incidente (CSIRT), a norma dell'articolo 9, paragrafo 5, della direttiva (UE) 2016/1148;

(d) gli Stati membri, su loro richiesta, nello sviluppo di strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi, a norma dell'articolo 7, paragrafo 2, della direttiva (UE) 2016/1148; l'Agenzia promuove inoltre la diffusione di tali strategie e valuta i progressi compiuti nella loro attuazione in tutta l'Unione allo scopo di promuovere le migliori pratiche;

(e) le istituzioni dell'Unione nello sviluppo e nella revisione di strategie dell'Unione in materia di cibersicurezza, nella promozione della loro diffusione e nel monitoraggio dei progressi compiuti nella loro attuazione;

(f) i CSIRT nazionali e dell'Unione nell'innalzare il livello delle loro capacità, anche attraverso la promozione del dialogo e dello scambio di informazioni, al fine di assicurare che, tenuto conto dello stato dell'arte, tutti i CSIRT soddisfino una serie comune di capacità minime e operino secondo le migliori pratiche;

(g) gli Stati membri mediante l'organizzazione delle esercitazioni annuali di cibersicurezza su vasta scala a livello di Unione di cui all'articolo 7, paragrafo 6, e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

(h) i pertinenti enti pubblici attraverso l'offerta di formazione sulla cibersicurezza, se del caso in cooperazione con i portatori di interessi.

(i) il gruppo di cooperazione, attraverso lo scambio di migliori pratiche, in particolare per quanto riguarda l'identificazione degli operatori di servizi essenziali da parte degli Stati membri, anche in relazione alle dipendenze transfrontaliere, riguardo a rischi e incidenti, a norma dell'articolo 11, paragrafo 3, lettera l), della direttiva (UE) 2016/1148.

2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori

pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Articolo 7

Compiti relativi alla cooperazione operativa a livello di Unione

1. L'Agenzia sostiene la cooperazione operativa tra gli enti pubblici competenti e tra i portatori di interessi.

2. L'Agenzia coopera a livello operativo e stabilisce sinergie con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, compresi la CERT-UE, i servizi che si occupano della criminalità informatica e le autorità di vigilanza che si occupano della tutela della vita privata e della protezione dei dati personali, al fine di affrontare questioni di interesse comune, anche:

   (a) scambiando conoscenze e migliori pratiche;

   (b) fornendo consulenza e orientamenti sulle questioni pertinenti relative alla cibersicurezza;

   (c) predisponendo, previa consultazione della Commissione, le disposizioni pratiche per l'esecuzione di compiti specifici.

3. L'Agenzia svolge le funzioni di segretariato della rete di CSIRT, a norma dell'articolo 12, paragrafo 2, della direttiva (UE) 2016/1148, e si adopera per agevolare attivamente la condivisione delle informazioni e la cooperazione tra i suoi membri.

4. L'Agenzia contribuisce alla cooperazione operativa nell'ambito della rete di CSIRT fornendo sostegno agli Stati membri mediante:

   (a) consigli su come migliorare le loro capacità di prevenzione e rilevazione degli incidenti e di risposta agli stessi;

   (b) l'offerta, su richiesta degli Stati membri, di assistenza tecnica in caso di incidenti aventi un impatto rilevante o sostanziale;

   (c) l'analisi delle vulnerabilità, degli artefatti e degli incidenti.

Nello svolgimento di questi compiti, l'Agenzia e la CERT-UE intraprendono una cooperazione strutturata al fine di beneficiare delle sinergie, in particolare per quanto riguarda gli aspetti operativi.

5. Su richiesta di due o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di due Stati membri.

   L'ambito dell'indagine e la procedura da seguire nel suo svolgimento sono concordati dagli Stati membri interessati e dall'Agenzia e non pregiudicano eventuali indagini penali in corso relative allo stesso incidente. L'indagine si conclude con una relazione tecnica finale redatta dall'Agenzia, in particolare sulla base delle informazioni e dei commenti forniti dagli Stati membri e dalla o dalle imprese

interessati, e concordata con gli Stati membri interessati. Una sintesi della relazione, incentrata sulle raccomandazioni per la prevenzione di futuri incidenti, è condivisa con la rete di CSIRT.

6. L'Agenzia organizza esercitazioni annuali di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organi dell'UE nell'organizzazione di esercitazioni. Le esercitazioni annuali a livello di Unione includono gli elementi tecnici, operativi e strategici e contribuiscono a preparare la risposta cooperativa a livello di Unione agli incidenti di cibersicurezza transfrontalieri di vasta portata. L'Agenzia inoltre contribuisce e aiuta ad organizzare, se del caso, esercitazioni di cibersicurezza settoriali insieme ai pertinenti ISAC e consente agli ISAC di partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.

7. L'Agenzia elabora periodicamente una relazione sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro: dai CSIRT degli Stati membri (su base volontaria) o dai punti di contatto unici istituiti dalla direttiva NIS (conformemente all'articolo 14, paragrafo 5, della direttiva NIS), dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol e dalla CERT-UE.

8. L'Agenzia contribuisce a sviluppare una risposta cooperativa, a livello di Unione e di Stati membri, agli incidenti o alle crisi transfrontalieri su vasta scala connessi alla cibersicurezza, soprattutto:

   (a) aggregando le relazioni delle fonti nazionali al fine di contribuire a creare una conoscenza situazionale comune;

   (b) assicurando un flusso di informazioni efficiente e la disponibilità di meccanismi di attivazione tra la rete di CSIRT e i responsabili delle decisioni politiche e tecniche a livello di Unione;

   (c) fornendo assistenza nel trattamento tecnico di un incidente o di una crisi, anche agevolando la condivisione di soluzioni tecniche tra gli Stati membri;

   (d) favorendo la comunicazione pubblica in merito all'incidente o alla crisi;

   (e) testando i piani di cooperazione per rispondere a detti incidenti o crisi.

Articolo 8

Compiti relativi al mercato, alla certificazione della cibersicurezza e alla normazione

L'Agenzia:

(a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti e dei servizi TIC, come stabilito al titolo III del presente regolamento:

   (1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;

   (2) assistendo la Commissione nel provvedere alle funzioni di segretariato del gruppo europeo per la certificazione della cibersicurezza a norma dell'articolo 53 del presente regolamento;

(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

(b) agevola la definizione e l'adozione di norme tecniche europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;

(c) effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante della domanda e dell'offerta, al fine di promuovere tale mercato nell'Unione.

Articolo 9

Compiti relativi alle conoscenze, alle informazioni e alla sensibilizzazione

L'Agenzia:

(a) esegue analisi delle tecnologie emergenti e fornisce valutazioni su temi specifici in relazione agli impatti previsti, dal punto di vista sociale, giuridico, economico e regolamentare, delle innovazioni tecnologiche sulla cibersicurezza;

(b) effettua analisi strategiche a lungo termine delle minacce e degli incidenti di cibersicurezza al fine di individuare le tendenze emergenti e contribuire a prevenire i problemi connessi alla cibersicurezza;

(c) fornisce, in cooperazione con esperti delle autorità degli Stati membri, consulenza, orientamenti e migliori pratiche per la sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture di internet e delle infrastrutture su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148;

(d) raggruppa, organizza e mette a disposizione del pubblico, tramite un portale dedicato, informazioni sulla cibersicurezza, fornite dalle istituzioni, dalle agenzie e dagli organi dell'Unione;

(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;

(f) raccoglie e analizza le informazioni pubblicamente disponibili sugli incidenti rilevanti e redige relazioni al fine di fornire orientamenti alle imprese e ai cittadini in tutta l'Unione;

(g) organizza regolarmente, in collaborazione con gli Stati membri e con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, campagne di sensibilizzazione al fine di rafforzare la cibersicurezza e la sua visibilità nell'Unione.

Articolo 10

Compiti relativi alla ricerca e all'innovazione

Per quanto riguarda la ricerca e l'innovazione, l'Agenzia:

(a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

(b) partecipa, qualora la Commissione le abbia delegato i pertinenti poteri, alla fase di attuazione dei programmi di finanziamento per la ricerca e l'innovazione o in qualità di beneficiario.

Articolo 11

Compiti relativi alla cooperazione internazionale

L'Agenzia contribuisce all'impegno dell'Unione nella cooperazione con i paesi terzi e le organizzazioni internazionali per promuovere la cooperazione internazionale sulle questioni connesse alla cibersicurezza:

(a) impegnandosi, ove opportuno, in qualità di osservatore e nell'organizzazione delle esercitazioni internazionali, nonché analizzando i risultati di tali esercitazioni e comunicandoli al consiglio di amministrazione;

(b) agevolando, su richiesta della Commissione, lo scambio di migliori pratiche tra le organizzazioni internazionali pertinenti;

(c) fornendo competenze specialistiche alla Commissione su richiesta.

CAPO II
ORGANIZZAZIONE DELL'AGENZIA

Articolo 12

Struttura

La struttura amministrativa e di gestione dell'Agenzia è composta da:

(a) un consiglio di amministrazione, che esercita le funzioni di cui all'articolo 14;

(b) un comitato esecutivo, che esercita le funzioni di cui all'articolo 18;

(c) un direttore esecutivo, che esercita le funzioni di cui all'articolo 19 e

(d) un gruppo permanente di portatori di interessi che esercita le funzioni di cui all'articolo 20.

SEZIONE 1
CONSIGLIO DI AMMINISTRAZIONE

Articolo 13
Composizione del consiglio di amministrazione

1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.

2. Ciascun membro del consiglio di amministrazione ha un supplente che lo rappresenta in sua assenza.

3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata tra uomini e donne nel consiglio di amministrazione.

4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di quattro anni. Il mandato è rinnovabile.

Articolo 14
Funzioni del consiglio di amministrazione

1. Il consiglio di amministrazione:

   (a) definisce gli orientamenti generali del funzionamento dell'Agenzia e assicura che operi secondo le norme e i principi stabiliti dal presente regolamento. Assicura inoltre la coerenza del lavoro dell'Agenzia con le attività svolte dagli Stati membri e a livello di Unione;

   (b) adotta il progetto di documento unico di programmazione dell'Agenzia di cui all'articolo 21 prima che venga trasmesso alla Commissione per parere;

   (c) adotta, tenendo conto del parere della Commissione, il documento unico di programmazione dell'Agenzia a maggioranza dei due terzi dei membri e conformemente all'articolo 17;

   (d) adotta, a maggioranza dei due terzi dei membri, il bilancio annuale dell'Agenzia ed esercita altre funzioni in relazione al bilancio dell'Agenzia a norma del capo III;

   (e) valuta e adotta la relazione annuale consolidata sulle attività dell'Agenzia e trasmette, entro il 1° luglio dell'anno successivo, sia la relazione che la sua valutazione al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti. La relazione annuale include i conti e descrive in che modo l'Agenzia ha conseguito i propri indicatori di risultato. La relazione annuale è resa pubblica;

   (f) adotta la regolamentazione finanziaria applicabile all'Agenzia in conformità dell'articolo 29;

(g) adotta una strategia antifrode, proporzionata ai rischi di frode, tenendo conto dei costi e dei benefici delle misure da attuare;

(h) adotta norme di prevenzione e gestione dei conflitti di interesse in relazione ai suoi membri;

(i) garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e dalle relazioni di revisione contabile e valutazioni interne o esterne.

(j) adotta il proprio regolamento interno;

(k) a norma del paragrafo 2, esercita, nei confronti del personale dell'Agenzia, i poteri conferiti dallo statuto dei funzionari all'autorità che ha il potere di nomina e dal regime applicabile agli altri agenti dell'Unione europea all'autorità abilitata a concludere i contratti di assunzione ("poteri dell'autorità che ha il potere di nomina");

(l) adotta le norme di esecuzione dello statuto dei funzionari e del regime applicabile agli altri agenti secondo la procedura di cui all'articolo 110 dello statuto dei funzionari;

(m) nomina il direttore esecutivo e, se del caso, ne proroga il mandato o lo rimuove dall'incarico, a norma dell'articolo 33 del presente regolamento;

(n) nomina un contabile, che può essere il contabile della Commissione, che opera in piena indipendenza nell'esercizio delle sue funzioni;

(o) prende tutte le decisioni sull'istituzione delle strutture interne dell'Agenzia e, se necessario, sulla relativa modifica, in considerazione delle necessità per l'attività dell'Agenzia e secondo una gestione di bilancio sana;

(p) autorizza la conclusione di accordi operativi conformemente agli articoli 7 e 39.

2. Il consiglio di amministrazione adotta, in conformità dell'articolo 110 dello statuto dei funzionari, una decisione basata sull'articolo 2, paragrafo 1, dello statuto dei funzionari e sull'articolo 6 del regime applicabile agli altri agenti, con cui delega al direttore esecutivo i poteri di autorità che ha il potere di nomina e stabilisce le condizioni di sospensione della delega di poteri. Il direttore esecutivo è autorizzato a subdelegare tali poteri.

3. Qualora circostanze eccezionali lo richiedano, il consiglio di amministrazione può, mediante decisione, sospendere temporaneamente la delega dei poteri di autorità che ha il potere di nomina delegati al direttore esecutivo e quelli subdelegati da quest'ultimo ed esercitarli esso stesso o delegarli a uno dei suoi membri o a un membro del personale diverso dal direttore esecutivo.

Articolo 15
Presidente del consiglio di amministrazione

Il consiglio di amministrazione elegge tra i propri membri, a maggioranza dei due terzi dei membri, un presidente e un vicepresidente con un mandato di quattro anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio

di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Articolo 16
Riunioni del consiglio di amministrazione

1. Il consiglio di amministrazione si riunisce su convocazione del suo presidente.
2. Il consiglio di amministrazione tiene almeno due riunioni ordinarie l'anno. Si riunisce inoltre in seduta straordinaria su richiesta del presidente, della Commissione o di almeno un terzo dei suoi membri.
3. Il direttore esecutivo partecipa, senza diritto di voto, alle riunioni del consiglio di amministrazione.
4. I membri del gruppo permanente di portatori di interessi, su invito del presidente, possono partecipare senza diritto di voto alle riunioni del consiglio di amministrazione.
5. I membri del consiglio di amministrazione e i loro supplenti possono farsi assistere da consulenti o esperti, fatte salve le disposizioni del regolamento interno.
6. L'Agenzia provvede alle funzioni di segretariato del consiglio di amministrazione.

Articolo 17
Modalità di voto del consiglio di amministrazione

1. Il consiglio di amministrazione adotta le proprie decisioni a maggioranza dei suoi membri.
2. La maggioranza di due terzi di tutti i membri del consiglio di amministrazione è necessaria per il documento unico di programmazione, il bilancio annuale, la nomina del direttore esecutivo, la proroga del suo mandato o la sua rimozione dall'incarico.
3. Ogni membro dispone di un voto. In assenza di un membro, il supplente è abilitato a esercitare il suo diritto di voto.
4. Il presidente partecipa al voto.
5. Il direttore esecutivo non partecipa al voto.
6. Il regolamento interno del consiglio di amministrazione stabilisce le regole dettagliate concernenti la votazione, in particolare le circostanze in cui un membro può agire per conto di un altro.

SEZIONE 2
COMITATO ESECUTIVO

Articolo 18
Comitato esecutivo

1. Il consiglio direttivo è assistito da un comitato esecutivo.
2. Il comitato esecutivo:

(a) prepara le decisioni che dovranno essere adottate dal consiglio di amministrazione;

(b) insieme con il consiglio di amministrazione, garantisce un seguito adeguato alle risultanze e alle raccomandazioni derivanti dalle indagini svolte dall'OLAF, nonché dalle relazioni di revisione contabile e valutazioni interne ed esterne;

(c) fatte salve le responsabilità del direttore esecutivo quali stabilite all'articolo 19, fornisce assistenza e consulenza al direttore esecutivo nell'attuazione delle decisioni del consiglio di amministrazione sulle questioni amministrative e di bilancio di cui all'articolo 19.

3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.

4. La durata del mandato dei membri del consiglio di amministrazione è di quattro anni. Il mandato è rinnovabile.

5. Il comitato esecutivo si riunisce almeno una volta ogni tre mesi. Il presidente del comitato esecutivo convoca riunioni supplementari su richiesta dei suoi membri.

6. Il consiglio di amministrazione stabilisce il regolamento interno del comitato esecutivo.

7. Se necessario, per motivi di urgenza, il comitato esecutivo può prendere determinate decisioni provvisorie a nome del consiglio di amministrazione, in particolare su questioni di gestione amministrativa, tra cui la sospensione della delega dei poteri dell'autorità che ha il potere di nomina e le questioni di bilancio.

SEZIONE 3
DIRETTORE ESECUTIVO

Articolo 19
Compiti del direttore esecutivo

1. L'Agenzia è diretta dal suo direttore esecutivo che è indipendente nell'espletamento delle sue funzioni. Il direttore esecutivo risponde al consiglio di amministrazione.

2. Su richiesta, il direttore esecutivo riferisce al Parlamento europeo sull'esercizio delle sue funzioni. Il Consiglio può invitare il direttore esecutivo a riferire sull'esercizio delle sue funzioni.

3. Il direttore esecutivo ha la responsabilità di:

(a) provvedere all'amministrazione corrente dell'Agenzia;

(b) attuare le decisioni adottate dal consiglio di amministrazione;

(c) preparare il documento unico di programmazione e presentarlo al consiglio di amministrazione per approvazione prima di trasmetterlo alla Commissione;

(d) attuare il documento unico di programmazione e riferire in merito al consiglio di amministrazione;

(e) elaborare la relazione annuale consolidata sulle attività dell'Agenzia e presentarla al consiglio di amministrazione per valutazione e adozione;

(f) predisporre un piano d'azione per dare seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti;

(g) predisporre un piano d'azione a seguito delle conclusioni delle relazioni di revisione contabile interne ed esterne e delle indagini dell'Ufficio europeo per la lotta antifrode (OLAF) e riferire due volte l'anno sui progressi compiuti alla Commissione e periodicamente al consiglio di amministrazione;

(h) predisporre il progetto della regolamentazione finanziaria applicabile all'Agenzia;

(i) predisporre il progetto di stato di previsione delle entrate e delle spese dell'Agenzia e l'esecuzione del bilancio;

(j) proteggere gli interessi finanziari dell'Unione mediante l'applicazione di misure preventive contro la frode, la corruzione e qualsiasi altra attività illecita, mediante controlli efficaci e, in caso di irregolarità rilevate, mediante il recupero degli importi erroneamente versati e, se del caso, mediante sanzioni amministrative e pecuniarie efficaci, proporzionate e dissuasive;

(k) elaborare una strategia antifrode dell'Agenzia e presentarla al consiglio di amministrazione per approvazione;

(l) sviluppare e mantenere i contatti con le imprese e le organizzazioni dei consumatori per assicurare un dialogo regolare con i portatori di interessi;

(m) svolgere gli altri compiti attribuiti al direttore esecutivo dal presente regolamento.

4. In base alle esigenze e nell'ambito del mandato dell'Agenzia, e conformemente ai suoi obiettivi e compiti, il direttore esecutivo può istituire gruppi di lavoro ad hoc composti da esperti, anche inviati dalle autorità competenti degli Stati membri. Il consiglio di amministrazione ne è informato in anticipo. Le procedure relative in particolare alla composizione dei gruppi di lavoro, alla nomina degli esperti dei gruppi di lavoro da parte del direttore esecutivo e il funzionamento dei gruppi di lavoro sono specificati nel regolamento interno dell'Agenzia.

5. Il direttore esecutivo decide se sia necessario collocare personale in uno o più Stati membri per svolgere i compiti dell'Agenzia in maniera efficiente ed efficace. Prima di decidere di istituire un ufficio locale, il direttore esecutivo deve ottenere il consenso della Commissione, del consiglio di amministrazione e dello o degli Stati membri interessati. La decisione precisa la gamma di attività che vanno espletate presso l'ufficio locale al fine di evitare costi inutili e duplicazioni di funzioni amministrative dell'Agenzia. Ove necessario o opportuno, è raggiunto un accordo con lo o gli Stati membri interessati.

SEZIONE 4
GRUPPO PERMANENTE DEI PORTATORI DI INTERESSI

Articolo 20
Gruppo permanente dei portatori di interessi

1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.
2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici.
3. Il gruppo permanente di portatori di interessi è presieduto dal direttore esecutivo o da qualsiasi altra persona nominata dal direttore esecutivo caso per caso.
4. Il mandato dei membri del gruppo permanente di portatori di interessi è di due anni e mezzo. I membri del consiglio di amministrazione non possono essere membri del gruppo permanente di portatori di interessi. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare alle riunioni del gruppo permanente di portatori di interessi e a partecipare alle sue attività. I rappresentanti di altri organismi considerati pertinenti dal direttore esecutivo che non sono membri del gruppo permanente di portatori di interessi possono essere invitati a partecipare alle riunioni di tale gruppo e alle sue attività.
5. Il gruppo permanente di portatori di interessi fornisce consulenza all'Agenzia relativamente allo svolgimento delle sue attività. In particolare, esso consiglia il direttore esecutivo ai fini della stesura della proposta relativa al programma di lavoro dell'Agenzia e della comunicazione con i relativi portatori di interessi su tutte le questioni inerenti al programma di lavoro.

SEZIONE 5
FUNZIONAMENTO

Articolo 21
Documento unico di programmazione

1. L'Agenzia svolge la sua attività in conformità di un documento unico di programmazione contenente la programmazione annuale e pluriennale, che include tutte le attività pianificate.
2. Ogni anno il direttore esecutivo, tenendo conto degli orientamenti stabiliti della Commissione, predispone un progetto di documento unico di programmazione contenente la pianificazione delle risorse umane e finanziarie corrispondenti,

secondo quanto previsto all'articolo 32 del regolamento delegato (UE) n. 1271/2013[36] della Commissione.

3. Entro il 30 novembre di ogni anno il consiglio di amministrazione adotta il documento unico di programmazione di cui al paragrafo 1 e lo trasmette al Parlamento europeo, al Consiglio e alla Commissione entro il 31 gennaio dell'anno successivo, nonché eventuali versioni aggiornate di tale documento.

4. Il documento unico di programmazione diventa definitivo dopo l'approvazione definitiva del bilancio generale dell'Unione e, se necessario, è adeguato di conseguenza.

5. Il programma di lavoro annuale comprende gli obiettivi dettagliati e i risultati attesi, compresi gli indicatori di risultato. Esso contiene inoltre una descrizione delle azioni da finanziare e un'indicazione delle risorse finanziarie e umane assegnate a ciascuna azione, conformemente ai principi di formazione del bilancio per attività e gestione per attività. Il programma di lavoro annuale è coerente con il programma di lavoro pluriennale di cui al paragrafo 7. Indica chiaramente i compiti aggiunti, modificati o soppressi rispetto all'esercizio finanziario precedente.

6. Quando all'Agenzia è assegnato un nuovo compito, il consiglio di amministrazione modifica il programma di lavoro annuale adottato. Le modifiche sostanziali del programma di lavoro annuale sono adottate con la stessa procedura di quella applicabile al programma di lavoro annuale iniziale. Il consiglio di amministrazione può delegare al direttore esecutivo il potere di apportare modifiche non sostanziali al programma di lavoro annuale.

7. Il programma di lavoro pluriennale definisce la programmazione strategica generale, compresi gli obiettivi, i risultati attesi e gli indicatori di prestazione. Riporta inoltre la programmazione delle risorse, compresi il bilancio pluriennale e il personale.

8. La programmazione delle risorse è aggiornata ogni anno. La programmazione strategica è aggiornata secondo necessità, in particolare per adattarla all'esito della valutazione di cui all'articolo 56.

Articolo 22
Dichiarazione di interessi

1. I membri del consiglio di amministrazione, il direttore esecutivo, come pure i funzionari distaccati dagli Stati membri a titolo temporaneo, rendono ciascuno una dichiarazione di impegni e una dichiarazione con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza. Le dichiarazioni sono precise e complete, presentate ogni anno per iscritto e aggiornate ogniqualvolta sia necessario.

2. I membri del consiglio di amministrazione, il direttore esecutivo e gli esperti esterni che partecipano ai gruppi di lavoro ad hoc dichiarano ciascuno in modo preciso e completo, al più tardi all'inizio di ogni riunione, qualsiasi interesse che possa essere considerato in contrasto con la loro indipendenza in relazione ai punti all'ordine del

[36] Regolamento delegato (UE) n. 1271/2013 della Commissione, del 30 settembre 2013, che stabilisce il regolamento finanziario quadro degli organismi di cui all'articolo 208 del regolamento (UE, Euratom) n. 966/2012 del Parlamento europeo e del Consiglio (GU L 328 del 7.12.2013, pag. 42).

giorno e si astengono dal partecipare alle discussioni e alle votazioni inerenti tali punti.

3. L'Agenzia stabilisce nel proprio regolamento interno le disposizioni pratiche per le norme sulle dichiarazioni di interessi di cui ai paragrafi 1 e 2.

Articolo 23
Trasparenza

1. L'Agenzia svolge le proprie attività con un livello elevato di trasparenza e nel rispetto dell'articolo 25.

2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.

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

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

Articolo 24
Riservatezza

1. Fatto salvo l'articolo 25, l'Agenzia non rivela a terzi le informazioni da essa trattate o ricevute in relazione alle quali è stata presentata una richiesta motivata di trattamento riservato, integralmente o in parte.

2. I membri del consiglio di amministrazione, il direttore esecutivo, i membri del gruppo permanente di portatori di interessi, gli esperti esterni che partecipano ai gruppi di lavoro ad hoc e il personale dell'Agenzia, compresi i funzionari distaccati dagli Stati membri a titolo temporaneo, rispettano gli obblighi di riservatezza di cui all'articolo 339 del trattato sul funzionamento dell'Unione europea (TFUE) anche dopo la cessazione delle proprie funzioni.

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

4. Se necessario ai fini dell'esecuzione dei compiti dell'Agenzia, il consiglio di amministrazione decide di consentire all'Agenzia di trattare informazioni riservate. In questo caso, il consiglio di amministrazione, in accordo con i servizi della Commissione, adotta un regolamento interno che applichi i principi di sicurezza enunciati nelle decisioni (UE, Euratom) 2015/443[37] e 2015/444[38] della Commissione. Tale regolamento disciplina, tra l'altro, lo scambio, il trattamento e la conservazione di informazioni classificate.

---

37 Decisione (UE, Euratom) 2015/443 della Commissione, del 13 marzo 2015, sulla sicurezza nella Commissione (GU L 72 del 17.3.2015, pag. 41).

38 Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

Articolo 25
Accesso ai documenti

1. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dall'Agenzia.
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 formare oggetto di una denuncia presentata al Mediatore europeo a norma dell'articolo 228 TFUE o di un ricorso dinanzi alla Corte di giustizia dell'Unione europea a norma dell'articolo 263 TFUE.

CAPO III
FORMAZIONE E STRUTTURA DEL BILANCIO

Articolo 26
Formazione del bilancio

1. 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. Le entrate e le spese risultano in pareggio.
2. Ogni anno il consiglio di amministrazione elabora, sulla base del progetto di stato di previsione delle entrate e delle spese di cui al paragrafo 1, lo stato di previsione delle entrate e delle spese dell'Agenzia per l'esercizio finanziario successivo.
3. Entro il 31 gennaio di ogni anno il consiglio di amministrazione invia lo stato di previsione di cui al paragrafo 2, come parte integrante del progetto di documento unico di programmazione, alla Commissione e ai paesi terzi con cui l'Unione ha concluso accordi a norma dell'articolo 39.
4. Sulla base di tale stato di previsione, la Commissione iscrive le stime che ritiene necessarie per quanto concerne la tabella dell'organico e l'importo del contributo a carico del bilancio generale nel progetto di bilancio dell'Unione che sottopone al Parlamento europeo e al Consiglio conformemente all'articolo 314 TFUE.
5. Il Parlamento europeo e il Consiglio autorizzano gli stanziamenti a titolo del contributo destinato all'Agenzia.
6. Il Parlamento europeo e il Consiglio adottano la tabella dell'organico dell'Agenzia.
7. Insieme al documento unico di programmazione, il consiglio di amministrazione adotta il bilancio dell'Agenzia. Esso diventa definitivo dopo l'adozione definitiva del bilancio generale dell'Unione. Se del caso, il consiglio di amministrazione modifica il bilancio e il documento unico di programmazione dell'Agenzia per conformarli al bilancio generale dell'Unione.

Articolo 27
Struttura del bilancio

1. Fatte salve altre risorse, le entrate dell'Agenzia comprendono:

   (a) un contributo dal bilancio dell'Unione;

   (b) entrate con destinazione specifica volte a finanziare spese specifiche conformemente alla regolamentazione finanziaria di cui all'articolo 29;

   (c) finanziamenti dell'Unione sotto forma di accordi di delega o di sovvenzioni ad hoc secondo la regolamentazione finanziaria di cui all'articolo 29 e le disposizioni dei pertinenti strumenti di sostegno alle politiche dell'Unione;

   (d) contributi dei paesi terzi che partecipano ai lavori dell'Agenzia a norma dell'articolo 39;

   (e) eventuali contributi volontari degli Stati membri, in denaro o in natura; Gli Stati membri che versano contributi volontari non possono rivendicare alcun diritto o servizio specifico per effetto di tale contributo.

2. Le spese dell'Agenzia comprendono la retribuzione del personale, l'assistenza amministrativa e tecnica, le spese infrastrutturali e di esercizio, nonché quelle conseguenti a contratti stipulati con terzi.

Articolo 28
Esecuzione del bilancio

1. Il direttore esecutivo è responsabile dell'esecuzione del 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 (1° marzo dell'anno N + 1), il contabile dell'Agenzia comunica i conti provvisori al contabile della Commissione e alla Corte dei conti.
4. In seguito al ricevimento delle osservazioni della Corte dei conti sui conti provvisori dell'Agenzia, il contabile dell'Agenzia redige i conti definitivi sotto la propria responsabilità.
5. Il direttore esecutivo li presenta al consiglio di amministrazione per parere.
6. Entro il 31 marzo dell'anno N + 1, il direttore esecutivo trasmette la relazione sulla gestione di bilancio e finanziaria al Parlamento europeo, al Consiglio, alla Commissione e alla Corte dei conti.
7. Entro il 1° luglio dell'anno N + 1, il contabile trasmette i conti definitivi, accompagnati dal parere del consiglio di amministrazione, al Parlamento europeo, al Consiglio, al contabile della Commissione e alla Corte dei conti.
8. Allo scadere del termine previsto per la trasmissione dei conti definitivi, il contabile trasmette altresì alla Corte dei conti, e in copia al contabile della Commissione, una dichiarazione ad essi relativa.
9. Il direttore esecutivo pubblica i conti definitivi entro il 15 novembre dell'anno successivo.

10. Entro il 30 settembre dell'anno N + 1 il direttore esecutivo invia alla Corte dei conti una risposta alle osservazioni da essa formulate e ne trasmette copia al consiglio di amministrazione e alla Commissione.

11. Il direttore esecutivo presenta al Parlamento europeo, su richiesta di quest'ultimo, tutte le informazioni necessarie al corretto svolgimento della procedura di discarico per l'esercizio in oggetto, conformemente all'articolo 165, paragrafo 3, del regolamento finanziario.

12. Il Parlamento europeo, su raccomandazione del Consiglio, concede il discarico al direttore esecutivo, entro il 15 maggio dell'anno N + 2, per l'esecuzione del bilancio dell'esercizio N.

Articolo 29
Regolamentazione finanziaria

La regolamentazione finanziaria applicabile all'Agenzia è adottata dal consiglio di amministrazione previa consultazione della Commissione. Essa si discosta dal regolamento (UE) n. 1271/2013 solo per esigenze specifiche di funzionamento dell'Agenzia e previo accordo della Commissione.

Articolo 30
Lotta antifrode

1. Per facilitare la lotta contro la frode, la corruzione e altre attività illecite ai sensi del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio[39], entro sei mesi dalla data in cui diventa operativa l'Agenzia aderisce all'accordo interistituzionale del 25 maggio 1999 relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e adotta le opportune disposizioni valide per l'insieme dei dipendenti dell'Agenzia, utilizzando i modelli riportati nell'allegato di tale accordo.

2. La Corte dei conti ha il potere di revisione contabile, esercitabile sulla base di documenti e sul posto, su tutti i beneficiari di sovvenzioni, contraenti e subcontraenti cui l'Agenzia ha concesso finanziamenti dell'Unione.

3. L'OLAF può eseguire indagini, compresi controlli e verifiche sul posto, in conformità delle disposizioni e delle procedure stabilite dal regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio e dal regolamento (Euratom, CE) n. 2185/96 del Consiglio[40], dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari dell'Unione contro le frodi e altre irregolarità, per accertare casi di frode, corruzione o altre attività illecite lesive degli interessi finanziari dell'Unione in relazione a sovvenzioni o contratti finanziati dall'Agenzia.

---

39 Regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF) e che abroga il regolamento (CE) n. 1073/1999 del Parlamento europeo e del Consiglio e il regolamento (Euratom) n. 1074/1999 del Consiglio (GU L 248 del 18.9.2013, pag. 1).

40 Regolamento (Euratom, CE) n 2185/96 del Consiglio, dell'11 novembre 1996, relativo ai controlli e alle verifiche sul posto effettuati dalla Commissione ai fini della tutela degli interessi finanziari delle Comunità europee contro le frodi e altre irregolarità (GU L 292 del 15.11.1996, pag. 2).

4. Fatti salvi i paragrafi 1, 2 e 3, gli accordi di cooperazione con paesi terzi e organizzazioni internazionali, i contratti, le convenzioni di sovvenzione e le decisioni di sovvenzione dell'Agenzia contengono disposizioni che autorizzano esplicitamente la Corte dei conti e l'OLAF a procedere a tali revisioni contabili e indagini conformemente alle loro rispettive competenze.

CAPO IV
PERSONALE DELL'AGENZIA

Articolo 31
Disposizioni generali

Al personale dell'Agenzia si applicano lo statuto dei funzionari, il regime applicabile agli altri agenti e le norme adottate di comune accordo dalle istituzioni dell'Unione per dare applicazione a detto statuto.

Articolo 32
Privilegi e immunità

All'Agenzia e al suo personale si applica il protocollo n. 7 sui privilegi e sulle immunità dell'Unione europea allegato al trattato sull'Unione europea e al TFUE.

Articolo 33
Direttore esecutivo

1. Il direttore esecutivo è assunto come agente temporaneo dell'Agenzia ai sensi dell'articolo 2, lettera a), del regime applicabile agli altri agenti.
2. Il direttore esecutivo è nominato dal consiglio di amministrazione in base a un elenco di candidati proposto dalla Commissione, secondo una procedura di selezione aperta e trasparente.
3. Ai fini della conclusione del contratto del direttore esecutivo, l'Agenzia è rappresentata dal presidente del consiglio di amministrazione.
4. Prima di essere nominato, il candidato selezionato dal consiglio di amministrazione è invitato a fare una dichiarazione dinanzi alla commissione competente del Parlamento europeo e a rispondere alle domande dei deputati.
5. La durata del mandato del direttore esecutivo è di cinque anni. Entro la fine di tale periodo, la Commissione esegue una valutazione che tiene conto della prestazione del direttore esecutivo e dei compiti e delle sfide futuri dell'Agenzia.
6. Il consiglio di amministrazione adotta le decisioni riguardanti la nomina del direttore esecutivo, la proroga del suo mandato e la sua rimozione dall'incarico a maggioranza di due terzi dei suoi membri con diritto di voto.
7. Agendo su proposta della Commissione, la quale tiene conto della valutazione di cui al paragrafo 5, il consiglio di amministrazione può prorogare il mandato del direttore esecutivo una sola volta, per non più di cinque anni.
8. Il consiglio di amministrazione informa il Parlamento europeo dell'intenzione di prorogare il mandato del direttore esecutivo. Entro i tre mesi che precedono tale

proroga, il direttore esecutivo, se invitato, fa una dichiarazione davanti alla commissione competente del Parlamento europeo e risponde alle domande dei deputati.

9. Un direttore esecutivo il cui mandato sia stato prorogato non può partecipare a un'altra procedura di selezione per lo stesso posto.

10. Il direttore esecutivo può essere rimosso dall'incarico solo su decisione del consiglio di amministrazione, che agisce su proposta della Commissione.

Articolo 34
Esperti nazionali distaccati e altro personale

1. L'Agenzia può avvalersi di esperti nazionali distaccati o di altro personale non alle sue dipendenze. Lo statuto dei funzionari e il regime applicabile agli altri agenti non si applicano a tale personale.

2. Il consiglio di amministrazione adotta una decisione che stabilisce le norme relative al distacco di esperti nazionali presso l'Agenzia.

CAPO V
DISPOSIZIONI GENERALI

Articolo 35
Status giuridico dell'Agenzia

1. L'Agenzia è un organismo dell'Unione ed è dotata di personalità giuridica.

2. L'Agenzia gode, in ciascuno Stato membro, della più ampia capacità giuridica riconosciuta alle persone giuridiche dalla legislazione nazionale. In particolare, essa può acquistare o alienare beni mobili e immobili e può stare in giudizio.

3. L'Agenzia è rappresentata dal direttore esecutivo.

Articolo 36
Responsabilità dell'Agenzia

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

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

3. 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.

4. La Corte di giustizia dell'Unione europea è competente a conoscere delle controversie relative al risarcimento di tali danni.

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

Articolo 37

Regime linguistico

1. All'Agenzia si applicano le disposizioni previste dal regolamento n. 1 del Consiglio[41]. Gli Stati membri e gli altri organismi da essi designati possono rivolgersi all'Agenzia e ottenere la risposta in una delle lingue ufficiali delle istituzioni dell'Unione di loro scelta.

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

Articolo 38

Protezione dei dati personali

1. Il trattamento dei dati personali da parte dell'Agenzia è soggetto al regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[42].

2. Il consiglio di amministrazione adotta le misure di attuazione di cui all'articolo 24, paragrafo 8, del regolamento (CE) n. 45/2001. Il consiglio di amministrazione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (CE) n. 45/2001 da parte dell'Agenzia.

Articolo 39

Cooperazione con paesi terzi e organizzazioni internazionali

1. Se necessario ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'Agenzia può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'Agenzia può, previa approvazione da parte della Commissione, istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali. Detti accordi non creano obblighi giuridici per l'Unione e gli Stati membri.

2. L'Agenzia è aperta alla partecipazione di paesi terzi che hanno concluso con l'Unione accordi in tal senso. Nell'ambito delle pertinenti disposizioni di tali accordi, sono elaborate disposizioni che specificano, in particolare, la natura, la portata e le modalità di partecipazione di detti paesi ai lavori dell'Agenzia, comprese le disposizioni sulla partecipazione alle iniziative intraprese dall'Agenzia, sui contributi finanziari e sul personale. In materia di personale, tali disposizioni rispettano in ogni caso lo statuto dei funzionari.

3. Il consiglio di amministrazione adotta una strategia per le relazioni con paesi terzi o organizzazioni internazionali riguardo a questioni che rientrano tra le competenze dell'Agenzia. La Commissione garantisce che l'Agenzia operi nell'ambito del proprio mandato e del quadro istituzionale vigente stipulando un accordo di lavoro adeguato con il direttore esecutivo dell'Agenzia.

---

41 Regolamento n. 1 che stabilisce il regime linguistico della Comunità economica europea (GU 17 del 6.10.1958, pag. 401).

42 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).

Articolo 40

Norme di sicurezza per la protezione delle informazioni classificate e delle informazioni sensibili non classificate

In consultazione con la Commissione, l'Agenzia adotta le proprie norme di sicurezza applicando i principi di sicurezza contenuti nelle norme di sicurezza della Commissione per la protezione delle informazioni classificate UE (ICUE) e delle informazioni sensibili non classificate di cui alle decisioni (UE, Euratom) 2015/443 e 2015/444 della Commissione. Esse riguardano, tra l'altro, le disposizioni che disciplinano lo scambio, il trattamento e la conservazione di tali informazioni.

Articolo 41

Accordo sulla sede e condizioni operative

1. Le necessarie disposizioni relative all'insediamento dell'Agenzia nello Stato membro ospitante e alle strutture che quest'ultimo deve mettere a disposizione nonché le norme specifiche applicabili in tale Stato membro al direttore esecutivo, ai membri del consiglio di amministrazione, al personale dell'Agenzia e ai membri delle rispettive famiglie sono fissate in un accordo di sede concluso, previa approvazione del consiglio di amministrazione ed entro [due anni dall'entrata in vigore del presente regolamento].
2. Lo Stato membro che ospita l'Agenzia fornisce le migliori condizioni possibili al fine di garantire il corretto funzionamento dell'Agenzia, compresi l'accessibilità della sede, l'esistenza di strutture scolastiche adeguate per i figli del personale, un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi.

Articolo 42

Controllo amministrativo

L'operato dell'Agenzia è sottoposto al controllo del Mediatore in conformità dell'articolo 228 TFUE.

TITOLO III
QUADRO DI CERTIFICAZIONE DELLA CIBERSICUREZZA

Articolo 43

Sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza attestano che i prodotti e servizi TIC certificati nel loro ambito sono conformi a determinati requisiti per quanto riguarda la loro capacità di resistere, a un determinato livello di affidabilità, ad azioni volte a compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, processi, servizi e sistemi o accessibili tramite essi.

Articolo 44

Preparazione e adozione di un sistema europeo di certificazione della cibersicurezza

1. A seguito di una richiesta della Commissione, l'ENISA prepara un sistema europeo di certificazione della cibersicurezza che soddisfa i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento. Gli Stati membri o il gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza.
2. Nella preparazione delle proposte di sistemi di cui al paragrafo 1, l'ENISA consulta tutti i portatori di interessi e coopera strettamente con il gruppo. Il gruppo fornisce all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.
3. L'ENISA trasmette alla Commissione il sistema europeo di certificazione della cibersicurezza preparato in conformità del paragrafo 2.
4. La Commissione, sulla base del sistema proposto dall'ENISA, può adottare atti di esecuzione in conformità dell'articolo 55, paragrafo 2, prevedendo sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC che soddisfano i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.
5. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza e li pubblicizza.

Articolo 45

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza

I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da tener conto, se del caso, dei seguenti obiettivi di sicurezza:

(a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati;

(b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distribuzione accidentale o non autorizzata, dalla perdita accidentale o dall'alterazione;

(c) assicurare che le persone, i programmi o le macchine autorizzati possano accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

(d) registrare quali dati, funzioni o servizi sono stati comunicati, in quale momento e a chi;

(e) fare in modo che sia possibile verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso o che sono stati utilizzati, in quale momento e da chi;

(f) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;

(g) accertarsi che il software dei prodotti e dei servizi TIC sia aggiornato e non contenga vulnerabilità note e che tali prodotti e servizi dispongano di meccanismi per effettuare aggiornamenti del software protetti.

Articolo 46

Livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza

1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti e i servizi TIC rilasciati nel loro ambito uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato.

2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri:

(a) il livello di affidabilità di base si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità limitato riguardo alle qualità di cibersicurezza pretese o dichiarate di un prodotto o di un servizio TIC ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre il rischio di incidenti di cibersicurezza;

(b) il livello di affidabilità sostanziale si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità sostanziale riguardo alle qualità di cibersicurezza pretese o dichiarate di un prodotto o di un servizio TIC ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre in modo significativo il rischio di incidenti di cibersicurezza;

(c) il livello di affidabilità elevato si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità più elevato riguardo alle qualità di cibersicurezza pretese o dichiarate di un prodotto o di un servizio TIC rispetto ai certificati con livello di affidabilità sostanziale ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di prevenire gli incidenti di cibersicurezza.

Articolo 47

Elementi dei sistemi europei di certificazione della cibersicurezza

1. Un sistema europeo di certificazione della cibersicurezza comprende i seguenti elementi:

   (a) l'oggetto e l'ambito di applicazione della certificazione, compresi il tipo o le categorie di prodotti e servizi TIC coperti;

   (b) l'indicazione dettagliata dei requisiti di cibersicurezza rispetto ai quali i prodotti e servizi TIC sono valutati, ad esempio in riferimento a norme tecniche o a specifiche tecniche dell'Unione o internazionali;

   (c) se del caso, uno o più livelli di affidabilità;

   (d) i criteri e i metodi di valutazione specifici utilizzati, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti;

   (e) le informazioni che un richiedente deve fornire agli organismi di valutazione della conformità che sono necessarie per la certificazione;

   (f) le condizioni alle quali possono essere utilizzati gli eventuali marchi o etichette previsti dal sistema;

   (g) se la vigilanza rientra nel sistema, le norme per il controllo della conformità dei certificati ai requisiti, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;

   (h) le condizioni per il rilascio, il mantenimento, la prosecuzione e l'estensione della certificazione e la riduzione del suo campo di applicazione;

   (i) le regole riguardanti le conseguenze della non conformità dei prodotti e servizi TIC ai requisiti in materia di certificazione;

   (j) le regole riguardanti il modo in cui segnalare e trattare le vulnerabilità della cibersicurezza nei prodotti e servizi TIC precedentemente non rilevate;

   (k) le regole riguardanti la conservazione delle registrazioni da parte degli organismi di valutazione della conformità;

   (l) l'individuazione dei sistemi nazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti e servizi TIC;

   (m) il contenuto del certificato rilasciato.

2. I requisiti specificati del sistema non sono in contrasto con gli obblighi di legge applicabili, in particolare quelli derivanti dalla normativa armonizzata dell'Unione.

3. Se un atto specifico dell'Unione lo prevede, la certificazione nell'ambito di un sistema europeo di certificazione della cibersicurezza può essere utilizzata per dimostrare la presunzione di conformità agli obblighi imposti da tale atto.

4. In assenza di una normativa armonizzata dell'Unione, anche la legislazione degli Stati membri può disporre che un sistema europeo di certificazione della cibersicurezza può essere utilizzato per stabilire la presunzione di conformità agli obblighi di legge.

Articolo 48

Certificazione della cibersicurezza

1. I prodotti e i servizi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.
2. La certificazione è volontaria, salvo diversamente specificato nel diritto dell'Unione.
3. Un certificato europeo della cibersicurezza ai sensi del presente articolo è rilasciato dagli organismi di valutazione della conformità di cui all'articolo 51 sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza, adottato a norma dell'articolo 44.
4. In deroga al paragrafo 3, in casi debitamente giustificati un determinato sistema europeo della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è uno dei seguenti:
   (a) un'autorità nazionale di controllo della certificazione ai sensi dell'articolo 50, paragrafo 1;
   (b) un organismo accreditato come organismo di valutazione della conformità a norma dell'articolo 51, paragrafo 1, o
   (c) un organismo istituito in virtù di leggi, disposizioni legali o altre procedure amministrative dello Stato membro interessato che soddisfa i requisiti previsti per gli organismi che certificano prodotti, processi e servizi secondo la norma ISO/IEC 17065: 2012.
5. La persona fisica o giuridica che presenta i suoi prodotti o servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.
6. I certificati sono rilasciati per un periodo massimo di tre anni e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.
7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.

Articolo 49

Sistemi nazionali di certificazione della cibersicurezza e certificati nazionali della cibersicurezza

1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.

2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti e servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza in vigore.

3. I certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza restano validi fino alla loro data di scadenza.

Articolo 50
Autorità nazionali di controllo della certificazione

1. Ciascuno Stato membro designa un'autorità nazionale di controllo della certificazione.

2. Ciascuno Stato membro comunica alla Commissione l'identità dell'autorità designata.

3. Ciascuna autorità nazionale di controllo della certificazione, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila.

4. Gli Stati membri provvedono affinché le autorità nazionali di controllo della certificazione dispongano di risorse adeguate per l'esercizio dei loro poteri e l'esecuzione efficiente ed efficace dei compiti loro assegnati.

5. Ai fini dell'effettiva attuazione del regolamento, è opportuno che dette autorità partecipino in modo attivo, efficace, efficiente e sicuro al gruppo europeo per la certificazione della cibersicurezza istituito a norma dell'articolo 53.

6. Le autorità nazionali di controllo della certificazione:

   (a) sorvegliano e garantiscono l'applicazione delle disposizioni del presente titolo a livello nazionale e vigilano sulla conformità dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nei rispettivi territori ai requisiti fissati nel presente titolo e nel corrispondente sistema europeo di certificazione della cibersicurezza;

   (b) monitorano e supervisionano le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;

   (c) trattano i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio, svolgono le indagini opportune sull'oggetto del reclamo e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole.

   (d) cooperano con le altre autorità nazionali di controllo della certificazione o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi europei di certificazione della cibersicurezza;

   (e) sorvegliano gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza.

7. Ciascuna autorità nazionale di controllo della certificazione dispone almeno dei seguenti poteri:

   (a) richiedere agli organismi di valutazione della conformità e ai titolari di certificati europei della cibersicurezza di fornire le eventuali informazioni necessarie all'esecuzione dei suoi compiti;

   (b) condurre indagini, sotto forma di verifiche contabili, nei confronti degli organismi di valutazione della conformità e dei titolari dei certificati europei della cibersicurezza allo scopo di verificare l'osservanza delle disposizioni di cui al titolo III;

   (c) adottare misure appropriate, nel rispetto della legislazione nazionale, al fine di accertare che gli organismi di valutazione della conformità o i titolari di certificati si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

   (d) ottenere accesso a tutti i locali degli organismi di valutazione della conformità e dei titolari dei certificati europei della cibersicurezza al fine di espletare le indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;

   (e) revocare, in conformità del diritto nazionale, i certificati non conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

   (f) irrogare sanzioni a norma dell'articolo 54, conformemente al diritto nazionale, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento.

8. Le autorità nazionali di controllo della certificazione cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti e servizi TIC.

Articolo 51
Organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità sono accreditati dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 solo se soddisfano i requisiti indicati nell'allegato del presente regolamento.

2. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Gli organismi di accreditamento revocano l'accreditamento di un organismo di valutazione della conformità di cui al paragrafo 1 se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

Articolo 52
Notifica

1. Per ciascun sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44, le autorità nazionali di controllo della certificazione notificano alla Commissione gli organismi di valutazione della conformità accreditati a rilasciare i certificati a determinati livelli di affidabilità di cui all'articolo 46 e, senza indebiti ritardi, ogni successiva modifica degli stessi.
2. Un anno dopo l'entrata in vigore di un sistema europeo di certificazione della cibersicurezza, la Commissione pubblica nella Gazzetta ufficiale un elenco degli organismi di valutazione della conformità notificati.
3. Se la Commissione riceve una notifica dopo lo scadere del periodo di cui al paragrafo 2, pubblica nella Gazzetta ufficiale dell'Unione europea le modifiche dell'elenco di cui al paragrafo 2 entro due mesi dalla data di ricevimento di tale notifica.
4. Un'autorità nazionale di controllo della certificazione può presentare alla Commissione una richiesta di rimozione di un organismo di valutazione della conformità notificato dall'autorità stessa dall'elenco di cui al paragrafo 2. La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea le corrispondenti modifiche dell'elenco entro un mese dalla data di ricevimento della richiesta dell'autorità nazionale di controllo della certificazione.
5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 55, paragrafo 2.

Articolo 53
Gruppo europeo per la certificazione della cibersicurezza

1. È istituito il gruppo europeo per la certificazione della cibersicurezza (di seguito il "gruppo").
2. Il gruppo è composto dalle autorità nazionali di controllo della certificazione. Le autorità sono rappresentate dai capi o da rappresentanti ad alto livello delle autorità nazionali di controllo della certificazione.
3. Il gruppo ha i seguenti compiti:
   (a) consigliare e coadiuvare la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti delle disposizioni del presente titolo, in particolare per quanto riguarda le questioni relative alla politica in materia di certificazione della cibersicurezza, al coordinamento degli approcci politici e alla preparazione dei sistemi europei di certificazione della cibersicurezza;
   (b) assistere, consigliare e collaborare con l'ENISA in relazione alla preparazione di una proposta di sistema conformemente all'articolo 44 del presente regolamento;
   (c) proporre alla Commissione di chiedere all'Agenzia di preparare una proposta di sistema europeo di certificazione della cibersicurezza conformemente all'articolo 44 del presente regolamento;

(d) adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza.

(e) esaminare gli sviluppi che presentano un interesse in materia di certificazione della cibersicurezza e scambio di buone pratiche sui sistemi di certificazione della cibersicurezza;

(f) agevolare la cooperazione tra le autorità nazionali di controllo della certificazione di cui al presente titolo attraverso lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente scambio di informazioni in relazione a tutti gli aspetti riguardanti la certificazione della cibersicurezza.

4. La Commissione presiede il gruppo, per il quale svolge le funzioni di segretariato, con l'assistenza dell'ENISA conformemente all'articolo 8, lettera a).

Articolo 54
Sanzioni

Gli Stati membri stabiliscono le norme sulle sanzioni da irrogare in caso di violazione del presente titolo e dei sistemi europei di certificazione della cibersicurezza e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano [entro il …/senza indugio] tali norme e misure alla Commissione, nonché eventuali successive modifiche delle stesse.

TITOLO IV
DISPOSIZIONI FINALI

Articolo 55
Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 56
Valutazione e riesame

1. Entro cinque anni dalla data di cui all'articolo 58, e successivamente ogni cinque anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'Agenzia e delle sue prassi di lavoro, come pure l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro pervenuto all'Agenzia in relazione alle sue attività. Se ritiene che il mantenimento dell'Agenzia non sia più giustificato rispetto agli obiettivi, al mandato e ai compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'Agenzia.
2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti e servizi TIC nell'Unione e di migliorare il funzionamento del mercato interno.
3. La Commissione trasmette la relazione di valutazione unitamente alle sue conclusioni al Parlamento europeo, al Consiglio e al consiglio di amministrazione. I risultati della valutazione sono resi pubblici.

Articolo 57
Abrogazione e sostituzione

1. Il regolamento (CE) n. 526/2013 è abrogato con effetto a decorrere dal [….].
2. I riferimenti al regolamento (CE) n. 526/2013 e all'ENISA si intendono fatti al presente regolamento e all'Agenzia.
3. L'Agenzia sostituisce l'Agenzia istituita dal regolamento (CE) n. 526/2013 per quanto riguarda diritti di proprietà, accordi, obblighi di legge, contratti di lavoro, impegni finanziari e responsabilità. Tutte le decisioni già prese dal consiglio di amministrazione e dal comitato esecutivo restano valide, purché non siano in conflitto con le disposizioni del presente regolamento.
4. L'Agenzia è istituita per un periodo di tempo indeterminato a decorrere dal […].

5. Il direttore esecutivo nominato a norma dell'articolo 24, paragrafo 4, del regolamento (CE) n. 526/2013 è il direttore esecutivo dell'Agenzia per la restante durata del mandato.

6. I membri del consiglio di amministrazione e i loro supplenti nominati a norma dell'articolo 6 del regolamento (CE) n. 526/2013 sono i membri e i rispettivi supplenti del consiglio di amministrazione dell'Agenzia per la restante durata del mandato.

Articolo 58

Entrata in vigore

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

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

Fatto a Bruxelles, il

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

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")

1.2. Settore/settori interessati

Settore: 09 - Reti di comunicazione, contenuti e tecnologie

Attività: 09.02 Mercato unico digitale

1.3. Natura della proposta/iniziativa

☒ La proposta/iniziativa riguarda **una nuova azione (Titolo III - Certificazione)**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[43]

☒La proposta/iniziativa riguarda **la proroga di un'azione esistente**(**Titolo II – Mandato di ENISA)**

☐ 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

1. Aumentare la resilienza degli Stati membri, delle imprese e dell'UE nel suo insieme

2. Garantire il corretto funzionamento del mercato interno per i prodotti e i servizi TIC

3. Aumentare la competitività globale delle imprese dell'UE che operano nel settore delle TIC

4. Ravvicinare le disposizioni legislative, regolamentari e amministrative degli Stati membri che hanno bisogno di cibersicurezza

1.4.2. Obiettivi specifici

Alla luce degli obiettivi generali, nel più ampio contesto della nuova strategia per la cibersicurezza, lo strumento, che definisce la portata e il mandato dell'ENISA e che istituisce un quadro europeo di certificazione per i prodotti e i servizi TIC, intende raggiungere i seguenti obiettivi specifici:

1. accrescere le **capacità e la preparazione** degli Stati membri e delle imprese;
2. migliorare **la cooperazione e il coordinamento** tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE;
3. aumentare **le capacità a livello dell'UE per integrare l'azione degli Stati membri**, in particolare in caso di crisi informatiche transfrontaliere;
4. accrescere la **consapevolezza** di cittadini e imprese sulle questioni riguardanti la cibersicurezza;

[43] A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

5. rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale aumentando la **trasparenza complessiva dell'affidabilità in termini di cibersicurezza**[44] dei prodotti e servizi TIC.

L'ENISA contribuirà al raggiungimento degli obiettivi di cui sopra mediante:

Un **maggiore sostegno all'elaborazione delle politiche** – fornirà orientamenti e consulenze alla Commissione e agli Stati membri per l'aggiornamento e la definizione di un quadro normativo globale nel campo della cibersicurezza, nonché delle politiche e iniziative settoriali in materia di cibersicurezza; contribuirà ai lavori del gruppo di cooperazione (articolo 11 della direttiva (UE) 2016/1148), fornendo consulenza e assistenza; sosterrà lo sviluppo e l'attuazione delle politiche in materia di identificazione elettronica e servizi fiduciari; promuoverà lo scambio delle migliori pratiche tra le autorità locali.

Un **maggiore sostegno allo sviluppo delle capacità** – fornirà sostegno agli Stati membri alle istituzioni, agli organismi, agli uffici e alle agenzie dell'Unione per sviluppare e migliorare la prevenzione, l'individuazione e l'analisi di problemi e incidenti in materia di cibersicurezza e la capacità di reazione agli stessi; assisterà gli Stati membri, su loro richiesta, nello sviluppo di CSIRT nazionali e di strategie nazionali in materia di cibersicurezza; assisterà le istituzioni dell'Unione nell'elaborazione e revisione delle strategie in materia di sicurezza informatica dell'Unione; offrirà formazioni in materia di sicurezza informatica; assisterà gli Stati membri mediante il gruppo di cooperazione nello scambio di buone pratiche; agevolerà la creazione di centri settoriali di condivisione e di analisi delle informazioni (ISAC).

La **cooperazione operativa e il sostegno alla gestione delle crisi** – sosterrà la cooperazione tra gli organismi pubblici competenti e tra i portatori d'interessi grazie a una cooperazione sistematica con le istituzioni, gli organismi, gli uffici e le agenzie dell'Unione che si occupano di cibersicurezza, criminalità informatica e della tutela della vita privata e protezione dei dati personali; assicurerà il segretariato della rete di CSIRT (art. 12, paragrafo 2, della direttiva (UE) 2016/1148) e contribuirà alla cooperazione operativa all'interno della rete, fornendo, in cooperazione con la CERT-UE, sostegno agli Stati membri su loro richiesta; organizzerà periodiche esercitazioni in materia di cibersicurezza; contribuirà alla messa a punto di una cooperazione transfrontaliera su vasta scala in risposta a incidenti e crisi che minacciano la cibersicurezza; svolgerà, in cooperazione con la rete di CSIRT, indagini tecniche ex post nel caso di incidenti significativi e formulerà raccomandazioni sulle azioni di seguito da intraprendere;

Funzioni connesse al mercato (normazione, certificazione) – svolgerà una serie di funzioni, in particolare sostenendo il mercato interno: "osservatorio del mercato" della cibersicurezza, analizzando l'evoluzione del mercato della sicurezza informatica per conciliare meglio domanda e offerta; sosterrà e promuoverà lo sviluppo e l'attuazione della politica dell'Unione in materia di cibersicurezza, la certificazione di prodotti e servizi TIC attraverso la preparazione di proposte di sistemi europei di certificazione per i prodotti e i servizi delle TIC, assicurando il segretariato del gruppo europeo per la certificazione della cibersicurezza, fornendo orientamenti e buone pratiche in materia di requisiti di sicurezza dei prodotti e servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e l'industria;

[44] Per trasparenza della affidabilità in termini di cibersicurezza si intende fornire agli utenti informazioni sufficienti sulla proprietà di cibersicurezza, il che permette loro di stabilire oggettivamente il livello di sicurezza di un determinato prodotto, servizio o processo nel settore delle TIC.

Migliorare la conoscenza e l'informazione e aumentare la consapevolezza – fornirà 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 ai portatori d'interessi dell'industria. Ciò presuppone anche la messa in comune, l'organizzazione e la messa a disposizione del pubblico, tramite un portale dedicato, di informazioni in materia di sicurezza delle reti e dei sistemi informativi [o in materia di cibersicurezza]. Un altro elemento importante sono le attività e le campagne di sensibilizzazione destinate al grande pubblico circa i rischi relativi alla cibersicurezza.

Un **maggiore sostegno alla ricerca e all'innovazione** – fornirà consulenza sulle esigenze di ricerca e sulla definizione delle priorità nel settore della sicurezza informatica;

Sostegno alla cooperazione internazionale – sosterrà gli sforzi dell'Unione per cooperare con i paesi terzi e le organizzazioni internazionali per promuovere la cooperazione internazionale in materia di sicurezza informatica.

CERTIFICAZIONE

Il quadro della certificazione contribuirà a conseguire gli obiettivi migliorando la **trasparenza complessiva dell'affidabilità della cibersicurezza**[45] dei prodotti e dei servizi TIC, al fine di rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale. Ciò dovrebbe anche contribuire a evitare la frammentazione dei sistemi di certificazione nell'UE così come dei relativi requisiti di sicurezza e dei criteri di valutazione nei vari Stati membri e settori.

1.4.3. Risultati e incidenza previsti

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

Un'ENISA rafforzata (che sostiene le capacità, la prevenzione, la cooperazione e la consapevolezza a livello di UE e, pertanto, è finalizzata ad aumentare la ciberresilienza globale dell'UE) e che sostiene inoltre il quadro dell'UE in materia di certificazione dei prodotti e servizi TIC avrà prevedibilmente i seguenti impatti (elenco non esaustivo):

Impatto complessivo:

– Impatto positivo complessivo sul mercato interno grazie alla riduzione della frammentazione del mercato e la creazione di fiducia nelle tecnologie digitali grazie a una migliore cooperazione, a una maggiore armonizzazione degli approcci alle politiche dell'UE in materia di cibersicurezza e all'aumento di capacità a livello dell'UE. Ciò dovrebbe tradursi in un impatto economico positivo grazie alla riduzione dei costi della cibersicurezza/cibercriminalità, per i quali l'impatto economico stimato nell'Unione è pari allo 0,41% del PIL dell'UE (ossia circa 55 miliardi di EUR).

Risultati specifici:

Maggiori capacità e migliore preparazione degli Stati membri e delle imprese in materia di cibersicurezza

– Maggiori capacità e migliore preparazione degli Stati membri in materia di cibersicurezza (mediante un'analisi strategica a lungo termine delle minacce e degli incidenti informatici, l'orientamento e le relazioni, l'intermediazione di esperienze e di

[45] Per trasparenza dell'affidabilità in termini di cibersicurezza si intende fornire agli utenti informazioni sufficienti sulle caratteristiche di cibersicurezza, il che permette loro di stabilire oggettivamente il livello di sicurezza di un determinato prodotto, servizio o processo nel settore delle TIC.

buone pratiche, la formazione e la disponibilità di materiali di formazione, le esercitazioni potenziate di CyberEurope)

– Maggiori capacità degli operatori privati grazie al sostegno all'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) in vari settori.

– Migliore preparazione dell'UE in materia di cibersicurezza e degli Stati membri grazie alla disponibilità di piani approvati e ben collaudati per il caso di incidenti di cibersicurezza transfrontaliera su vasta scala testati in esercitazioni CyberEurope;

Migliore cooperazione e coordinamento tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE

– Migliore cooperazione all'interno e tra i settori pubblico e privato.

– Maggiore coerenza di approccio all'attuazione della direttiva NIS a livello transfrontaliero e transettoriale.

– Migliore cooperazione in materia di certificazione grazie a un quadro istituzionale che permetta lo sviluppo di sistemi di certificazione della cibersicurezza e lo sviluppo di una politica comune in materia.

Una maggiore capacità a livello di UE di integrare l'azione degli Stati membri

– Migliore "capacità operativa dell'UE" di integrare le azioni degli Stati membri e sostenerle, su richiesta e in relazione a servizi limitati e predeterminati. Ciò dovrebbe avere un impatto positivo sul successo della prevenzione degli incidenti, dell'individuazione e della risposta, sia a livello di Stati membri che a livello dell'Unione.

Accresciuta consapevolezza di cittadini e imprese sulle questioni riguardanti la cibersicurezza.

– Accresciuta consapevolezza di cittadini e imprese sulle questioni riguardanti la cibersicurezza.

– Migliore capacità di prendere decisioni informate di acquisto relative a prodotti e servizi TIC grazie alla certificazione della cibersicurezza.

Fiducia rafforzata nel mercato unico digitale e nell'innovazione digitale grazie all'aumento della trasparenza complessiva dell'affidabilità in termini di cibersicurezza dei prodotti e servizi TIC.

– Maggiore trasparenza dell'affidabilità della cibersicurezza[46] dei prodotti e dei servizi TIC grazie alla semplificazione delle procedure di certificazione di sicurezza attraverso un quadro normativo a livello dell'UE.

– Maggiore livello di affidabilità delle caratteristiche di sicurezza dei prodotti e servizi TIC.

– Maggiore diffusione della certificazione della cibersicurezza incentivata da procedure semplificate, dalla riduzione dei costi e da una prospettiva di opportunità commerciali a livello dell'UE non ostacolata dalla frammentazione del mercato.

– Maggiore competitività nel mercato della cibersicurezza dell'UE grazie a una riduzione dei costi e degli oneri amministrativi per le PMI e l'eliminazione di potenziali ostacoli all'accesso al mercato dovuti all'esistenza di numerosi sistemi di certificazione nazionali.

[46] Per trasparenza della affidabilità in termini di cibersicurezza si intende fornire agli utenti informazioni sufficienti sulla proprietà di cibersicurezza, il che permette loro di stabilire oggettivamente il livello di sicurezza di un determinato prodotto, servizio o processo nel settore delle TIC.

Altro

– Non si prevede un impatto ambientale significativo per nessuno degli obiettivi fissati.

– Per quanto riguarda il bilancio dell'UE, è possibile conseguire una maggiore efficienza attraverso una cooperazione e un coordinamento maggiori delle attività tra istituzioni, agenzie e organismi dell'UE.

1.4.4. Indicatori di risultato e di incidenza

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

(a)

Obiettivo: Accrescere le capacità e la preparazione degli Stati membri e delle imprese:

- Numero di formazioni organizzate dall'ENISA
- Copertura geografica (numero di paesi e aree) dell'assistenza diretta fornita dall'ENISA
- Livello di preparazione raggiunto dagli Stati membri in termini di maturità dei CSIRT e di vigilanza delle misure di regolamentazione in materia di sicurezza informatica.
- Numero di buone pratiche a livello dell'UE per le infrastrutture critiche da parte dell'ENISA
- Numero di buone pratiche a livello dell'UE per le PMI da parte dell'ENISA
- Pubblicazione di analisi strategica annuale delle minacce e degli incidenti informatici per individuare le tendenze emergenti dall'ENISA
- Contributo regolare dell'ENISA al lavoro dei gruppi di lavoro in materia di cibersicurezza degli organismi europei di normazione (OEN).

Obiettivo: Migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, gli organismi e le agenzie dell'UE

- Numero di Stati membri che si sono avvalsi delle raccomandazioni e dei pareri dell'Agenzia nell'ambito del processo decisionale
- Numero di istituzioni, agenzie e organi dell'UE che si sono avvalsi delle raccomandazioni e dei pareri dell'Agenzia nell'ambito del processo decisionale
- Regolare attuazione del programma di lavoro della rete di CSIRT e buon funzionamento delle infrastrutture IT e dei canali di comunicazione della rete di CSIRT
- Numero di relazioni tecniche messe a disposizione e utilizzate dal gruppo di cooperazione
- Approccio coerente all'attuazione della direttiva NIS a livello transfrontaliero e transettoriale
- Numero di valutazioni della conformità normativa svolte dall'ENISA
- Numero di centri ISAC in vari settori, in particolare per le infrastrutture critiche
- Creazione e regolare funzionamento della piattaforma d'informazione, di diffusione delle informazioni in materia di cibersicurezza derivanti dalle istituzioni, agenzie e organi dell'UE

- Contributo regolare alla preparazione dei programmi di lavoro per la ricerca e l'innovazione dell'UE
- Accordo di cooperazione in vigore tra l'ENISA, l'EC3 e del CERT-UE
- Numero di sistemi di certificazione inseriti e sviluppati nell'ambito del quadro

Obiettivo: Aumentare le capacità a livello dell'UE di integrare l'azione degli Stati membri, in particolare in caso di crisi informatiche transfrontaliere.

- Pubblicazione di analisi strategica annuale delle minacce e degli incidenti informatici per individuare le tendenze emergenti dall'ENISA
- Pubblicazione di informazioni aggregate sugli incidenti segnalati ai sensi della direttiva NIS dall'ENISA
- Numero di esercitazioni paneuropee coordinate dall'Agenzia e numero di Stati membri e organizzazioni partecipanti.
- Numero di richieste di sostegno all'ENISA da parte degli Stati membri in caso di emergenza e soddisfatte dall'Agenzia
- Numero di analisi delle vulnerabilità, artefatti e incidenti effettuate dall'ENISA in cooperazione con la CERT-UE.
- La disponibilità, a livello UE, di rapporti di situazione, sulla base delle informazioni messe a disposizione dell'ENISA dagli Stati membri e da altri soggetti, in caso di incidenti informatici su vasta scala a livello transfrontaliero.

Obiettivo: Accrescere la consapevolezza di cittadini e imprese sulle questioni riguardanti la cibersicurezza.

- Svolgimento periodico di campagne di sensibilizzazione a livello nazionale e a livello UE e aggiornamento periodico dei temi in funzione delle nuove esigenze in termini di apprendimento.
- Aumento della consapevolezza nel settore della sicurezza informatica tra i cittadini dell'UE.
- Svolgimento periodico di quiz sulla consapevolezza in materia di cibersicurezza e aumento nel corso del tempo della percentuale di risposte corrette.
- Pubblicazione periodica di buone pratiche sulla cibersicurezza e sull'igiene informatica destinate ai dipendenti e alle organizzazioni.

Obiettivo: Rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale aumentando la trasparenza complessiva dell'affidabilità in termini di cibersicurezza[47] dei prodotti e servizi TIC.

- Numero di sistemi che aderiscono al quadro dell'UE
- Riduzione dei costi per ottenere un certificato di sicurezza delle TIC.
- Numero di organismi di valutazione della conformità specializzati in materia di certificazione delle TIC in tutti gli Stati membri.
- Costituzione del gruppo europeo per la certificazione della cibersicurezza e

[47] Per trasparenza dell'affidabilità in termini di cibersicurezza si intende fornire agli utenti informazioni sufficienti sulle caratteristiche di cibersicurezza, il che permette loro di stabilire oggettivamente il livello di sicurezza di un determinato prodotto, servizio o processo nel settore delle TIC.

organizzazione di riunioni regolari.

- Orientamenti per la certificazione in base al quadro dell'UE in vigore.
- Pubblicazione periodica di analisi delle principali tendenze nel mercato della cibersicurezza dell'UE.
- Numero di prodotti e servizi TIC certificati in base alle norme del quadro europeo di certificazione della sicurezza delle TIC.
- Aumento del numero di utenti finali che sono a conoscenza di elementi di sicurezza dei prodotti e servizi TIC.

(b)

1.4.5. Necessità nel breve e lungo termine

Alla luce dei requisiti regolamentari e della rapida evoluzione degli scenari relativi alle minacce alla cibersicurezza, è opportuno rivedere il mandato dell'ENISA per stabilire una serie rinnovata di compiti e funzioni, al fine di sostenere in modo efficace ed efficiente gli sforzi degli Stati membri, delle istituzioni dell'UE e degli altri portatori d'interessi volti a garantire un ciberspazio sicuro all'interno dell'Unione europea. Il campo di applicazione proposto per il mandato è definito, rafforzando quei settori in cui l'Agenzia ha dimostrato un chiaro valore aggiunto e integrandolo con i nuovi settori in cui è necessario un supporto alla luce delle nuove priorità politiche e dei nuovi strumenti, in particolare la direttiva NIS, il riesame della strategia dell'UE per la cibersicurezza, il prossimo programma di sicurezza informatica dell'UE per la cooperazione in caso di crisi cibernetica e la certificazione della cibersicurezza delle TIC. La proposta di nuovo mandato intende conferire all'Agenzia un ruolo più forte e centrale, in particolare anche sostenendo più fattivamente gli Stati membri nel contrastare le minacce (capacità operativa) e diventando un centro specializzato volto a sostenere gli Stati membri e la Commissione in materia di certificazione della cibersicurezza.

Al contempo, la proposta istituisce un quadro di certificazione europea della cibersicurezza per i prodotti e i servizi TIC e precisa le funzioni essenziali e i compiti dell'ENISA nel settore della certificazione della cibersicurezza. Il quadro stabilisce disposizioni e procedure comuni che permettano la creazione di sistemi di certificazione sulla cibersicurezza a livello dell'UE per specifici prodotti/servizi TIC o i rischi relativi alla cibersicurezza. La creazione di sistemi di certificazione della cibersicurezza conformi al quadro generale significherà che i certificati rilasciati nell'ambito di tali sistemi saranno validi e riconosciuti in tutti gli Stati membri e permetterà di affrontare l'attuale frammentazione del mercato.

1.4.6. Valore aggiunto dell'intervento dell'Unione

La sicurezza informatica è un problema di portata globale e di natura transfrontaliera e sta diventando sempre più intersettoriale a motivo delle interdipendenze tra le reti e i sistemi informativi. Il numero, la complessità e la portata degli incidenti connessi alla cibersicurezza e il loro impatto sull'economia e la società stanno crescendo nel tempo e si prevede un ulteriore aumento parallelo agli sviluppi tecnologici, ad esempio la diffusione dell'internet degli oggetti. Ne consegue che la necessità di un maggiore sforzo comune degli Stati membri, le istituzioni dell'UE, i portatori d'interessi del settore privato per affrontare le minacce alla cibersicurezza non dovrebbe diminuire in futuro.

Sin dalla sua istituzione nel 2004 l'ENISA ha avuto l'obiettivo di promuovere la cooperazione tra gli Stati membri e i portatori d'interessi in materia di NIS, compreso il

sostegno alla cooperazione tra pubblico e privato. Questo sostegno alla cooperazione, inclusi i lavori tecnici per fornire un quadro a livello dell'UE degli scenari di minaccia, la creazione di gruppi di esperti e l'organizzazione di incidenti informatici paneuropei ed esercitazioni di gestione delle crisi per i settori pubblico e privato (in particolare gli esercizi di simulazione "Cyber Europe"). La direttiva NIS ha affidato compiti supplementari all'ENISA, compreso il ruolo di segretariato della rete di CSIRT, per la cooperazione operativa tra gli Stati membri.

Il valore aggiunto di un'azione a livello di UE, in particolare per migliorare la cooperazione tra Stati membri, ma anche tra le comunità NIS è stato riconosciuto nelle conclusioni del Consiglio[48] del 2016 e 2017 e emerge anche chiaramente dalla valutazione dell'ENISA, il che dimostra che il valore aggiunto dell'Agenzia risiede principalmente nella sua capacità di migliorare la cooperazione tra questi soggetti. Nessun altro organismo sostiene – a livello dell'UE – la cooperazione di una comunità così ampia di portatori d'interessi nel settore della direttiva NIS.

Il valore aggiunto dell'ENISA nel riunire comunità e portatori d'interessi nel campo della cibersicurezza è valido anche nel settore della certificazione. L'aumento della criminalità informatica e le minacce alla cibersicurezza ha portato ad iniziative nazionali in materia di cibersicurezza che stabiliscono requisiti di alto livello di cibersicurezza e di certificazione per i componenti ITC utilizzati nelle infrastrutture tradizionali. Benché importanti, queste iniziative rischiano di provocare la frammentazione del mercato unico e di introdurre ostacoli all'interoperabilità. Un fornitore di TIC potrebbe dover sottoporsi a diversi processi di certificazione per essere in grado di vendere in diversi Stati membri. L'inefficacia/inefficienza degli attuali sistemi di certificazione non sembra poter essere ovviata in assenza di un intervento dell'UE. In assenza di azione, la frammentazione del mercato è molto probabilmente destinata ad aumentare nel medio termine (nei prossimi 5-10 anni) con l'emergere di nuovi sistemi di certificazione. La mancanza di coordinamento e interoperabilità fra tali sistemi è un elemento che riduce il potenziale del mercato unico digitale. Ciò dimostra il valore aggiunto dell'istituzione di un quadro europeo per la certificazione della cibersicurezza per i prodotti e i servizi TIC, ponendo le giuste condizioni per affrontare efficacemente i problemi legati alla coesistenza di molteplici procedure di certificazione in diversi Stati membri, riducendo i costi di certificazione, e, quindi, rendendo la certificazione più interessante da un punto di vista commerciale e concorrenziale nell'insieme dell'UE.

1.4.7. Insegnamenti tratti da esperienze analoghe

Conformemente alla base giuridica dell'ENISA, la Commissione ha proceduto a una valutazione dell'Agenzia, che comprende uno studio indipendente e una consultazione pubblica. La valutazione è giunta alla conclusione che gli obiettivi dell'ENISA rimangono d'attualità. In un contesto di sviluppi tecnologici e di evoluzione delle minacce e di un grande bisogno di una maggiore sicurezza delle reti e dell'informazione (NIS) nell'UE, si rendono necessarie competenze tecniche sull'evoluzione degli aspetti della sicurezza delle reti e dell'informazione. È necessario rafforzare la capacità degli Stati membri di capire e di rispondere alle minacce e i portatori d'interessi dovranno cooperare nei vari settori tematici e a livello interistituzionale.

[48] "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza" - conclusioni del Consiglio del 15 novembre 2016.

L'Agenzia ha contribuito con successo ad aumentare la sicurezza delle reti e dell'informazione in Europa, grazie all'offerta di capacità in 28 Stati membri, il rafforzamento della cooperazione tra gli Stati membri e i portatori d'interessi in materia di NIS, la messa a disposizione di competenze, la creazione di comunità e il sostegno alle politiche.

Benché l'ENISA abbia certamente avuto un impatto, almeno in certa misura, nel vasto campo della sicurezza delle reti e dell'informazione, essa non è pienamente riuscita a sviluppare una solida reputazione né ad acquisire una visibilità sufficiente per essere riconosciuta come "il" centro di competenza in Europa. La spiegazione va trovata nell'ampio mandato dell'ENISA, che non è stata dotata di risorse sufficienti in relazione ai suoi compiti. Inoltre, l'ENISA rimane l'unica agenzia dell'Unione europea con un mandato a tempo determinato, il che limita la sua capacità di elaborare una visione a lungo termine e assistere i portatori d'interessi in modo sostenibile. Tale situazione è anche in contrasto con le disposizioni della direttiva NIS che affida a ENISA compiti senza alcuna data di scadenza.

Attualmente non esiste un quadro europeo per quanto riguarda la certificazione della cibersicurezza per i prodotti e i servizi TIC. Tuttavia, l'aumento della criminalità informatica e le minacce per la sicurezza ha portato all'emergere di iniziative nazionali, il che crea il rischio di frammentazione del mercato unico.

1.4.8. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

L'iniziativa è altamente coerente con le politiche esistenti, in particolare nel settore del mercato interno. Infatti, secondo l'approccio globale alla cibersicurezza, quale definito dalla revisione della strategia per il mercato unico digitale, al fine di integrare un'ampia serie di misure, come ad esempio la revisione della strategia dell'UE per la cibersicurezza, il piano per la cooperazione in caso di crisi informatiche e le iniziative volte a combattere la criminalità informatica. Ciò dovrebbe garantire l'allineamento con le disposizioni esistenti in materia di cibersicurezza, in particolare la direttiva NIS, nonché lo sviluppo delle stesse, al fine di perseguire ulteriormente la resilienza informatica dell'UE attraverso una maggiore capacità, cooperazione, gestione dei rischi e consapevolezza nel settore della cibersicurezza.

Le proposte di misure di certificazione dovrebbero affrontare la potenziale frammentazione dovuta ai sistemi nazionali di certificazione esistenti ed emergenti, contribuendo così allo sviluppo del mercato unico digitale. L'iniziativa sostiene anche e integra l'attuazione della direttiva NIS, dotando le imprese soggette a tale direttiva di uno strumento molto utile per dimostrare la conformità con le disposizioni in materia di NIS in tutta l'Unione.

Il quadro di certificazione europea delle TIC in materia di cibersicurezza, come proposto, non pregiudica il regolamento generale sulla protezione dei dati (RGPD)[49] e, in particolare, le disposizioni pertinenti in materia di certificazione[50] applicabili per quanto riguarda la sicurezza del trattamento dei dati personali. Da ultimo, ma non meno importante, per quanto possibile i sistemi proposti nel futuro quadro europeo dovrebbero basarsi sulle

[49] Regolamento (UE) 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[50] Quali gli articoli 42 (certificazione) e 43 (organismi di certificazione), nonché agli articoli 57, 58 e 70 riguardanti rispettivamente le funzioni e i poteri dell'autorità di controllo indipendente e i compiti del comitato europeo per la protezione dei dati.

norme tecniche internazionali in modo da evitare la creazione di ostacoli al commercio e garantire la coerenza con le iniziative internazionali.

1.5. Durata e incidenza finanziaria

☐ Proposta/iniziativa di **durata limitata**

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

– ☐ Incidenza finanziaria dal AAAA al AAAA

☒ Proposta/iniziativa di **durata illimitata**

– Attuazione con un periodo di avviamento dal 2019 al 2020

– e successivo funzionamento a pieno ritmo.

1.6. Modalità di gestione previste[51]

☒ **Gestione diretta** della Commissione (Titolo III – Certificazione)

– ☐ agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☒ **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

☐ a organizzazioni internazionali e rispettive agenzie (specificare);

☐ alla BEI e al Fondo europeo per gli investimenti;

☒ agli organismi di cui agli articoli 208 e 209 (Titolo II - ENISA);

☐ a organismi di diritto pubblico;

☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui presentano sufficienti garanzie finanziarie;

☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che presentano sufficienti garanzie finanziarie;

☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC a norma del titolo V del TUE, che devono essere indicate nel pertinente atto di base.

Osservazioni

Il regolamento contempla i seguenti elementi: - il Titolo II del regolamento proposto rivede il mandato dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), attribuendole un ruolo importante in materia di certificazione, mentre - il Titolo III istituisce un quadro di riferimento per la creazione di sistemi di certificazione della cibersicurezza dei prodotti e servizi TIC, in cui l'ENISA svolge un ruolo fondamentale.

[51] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

Il monitoraggio avrà inizio subito dopo l'adozione dello strumento giuridico e si concentrerà sulla sua applicazione. La Commissione organizzerà riunioni con l'ENISA, con i rappresentanti degli Stati membri (ad es. gruppo di esperti) e i pertinenti portatori d'interessi, in particolare allo scopo di agevolare l'applicazione delle norme in materia di certificazione quali l'istituzione del consiglio di amministrazione.

La prima valutazione dovrebbe aver luogo 5 anni dopo l'entrata in vigore dello strumento giuridico, nella misura in cui siano disponibili dati sufficienti. Un'esplicita clausola di revisione e di valutazione [articolo XXX], con cui la Commissione eseguirà una valutazione indipendente, è inclusa nello strumento giuridico. Successivamente la Commissione riferisce al Parlamento europeo e al Consiglio sulla sua valutazione corredata se del caso di una proposta per il riesame, al fine di misurare l'impatto del regolamento e il suo valore aggiunto. Ulteriori valutazioni dovrebbero aver luogo ogni cinque anni. Sarà applicata la metodologia di valutazione della Commissione volta a "Legiferare meglio". Tali valutazioni saranno realizzate con l'aiuto di studi mirati, discussioni con esperti e ampie consultazioni con i portatori d'interessi.

Il direttore esecutivo dell'ENISA dovrebbe presentare al consiglio di amministrazione una valutazione ex post delle attività dell'ENISA ogni due anni. Inoltre, l'Agenzia dovrebbe elaborare un piano d'azione volto a dare seguito alle conclusioni delle valutazioni retrospettive e riferire ogni due anni alla Commissione sui progressi compiuti. Il consiglio di amministrazione dovrebbe essere responsabile della vigilanza sull'adeguato seguito da dare a tali conclusioni.

Presunti casi di cattiva amministrazione nelle attività dell'Agenzia possono formare oggetto di indagini da parte del Mediatore europeo ai sensi dell'articolo 228 del trattato.

Le fonti di dati per il previsto monitoraggio sarebbero prevalentemente l'ENISA, il gruppo europeo per la certificazione della cibersicurezza, il gruppo di cooperazione, la rete di CSIRT e le autorità degli Stati membri. Oltre ai dati desunti dalle relazioni (comprese le relazioni annuali di attività) dell'ENISA, del gruppo europeo per la certificazione della cibersicurezza, del gruppo di cooperazione e della rete di CSIRT, saranno utilizzati specifici strumenti di raccolta dati in caso di necessità (ad esempio indagini Eurobarometro e delle autorità nazionali, le relazioni della campagna mensile per la cibersicurezza, e le esercitazioni paneuropee).

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

I rischi individuati sono limitati: un'Agenzia dell'Unione esiste già e il suo mandato sarà definito, rafforzando quei settori in cui l'Agenzia ha dimostrato un chiaro valore aggiunto e integrandolo con i nuovi settori in cui è necessario un supporto alla luce delle nuove priorità politiche e dei nuovi strumenti, in particolare la direttiva NIS, il riesame della strategia

dell'UE per la cibersicurezza, il prossimo programma di sicurezza informatica dell'UE per la cooperazione in caso di crisi informatica e la certificazione della sicurezza delle TIC.

La proposta, pertanto, prevede i dettagli delle funzioni dell'Agenzia e porta a guadagni di efficienza. L'aumento delle competenze e dei compiti operativi non rappresenta un rischio reale, in quanto essi andrebbero a complemento dell'azione degli Stati membri e a loro sostegno, su richiesta e in relazione a servizi limitati e predeterminati.

Inoltre, la struttura, la governance e il modello di funzionamento dell'Agenzia proposti, conformemente all'orientamento comune, consentono di esercitare un sufficiente controllo per garantire che l'ENISA consegua i propri obiettivi. I rischi operativi e finanziari dei cambiamenti proposti sembrano essere limitati.

Al tempo stesso, è necessario garantire sufficienti risorse finanziarie affinché l'ENISA possa svolgere i compiti affidatile dal nuovo mandato, in particolare nel settore della certificazione.

2.2.2. Modalità di controllo previste

I conti dell'agenzia sono soggetti all'approvazione della Corte dei conti e alla procedura di scarico e sono previsti audit.

Anche l'operato dell'Agenzia è sottoposto al controllo del Mediatore, a norma delle disposizioni dell'articolo 228 del trattato.

Si vedano anche i punti 2.1 e 2.2.

2.3. Misure di prevenzione delle frodi e delle irregolarità

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

Si applicano le misure di prevenzione e protezione dell'ENISA, in particolare quanto segue:

- il controllo dei pagamenti per tutti i servizi o gli 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 i contratti stipulati tra l'Agenzia e i beneficiari dei pagamenti;

- nella lotta contro la frode, la corruzione e altre attività illegali si applicano senza limitazioni le disposizioni del regolamento (UE, Euratom) n. 883/2013 del Parlamento europeo e del Consiglio, dell'11 settembre 2013, relativo alle indagini svolte dall'Ufficio europeo per la lotta antifrode (OLAF);

- entro sei mesi dall'entrata in vigore del presente regolamento, 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 e adotta, senza indugio, le opportune disposizioni applicabili a tutto il personale dell'agenzia.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

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

- Linee di bilancio esistenti

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

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Contributo			
		Diss./Non-diss.[52]	dei paesi EFTA[53]	dei paesi candidati[54]	dei paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
1a Competitività per la crescita e l'occupazione	09.0203 ENISA e certificazione della sicurezza delle tecnologie dell'informazione e della comunicazione	Diss.	SÌ	NO	NO	NO
5 Spese amministrative	09.0101 Spese relative ai funzionari e agenti temporanei del settore "Reti di comunicazione, contenuti e tecnologie" 09.0102 Spese relative al personale esterno del settore "Reti di comunicazione, contenuti e tecnologie" 09.010211 Altre spese di gestione	Non diss.	NO	NO	NO	NO

[52] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.

[53] EFTA: *European Free Trade Association*.

[54] Paesi candidati e, se del caso, potenziali 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	1a	Competitività per la crescita e l'occupazione

ENISA			**Base di riferimento 2017 (31/12/2016)**		**2019** ***(dall'1.7.2019)***	**2020**	**2021**	**2022**	**TOTALE**
Titolo 1: Spese di personale *(incluse anche le spese relative al personale in materia di assunzioni, formazione, assistenza socio-sanitaria e dei servizi esterni)*	Impegni	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Pagamenti	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Titolo 2: spesa per infrastrutture & spesa di funzionamento	Impegni	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Pagamenti	(2a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Titolo 3: Spese operative	Impegni	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Pagamenti	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTALE degli stanziamenti per ENISA	Impegni	=1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Pagamenti	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rubrica del quadro finanziario pluriennale	5	"Spese amministrative"

Milioni di EUR (al terzo decimale)

		2019 *(dall'1.7.2019)*	2020	2021	2022	TOTALE
DG: CNECT						
•Risorse umane		0,216	0,846	0,846	0,846	**2,754**
•Altre spese amministrative		0,102	0,235	0,238	0,242	**0,817**
TOTALE DG CNECT	Stanziamenti	0,318	1,081	1,084	1,088	**3,571**

Le spese di personale sono state calcolate in base alla data di assunzione prevista (l'impiego è previsto a partire dall'1.7.2019).

Le prospettive in termini di risorse oltre il 2020 sono indicative e non pregiudicano le proposte della Commissione per il quadro finanziario pluriennale successivo al 2020

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	0,318	1,081	1,084	1,088	**3,571**

Milioni di EUR (al terzo decimale)

		2019	2020	2021	2022	TOTALE
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni	16,868	21,727	23,332	24,11	**86,038**
	Pagamenti	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Incidenza prevista sugli stanziamenti dell'agenzia

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

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

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTALE**
Accrescere le **capacità e la preparazione** degli Stati membri e delle imprese	1,408	1,900	1,931	1,969	7,208
Migliorare **la cooperazione e il coordinamento** tra gli Stati membri e le istituzioni, gli organi e le agenzie dell'UE	0,939	1,266	1,288	1,313	4,806
Aumentare le capacità a livello dell'UE per integrare l'azione degli Stati membri, in particolare in caso di crisi informatiche transfrontaliere.	0,704	0,950	0,965	0,985	3,604
Accrescere la **consapevolezza** di cittadini e imprese sulle questioni riguardanti la cibersicurezza.	0,704	0,950	0,965	0,985	3,604
Rafforzare la fiducia nel mercato unico digitale e nell'innovazione digitale aumentando la **trasparenza complessiva dell'affidabilità in termini di cibersicurezza** dei prodotti e servizi TIC.	0,939	1,266	1,288	1,313	4,806
COSTO TOTALE	4,694	6,332	6,437	6,565	24,028

[55] La presente tabella illustra soltanto le spese operative di cui al titolo 3.

3.2.3. Incidenza prevista sulle risorse umane dell'agenzia

3.2.3.1. Sintesi

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

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

Milioni di EUR (al terzo decimale)

	Q3/4 2019	**2020**	**2021**	**2022**
Agenti temporanei (gradi AD)	4,242	5,695	6,381	6,709
Agenti temporanei (gradi AST)	1,601	1,998	2,217	2,217
Agenti contrattuali	2,041	2,041	2,041	2,041
Esperti nazionali distaccati	0,306	0,447	0,656	0,796
TOTALE	**8,190**	**10,181**	**11,295**	**11,763**

Le spese di personale sono state calcolate in base alla data di assunzione prevista (per l'attuale personale dell'ENISA l'impiego è stato considerato a partire dall'1.1.2019). Per il nuovo personale l'impiego progressivo è previsto a partire dall'1.7.2019 per giungere alla piena occupazione entro il 2022. Le prospettive in termini di risorse oltre il 2020 sono indicative e non pregiudicano le proposte della Commissione per il quadro finanziario pluriennale successivo al 2020.

Incidenza stimata sul personale (ETP aggiuntivi) – Tabella dell'organico

Gruppo di funzioni e grado	2017 **Attuale ENISA**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Totale AD	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Totale AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Totale AST/SC					
TOTALE GENERALE	48	12	10	7	3

Compiti aggiuntivi per personale AD/AST in vista del conseguimento degli obiettivi dello strumento, come descritto nella sezione 1.4.2:

Compiti	AD	AST	END	Totale
Politiche e creazione di capacità	8	1		9
Cooperazione operativa	8	1	7	16
Certificazione (compiti connessi al mercato)	9	3	2	14
Conoscenza, informazione e sensibilizzazione	1	1		2
TOTALE	26	6	9	41

Descrizione dei compiti da svolgere:

Compiti	**Risorse supplementari necessarie**
Sviluppo e attuazione delle politiche dell'UE & creazione di capacità	I compiti dovrebbero comprendere l'assistenza del gruppo di cooperazione, sostenere l'attuazione transfrontaliera coerente in materia di NIS, le relazioni periodiche sullo stato di attuazione del quadro giuridico dell'UE, la consulenza e il coordinamento delle iniziative settoriali in materia di cibersicurezza nei settori dell'energia, dei trasporti aerei (ad esempio, strada, trasporto marittimo/veicoli connessi), la salute, la finanza,

	il sostegno alla creazione di centri di condivisione e di analisi delle informazioni (ISAC) in vari settori.
Cooperazione operativa e gestione delle crisi	**I compiti includerebbero:** Il segretariato della rete di CSIRT, garantendo, tra l'altro, il buon funzionamento dell'infrastruttura informatica e dei canali di comunicazione della rete di CSIRT. Garantire una cooperazione strutturata con la CERT-UE, EC3 e altri organismi competenti dell'UE. Organizzare le **esercitazioni Cyber Europe**[56] – compiti relativi all'aumento graduale delle esercitazioni da eventi biennali a eventi annuali e fare in modo che le esercitazioni esaminino l'incidente dall'inizio alla fine. **Assistenza tecnica** – i compiti includerebbero la cooperazione strutturata con la squadra CERT-UE per fornire assistenza tecnica in caso di incidenti rilevanti e sostenere l'analisi degli incidenti. Ciò significherebbe offrire agli Stati membri assistenza per affrontare incidenti e l'analisi delle vulnerabilità, artefatti e incidenti. Facilitare la cooperazione tra i singoli Stati membri che affrontano interventi di emergenza mediante l'analisi e l'aggregazione delle relazioni nazionali sulla situazione basate su informazioni messe a disposizione dell'Agenzia, su base volontaria, dagli Stati membri e da altri soggetti. **Programma per una risposta coordinata agli incidenti informatici transfrontalieri su larga scala** – l'Agenzia contribuirà a sviluppare una risposta di cooperazione, a livello dell'Unione e degli Stati membri, in caso di incidenti o crisi connesse alla cibersicurezza a livello transfrontaliero e su vasta scala attraverso una serie di compiti, che vanno dal contribuire a creare una consapevolezza situazionale a livello dell'Unione fino a testare i piani di collaborazione per gli incidenti. **Indagini su incidenti tecnici ex post** – svolgere o contribuire alle indagini sugli incidenti tecnici ex post in collaborazione con la rete di CSIRT,

[56] CyberEurope è, ad oggi, l'esercitazione più estesa e globale dell'UE in materia di cibersicurezza e interessa più di 700 professionisti del settore provenienti da tutti i 28 Stati membri. Essa si svolge ogni due anni. La valutazione dell'ENISA e la strategia dell'UE per la cibersicurezza del 2013 sottolineano il fatto che molti portatori d'interessi raccomandano di rendere Cyber Europe un evento annuale, data la natura in rapida evoluzione delle minacce informatiche. Tuttavia, ciò non è possibile per il momento in considerazione delle risorse limitate dell'Agenzia.

	con l'obiettivo di formulare raccomandazioni e di rafforzare le capacità in forma di relazioni pubbliche di prevenire futuri incidenti.
Compiti connessi al mercato (normazione, certificazione)	I compiti comprenderebbero le attività dirette a sostenere attivamente i lavori intrapresi nell'ambito del quadro di certificazione, anche fornendo competenze tecniche per elaborare sistemi europei di certificazione della cibersicurezza. Il compito comprenderà anche il supporto per lo sviluppo e l'attuazione della politica dell'Unione in materia di normazione, certificazione e l'osservatorio del mercato - ciò richiederà di facilitare la diffusione di norme in materia di gestione dei rischi dei prodotti, delle reti e dei servizi elettronici e di informare gli operatori di servizi essenziali e i fornitori di servizi digitali sui requisiti in materia di sicurezza. I compiti comprenderanno anche fornire un'analisi delle principali tendenze nel mercato della sicurezza informatica.
Conoscenze e informazioni, sensibilizzazione:	Al fine di garantire un accesso più agevole a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, la proposta conferisce all'Agenzia un nuovo compito di sviluppare e mantenere il "polo d'informazione" dell'Unione. I compiti consistono nel mettere in comune, organizzare e mettere a disposizione del pubblico, tramite un portale dedicato, informazioni sulla sicurezza delle reti e dei sistemi di informazione, in particolare la cibersicurezza, fornite dalle istituzioni, agenzie e organi dell'UE. I compiti potrebbero includere anche sostenere le attività dell'ENISA in materia di sensibilizzazione, per consentire all'Agenzia di intensificare gli sforzi.

3.2.3.2. Fabbisogno previsto di risorse umane per la DG di riferimento

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

– ☒ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito.

Stima da esprimere in valore intero (o al massimo con un decimale)

		Personale aggiuntivo			
	Scenario di base 2017	Q3/4 2019	2020	2021	2020
• **Posti della tabella dell'organico (funzionari e agenti temporanei)**					
09 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)	1	2	3		
• **Personale esterno (in equivalenti a tempo pieno: ETP)**[57]					
09 01 02 01 (AC, END e INT della dotazione globale)	1	2			
TOTALE		**4**	**3**		

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	Rappresentare la Commissione nel consiglio di amministrazione dell'Agenzia. Redigere il parere della Commissione sul documento di programmazione unico dell'ENISA e controllarne l'applicazione. Vigilare sull'elaborazione del bilancio dell'Agenzia e controllare l'esecuzione. Assistere l'Agenzia nell'elaborazione delle sue attività conformemente alle politiche dell'UE, anche attraverso la partecipazione alle riunioni pertinenti. Sorvegliare l'attuazione del quadro per la sicurezza informatica europea per i sistemi di certificazione dei prodotti e servizi TIC. Mantenere contatti con gli Stati membri e altri portatori d'interessi pertinenti in relazione all'attività di certificazione. Collaborare con l'ENISA per quanto riguarda i sistemi proposti. Preparare proposte per i sistemi europei di cibersicurezza.

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

Personale esterno	Come sopra

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

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

– ☒ La proposta/iniziativa richiede una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

La proposta implica una riprogrammazione dell'articolo 09 02 03 a seguito della revisione del mandato dell'ENISA, che conferisce all'Agenzia nuovi compiti relativi, tra l'altro, all'attuazione della direttiva NIS e al quadro di certificazione europea per la cibersicurezza. Gli importi corrispondenti:

Anno	Previsti	Richiesti
2019	10,739	16,550
2020	10,954	20,646
2021	n.p.	22,248*
2022	n.p.	23,023*

* Si tratta di una stima. Il finanziamento dell'UE dopo il 2020 sarà esaminato nell'ambito di una discussione a livello dell'intera Commissione su tutte le proposte per il periodo successivo al 2020. Ciò significa che, una volta presentata la proposta per il quadro finanziario pluriennale successivo, la Commissione presenterà una scheda finanziaria legislativa modificata che tiene conto delle conclusioni della valutazione d'impatto[58].

– ☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale[59].

3.2.5. Partecipazione di terzi al finanziamento

– ☐ La proposta/iniziativa non prevede cofinanziamenti da terzi.

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

[58] Link verso la pagina contenente la valutazione d'impatto.

[59] Cfr. gli articoli 11 e 17 del regolamento (UE, Euratom) n. 1311/2013 del Consiglio, che stabilisce il quadro finanziario pluriennale per il periodo 2014-2020.

	Anno **2019**	Anno **2020**	Anno **2021**	Anno **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

3.3. Incidenza prevista sulle entrate

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

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

  – ☐ sulle risorse proprie

  – ☐ sulle entrate varie

[60] L'importo esatto per gli anni successivi sarà noto quando sarà fissato il fattore di proporzionalità dell'EFTA per l'anno in questione.