

dossier

Maggio 2022

Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del Titolo III, "Quadro di certificazione della cibersecurity", del regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersecurity, e alla certificazione della cibersecurity per le tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersecurity")

Atto del Governo n. 388



Senato
della Repubblica



Camera
dei deputati

La verifica delle relazioni tecniche e degli effetti finanziari dei provvedimenti privi di relazione tecnica è curata dal Servizio Bilancio.

La verifica delle disposizioni di copertura è curata dalla Segreteria della Commissione Bilancio.

L'analisi è svolta a fini istruttori, a supporto delle valutazioni proprie degli organi parlamentari, ed ha lo scopo di segnalare ai parlamentari, ove ne ricorrano i presupposti, la necessità di acquisire chiarimenti ovvero ulteriori dati e informazioni in merito a specifici aspetti dei testi.



SERVIZIO DEL BILANCIO

Tel. 06 6706 5790 – ✉ SBilancioCU@senato.it – 🐦 @SR_Bilancio

Nota di lettura n. 309



SERVIZIO BILANCIO DELLO STATO

Tel. 06 6760 2174 / 9455 – ✉ bs_segreteria@camera.it

Verifica delle quantificazioni n. 446

La redazione del presente dossier è stata curata dal Servizio del bilancio del Senato della Repubblica.

INDICE

PREMESSA.....	1
Capo I Disposizioni generali	1
Articolo 1 (<i>Oggetto e ambito di applicazione</i>).....	1
Articolo 2 (<i>Trattamento dei dati personali</i>)	1
Articolo 3 (<i>Definizioni</i>)	1
Capo II Autorità nazionale, attività nazionale ed internazionale	4
Articolo 4 (<i>Designazione dell'autorità nazionale di certificazione della cybersicurezza, organizzazione e procedure per lo svolgimento dei compiti in ambito nazionale di certificazione della cybersicurezza</i>)	4
Articolo 5 (<i>Vigilanza nazionale</i>)	9
Articolo 6 (<i>Rilascio dei certificati di cybersicurezza</i>).....	13
Articolo 7 (<i>Dichiarazioni UE di conformità</i>).....	15
Articolo 8 (<i>Accreditamento ed autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia</i>)	15
Articolo 9 (<i>Attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza</i>)	18
Capo III Sanzioni, reclami e ricorsi giurisdizionali.....	19
Articolo 10 (<i>Quadro sanzionatorio</i>).....	19
Articolo 11 (<i>Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità</i>)	23
Articolo 12 (<i>Ricorso all'autorità giudiziaria</i>)	24
Capo IV Disposizioni finanziarie	24
Articolo 13 (<i>Destinazione dei proventi derivanti dalle attività dell'Agenzia</i>).....	24
Articolo 14 (<i>Ulteriori disposizioni finanziarie</i>)	25
Capo V Disposizioni finali	27
Articolo 15 (<i>Successiva attuazione nazionale dei sistemi europei di certificazione</i>)	27

INFORMAZIONI SUL PROVVEDIMENTO

Natura dell'atto:	Schema di decreto legislativo	
Atto del Governo n.	388	
Titolo breve:	Adeguamento della normativa nazionale al regolamento sulla cybersicurezza	
Riferimento normativo:	Articoli 1 e 18 della legge 22 aprile 2021, n. 53	
Relazione tecnica (RT):	Presente	
	Senato	Camera
Commissione competente:	1 ^a (Affari Costituzionali), 5 ^a (Bilancio) <i>in sede consultiva</i> 2 ^a (Giustizia), 8 ^a (Lavori pubblici, comunicazioni), 14 ^a (Politiche dell'Unione europea) <i>in sede osservazioni</i>	I (Affari costituzionali) e IX (Trasporti), V Bilancio, XIV Politiche dell'Unione Europea

PREMESSA

Lo schema A.G. 388 viene predisposto nell'esercizio della delega contenuta nell'articolo 18 della legge 22 aprile 2021, n. 53 — legge di delegazione europea 2019-2020 e contiene disposizioni per il completo adeguamento dell'ordinamento interno alle disposizioni del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cybersicurezza) (di seguito Regolamento).

CAPO I DISPOSIZIONI GENERALI

Articolo 1 (*Oggetto e ambito di applicazione*)

Le norme specificano oggetto e ambito di applicazione.

Articolo 2 (*Trattamento dei dati personali*)

L'articolo dispone che il trattamento dei dati personali derivante dall'applicazione del presente decreto è effettuato ai sensi del regolamento (UE) 2016/679 e del decreto legislativo 30 giugno 2003, n. 196.

Articolo 3 (*Definizioni*)

L'articolo prevede le definizioni che si applicano che ai fini del presente decreto, oltre alle definizioni contenute nel regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019

Tra le varie definizioni si segnalano le seguenti:

- «Agenzia»: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82
- «ECCG»: Gruppo europeo di certificazione della cybersicurezza, ai sensi dell'articolo 62 del Regolamento
- «ENISA»: l'Agenzia dell'Unione europea per la cybersicurezza di cui al Titolo II del regolamento (UE) 2019/881
- «organismo di certificazione»: organismo di valutazione della conformità che emette certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli standard di riferimento ai sensi dell'articolo 54, paragrafo 1, lettera c), del Regolamento per il sistema di certificazione in cui è accreditato
- «Organismo di accreditamento»: l'organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'articolo 2, paragrafo 1, numero 11, del regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99;

La RT conferma che la norma si limita alla definizione dell'organizzazione dell'autorità nazionale di certificazione della cybersicurezza in Italia, le relative modalità di cooperazione con le altre autorità pubbliche nazionali ed europee e con l'Organismo di accreditamento, nonché la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

Inoltre, rappresenta che l'autorità nazionale di certificazione della cybersicurezza, di cui all'articolo 58, paragrafo 1, del Regolamento, per l'Italia è l'Agenzia per la cybersicurezza nazionale, di cui all'articolo 5 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, designata in tale qualità dall'articolo 7, comma 1, lettera e), del medesimo decreto-legge. Certifica infine che, limitandosi a definire l'oggetto e l'ambito di applicazione dello schema di decreto legislativo, le disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Sull'articolo 2, la RT evidenzia che la disposizione si limita alla previsione che il trattamento dei dati personali in applicazione del presente decreto sia effettuato ai sensi del regolamento (UE) 2016/679 e del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni. Rileva che la norma ha l'unica finalità di specificare la normativa di riferimento per il trattamento dei dati personali e, dunque, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

Anche sull'articolo 3, la RT assicura che, stante la sua finalità, la norma non comporta nuovi o maggiori oneri a carico della finanza pubblica.

Al riguardo, ritenuto il tenore di mero rilievo ordinamentale delle disposizioni, non ci sono osservazioni.

- alla lettera a) «TIC»: *Tecnologia dell'Informazione e della Comunicazione*;

- alla lettera b) «*Regolamento*»: Titolo III del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013;
- -alla lettera c) «*quadro europeo di certificazione*»: il Regolamento ed i successivi sistemi europei di certificazione adottati a nonna dell'articolo 49 del Regolamento;
- alla lettera d) «*messa a disposizione sul mercato*»: la fornitura di un prodotto TIC o di un servizio TIC per la distribuzione, il consumo o l'uso sul mercato dell'Unione Europea nel corso di un'attività commerciale, a titolo oneroso o gratuito;
- alla lettera e) «*richiamo*»: qualsiasi provvedimento volto ad ottenere la restituzione di un prodotto TIC che è già stato reso disponibile all'utilizzatore finale;
- -alla lettera f) «*ritiro*»: qualsiasi provvedimento volto ad impedire la messa a disposizione sul mercato di un prodotto TIC o servizio TIC nella catena della fornitura;
- alla lettera g) «*vigilanza del mercato*»: le attività svolte ed i provvedimenti adottati dall'Agenzia e dalle altre autorità pubbliche competenti per garantire che i prodotti TIC, i servizi TIC ed i processi TIC ad essi collegati siano conformi ai requisiti stabiliti dal quadro europeo di certificazione e non pregiudichino la salute, la sicurezza o qualsiasi altro aspetto della protezione del pubblico interesse;
- alla lettera i) «*standard*» o «*norma*»: una specifica tecnica, adottata da un organismo di normazione riconosciuto ai sensi dell'articolo 2, paragrafo 1, numero 1), del regolamento (UE) 1025/2012;
- alla lettera l) «*norma armonizzata*»: una norma europea adottata sulla base di una richiesta della Commissione Europea ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione ai sensi dell'articolo 2, paragrafo 1, numero 1, lettera c), del regolamento (UE) n. 1025/2012;
- alla lettera n) «*autorizzazione*»: provvedimento con il quale l'Agenzia accerta il possesso, a norma dell'articolo 54, paragrafo 1, lettera f), del Regolamento, di requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità per poter operare nell'ambito di uno specifico sistema europeo di certificazione, in aggiunta a quanto già previsto nell'allegato del Regolamento;
- alla lettera o) «*abilitazione*»: provvedimento con il quale l'Agenzia accerta i requisiti necessari affinché un esperto o un laboratorio di prova possa coadiuvare l'Agenzia nelle attività di vigilanza nazionale o di rilascio dei certificati di cybersicurezza;
- alla lettera p) «*laboratorio di prova*»: organismo di valutazione della conformità che svolge verifiche documentali e/o prove in base alle norme armonizzate europee ed agli standard e specifiche tecniche nell'ambito del sistema europeo di certificazione in cui è accreditato;
- alla lettera q) «*organismo di certificazione*»: organismo di valutazione della conformità che emette certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli *standard* di riferimento ai sensi dell'articolo 54, paragrafo 1, lettera c), del Regolamento per il sistema di certificazione in cui è accreditato;
- alla lettera r) «*elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale*»: registro aggiornato dei laboratori di prova e degli esperti abilitati dall'Agenzia ad effettuare attività di valutazione di sicurezza informatica nell'ambito dei compiti di vigilanza nazionale dell'Agenzia;
- alla lettera s) «*elenco dei laboratori di prova e degli esperti per le attività di certificazione*»: registro aggiornato dei laboratori di prova e degli esperti abilitati dall'Agenzia ad effettuare attività di valutazione di sicurezza informatica nell'ambito dei compiti di rilascio dei certificati di cybersicurezza dell'Agenzia;

- alla lettera t) «*Organismo di Certificazione della Sicurezza Informatica*» o «*OCSI*»: organismo di certificazione dell'Agenzia, accreditato ai sensi dell'articolo 60, paragrafo 2 del Regolamento, istituito ai sensi dell'articolo 4 del decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004;
- alla lettera u) «*dichiarazione UE di conformità*»: attestazione di conformità rilasciata da un fabbricante di prodotti TIC o fornitore di servizi TIC ai sensi dell'articolo 53, paragrafo 1, del regolamento UE 2019/881, a seguito del processo di autovalutazione di conformità previsto dallo stesso articolo;
- alla lettera v) «*emittenti delle dichiarazioni di conformità UE*»: i soggetti di cui all'articolo 53, paragrafo 1, del regolamento UE 2019/881;
- alla lettera z) «*certificato europeo di cybersicurezza*»: un documento rilasciato da un organismo di certificazione che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità ai requisiti stabiliti da un sistema europeo di certificazione;
- alla lettera aa) «*certificato europeo di cybersicurezza (o dichiarazione UE di conformità) non conforme*»: certificato europeo di cybersicurezza (o dichiarazione UE di conformità) che non soddisfa uno o più requisiti di un sistema europeo di certificazione ai sensi dell'articolo 54, paragrafo 1 del Regolamento;
- alla lettera bb) «*revoca di un certificato europeo di cybersicurezza*»: annullamento di un certificato europeo di cybersicurezza prima della sua scadenza da parte dell'organismo di valutazione della conformità emittente o da parte dell'Agenzia;
- alla lettera cc) «*revoca di una dichiarazione UE di conformità*»: annullamento di una dichiarazione UE di conformità prima della sua scadenza da parte del fabbricante o fornitore emittente;
- alla lettera dd) «*livello di affidabilità di base*»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 5 dell'articolo 52 del Regolamento;
- alla lettera ee) «*livello di affidabilità sostanziale*»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 6 dell'articolo 52 del Regolamento;
- alla lettera ff) «*livello di affidabilità elevato*»: livello di affidabilità che soddisfa i requisiti ed è valutato con i criteri specificati al paragrafo 7 dell'articolo 52 del Regolamento;
- alla lettera gg) «*ECCG*»: Gruppo europeo di certificazione della cybersicurezza, ai sensi dell'articolo 62 del Regolamento;
- alla lettera hh) «*ENISA*»: l'Agenzia dell'Unione europea per la cybersicurezza di cui al Titolo II del regolamento (UE) 2019/881.

CAPO II

AUTORITÀ NAZIONALE, ATTIVITÀ NAZIONALE ED INTERNAZIONALE

Articolo 4

(Designazione dell'autorità nazionale di certificazione della cybersicurezza, organizzazione e procedure per lo svolgimento dei compiti in ambito nazionale di certificazione della cybersicurezza)

Il comma 1 prevede l'indicazione dell'Agenzia per la cybersicurezza nazionale, quale autorità nazionale di certificazione della cybersicurezza.

Il comma 2 stabilisce che con provvedimento dell'Agenzia, siano definite l'organizzazione e le procedure per lo svolgimento dei compiti dell'Agenzia quale Autorità nazionale di certificazione della cybersicurezza e sono definite le modalità applicative delle attività di cui al presente Capo ed all'articolo 11. È stabilito che il predetto provvedimento dispone altresì che le attività dell'Agenzia

relative al rilascio di certificati europei di cybersicurezza di cui all'articolo 6, comma 1, sono rigorosamente separate dalle attività di vigilanza di cui all'articolo 5 e che tali attività sono svolte indipendentemente le une dalle altre, nell'ambito di due distinte Divisioni. È altresì previsto che l'Agenzia partecipi alle attività internazionali dell'ECCG e del Comitato ai sensi degli articoli 62 e 66 del Regolamento con proprio personale.

Il comma 3 dispone che per lo svolgimento dei compiti attribuiti all'Agenzia, inerenti la realizzazione e la gestione dei sistemi informativi, la formazione del personale tecnico ed amministrativo, la ricerca e l'innovazione, la realizzazione e l'aggiornamento di laboratori interni, l'abilitazione di laboratori di prova ed esperti, l'autorizzazione di organismi di valutazione della conformità, la vigilanza, l'accREDITAMENTO, il rinnovo e l'estensione dell'Organismo di Certificazione della Sicurezza Informatica di cui all'articolo 6, comma 1, le missioni nazionali ed internazionali e le spese generali, sia autorizzata la spesa di 657.500 euro per l'anno 2022, 592.500 euro per l'anno 2023 e 637.500 euro annui a decorrere dall'anno 2024. Agli oneri derivanti dal presente comma si provvede ai sensi dell'articolo 14, comma 1.

La RT certifica sul comma 1, che la norma specifica che l'Agenzia per la cybersicurezza nazionale, ai sensi degli articoli 7, comma 1, lettera e), e 16, comma 12, lettera b), del citato decreto-legge n. 82 del 2021, è l'autorità nazionale di certificazione della cybersicurezza, ai sensi dell'articolo 58, paragrafo 1 del Regolamento.

Con il comma 2, evidenzia che si stabilisce che l'organizzazione e le procedure per lo svolgimento dei compiti dell'Agenzia quale autorità nazionale di certificazione della cybersicurezza, nonché la definizione delle modalità applicative delle attività di cui al presente Capo I ed all'articolo 11, saranno individuate con un provvedimento dell'Agenzia, adottato ai sensi dell'articolo 5, comma 3, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223. Inoltre, il comma 2, stabilisce che l'Agenzia partecipa alle attività internazionali dell'ECCG e del comitato ai sensi degli articoli 62 e 66 del Regolamento con proprio personale.

Quanto al comma 3, segnala che ivi si attribuisce all'Agenzia la dotazione finanziaria necessaria per lo svolgimento dei compiti per la realizzazione e la gestione dei sistemi informativi, la formazione del personale tecnico ed amministrativo, la ricerca e l'innovazione, la realizzazione e l'aggiornamento di laboratori interni, l'abilitazione di laboratori di prova ed esperti, l'autorizzazione di organismi di valutazione della conformità, la vigilanza, l'accREDITAMENTO, il rinnovo e l'estensione dell'organismo di certificazione della sicurezza informatica (OCSI), le missioni nazionali ed internazionali e le spese generali.

I limiti per la copertura dei predetti oneri per le spese di funzionamento dell'Agenzia sono indicati dall'articolo 14 dello schema di decreto e sono stimati in complessivi euro 657.500 per il 2022, euro 592.500 per l'anno 2023 e per euro 637.500 dal 2024.

Considerato che l'individuazione dell'autorità nazionale di certificazione della cybersicurezza e l'attribuzione alla stessa di adeguate risorse costituisce adempimento di obblighi europei e che, a tal fine, è stata conferita una delega al Governo con l'articolo 18 della citata legge n. 53 del 2021, alla copertura delle spese relative al

predetto adeguamento si farà fronte facendo ricorso al fondo per il recepimento della normativa europea di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234, come previsto dall'articolo 1 della medesima legge n. 53 del 2021.

In tabella è sintetizzata tale stima complessiva con riferimento al triennio 2022-2024:

Elementi per stima costi attività dell'autorità di certificazione per triennio 2022-2024	artt. Reg. (UE) 881/2019	2022	2023	2024
Missioni internazionali Commissione Europea, ENISA	47.4, 48.2, 49.2, 49.5-6, 58.6, 58.7(g)-(h), 58.9, 59, 62	15	25	35
Costi missioni internazionali (€)		22.500 €	37.500 €	52.500 €
Costi di accreditamento dell'organismo di certificazione (€)	60.2	15.000 €	5.000 €	5.000 €
Costi di ricerca, formazione e cooperazione internazionale (€)	56.5(a), 56.6, 58.7(i), 58.9	500.000 €	500.000 €	500.000 €
Costi di avvio e spese generali (€)		120.000 €	50.000 €	80.000 €
Totale costi (€)		657.500,00 €	592.500,00 €	637.500,00 €

In merito, specifica quanto segue:

- stima dei costi di missione: con riferimento alle missioni nazionali ed internazionali si rendono necessarie tipicamente due tipologie di missioni:
 - Missioni nazionali nell'ambito dell'attività di vigilanza dell'agenzia presso le sedi dei soggetti vigilati di cui all'articolo 58, par. 8 del Reg. UE 2019/881;
 - Missioni internazionali nell'ambito delle attività di cooperazione internazionale con la Commissione europea, ENISA, le altre autorità nazionali di certificazione della cybersicurezza europee o organismi omologhi da paesi terzi.

Per quanto riguarda le missioni nazionali dell'Autorità, esse deriverebbero dallo svolgimento di:

- funzioni di supporto e sostegno che ACN assicurerà ad Accredia ai fini del monitoraggio e della vigilanza delle attività degli organismi di valutazione della conformità (vds. Articolo 58, paragrafo 7, lettera c), del regolamento (UE) 2019/881);
- indagini presso le sedi degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza (vds. Articolo 58, paragrafo 8, lettera d), del regolamento (UE) 2019/881).

Con riferimento ai predetti casi, non si prevedono ulteriori oneri a carico della finanza pubblica poiché, nelle more che gli schemi di certificazione in corso di predisposizione trovino effettiva diffusione, essi si configurano come attività a supporto di soggetti terzi (Accredia), che ne detengono la titolarità, o come funzioni che potranno comunque trovare copertura finanziaria nelle dotazioni ordinarie dell'Agenzia, integrandosi efficientemente nei regolari programmi di ispezione.

La configurazione tipica di una missione internazionale a seconda delle necessità richiede l'impiego di uno o due delegati per la partecipazione ad incontri internazionali, in particolare se la partecipazione prevede lo svolgimento di più sessioni tecniche in parallelo.

Per la determinazione della stima di 1.500 euro per ciascuna missione internazionale è pertanto stata presa a riferimento una trasferta a Bruxelles della durata di due giorni (con due pernottamenti) di uno/due dipendenti appartenenti all'Area manageriale e alte professionalità inquadrati nel segmento professionale "Consigliere".

L'importo è stato determinato sulla base delle previsioni di cui all'art. 111 del Regolamento del Personale dell'Agenzia, in base al quale, per le missioni all'estero, al personale inviato in missione competono:

- la fruizione dei servizi di viaggio (sono stati considerati i biglietti aereo di andata e ritorno Roma-*Bruxelles*);
- il rimborso di ulteriori spese di viaggio (sono stati considerati i servizi taxi abitazione-aeroporto-Hotel);
- la fruizione dei servizi di alloggio messi a disposizione dall'Agenzia (sono stati considerati n. 2 pernottamenti in Hotel a Bruxelles);
- la diaria per i giorni di espletamento dell'incarico;
- stima dei costi di accreditamento: in base all'art. 60.2 del Regolamento (UE) 2019/881, l'organismo di certificazione dell'autorità dovrà essere accreditato dall'organismo nazionale di accreditamento (Reg. CE 765/2008 - Accredia per l'Italia) per ogni nuovo sistema di certificazione. Considerando per il primo accreditamento una stima di euro 15.000 IVA inclusa e 5.000 euro IVA inclusa per ogni anno successivo per spese di mantenimento/estensione dell'accREDITAMENTO di accREDITAMENTO, gli oneri per gli anni 2022, 2023, 2024 ammontano, rispettivamente, ad euro 15.000, 5.000 e 5.000;
- stima dei costi di ricerca e formazione: per sostenere le attività di ricerca per sviluppare nuove metodologie di valutazione, linee guida, strumenti e conoscenze, si ipotizza un investimento costante di euro 500.000 per ogni anno da impiegare per finanziare progetti di ricerca e borse di studio, in collaborazione con enti universitari e di ricerca;
- stima delle spese generali e di avvio: premesso che le capacità tecniche del Servizio Certificazione e Vigilanza potranno trarre beneficio anche da altre iniziative di investimento assunte in ambito Perimetro, appare cauto stimare, per il solo anno 2022, una spesa una tantum di euro 100.000 euro per l'allestimento di spazi e locali. Per l'acquisto di postazioni informatiche e per la manutenzione

si stimano per gli anni 2022, 2023 e 2024 rispettivamente euro 20.000, euro 50.000 ed euro 80.000. Pertanto, le spese generali e di avvio per il triennio ammontano rispettivamente a euro 120.000, euro 50.000 ed euro 80.000.

Rileva che tra i costi operativi che l'Agenzia dovrà sostenere ai sensi dell'articolo 4, comma 3, si individuano i costi di accreditamento per l'organismo di certificazione dell'autorità, che ai sensi dell'articolo 60, paragrafo 2 del Regolamento, dovrà essere fatto per l'organismo nazionale di accreditamento. Ai sensi dell'articolo 8, comma 3, dello schema di decreto, dal momento che l'Agenzia presterà assistenza all'organismo nazionale di accreditamento nel monitoraggio degli organismi di valutazione della conformità accreditati, ai sensi dell'articolo 58, paragrafo 7, lett. c) del Regolamento, il compenso ricevuto per tale attività di assistenza da parte dell'organismo nazionale di accreditamento potrà compensare in tutto o in parte i costi di accreditamento per l'organismo di certificazione dell'autorità da rimborsare all'organismo nazionale di accreditamento.

Al riguardo, in relazione all'autorizzazione di spesa prevista al comma 3, configurata come limite massimo di spesa, pur considerando le indicazioni fornite dalla RT in merito alle singole voci di spesa previste ai fini della stima dei fabbisogni annui conseguenti per il funzionamento dell'Autorità, appare utile soffermarsi sui criteri e le ipotesi assunte nella quantificazione degli oneri.

In tal senso, preliminarmente, si osserva che se la norma indica varie finalità per l'autorizzazione di spesa, alcune di queste non sono poi riportate nella tabella degli oneri della RT. In particolare, non si fa menzione della realizzazione e l'aggiornamento di laboratori interni, l'abilitazione di laboratori di prova ed esperti, la realizzazione e gestione di sistemi informativi (si menziona soltanto l'acquisto e manutenzione di postazioni informatiche), l'autorizzazione di organismi di valutazione della conformità, il rinnovo e l'estensione dell'Organismo di Certificazione della Sicurezza Informatica di cui all'articolo 6, comma 1. Andrebbero quindi approfonditi tali aspetti.

Con riferimento alla stima dei costi di missione espressamente previsti nell'ambito dell'attività di vigilanza svolte dell'agenzia presso le sedi dei soggetti vigilati di cui all'articolo 58, par. 8 del Reg. UE 2019/881, nonché per le missioni internazionali nell'ambito delle attività di cooperazione internazionale con la Commissione europea, ENISA, le altre autorità nazionali di certificazione della cybersicurezza europee o organismi omologhi da paesi terzi, andrebbero richieste conferme relativamente all'esclusione dalla stima in RT di nuovi o maggiori oneri anche per missioni nazionali, atteso che la stessa relazione assicura che alla copertura dei relativi fabbisogni l'organismo potrà provvedere avvalendosi della sola dotazione ordinaria già prevista ai sensi della legislazione vigente, escludendo espressamente ulteriori oneri a carico della finanza pubblica.

Poi, con riferimento alla stima degli oneri previsti per le missioni internazionali, pur considerando le ipotesi assunte dalla RT andrebbe spiegato il valore crescente nella

frequenza delle missioni per ciascun anno e quindi la congruità della copertura a decorrere dal 2024 nel senso di escludere ulteriori aumenti nelle spese per missioni negli anni successivi a quest'ultimo.

Inoltre, andrebbero precisati i parametri retributivi indennitari considerati nella stima per cui la RT si limita a precisare la trasferta a Bruxelles della durata di due giorni (con due pernottamenti) di n.1/2 dipendenti appartenenti all'Area manageriale e alte professionalità inquadrati nel segmento professionale "Consigliere", tenuto conto della flessibilità nella disciplina dei trattamenti per il personale inviato in missione prevista, in particolare, ai commi 3-4 e 6 del richiamato articolo 111 del Regolamento del personale dell'Agenzia.

Quanto alla stima dei costi di "accreditamento", per cui la RT indica una stima di euro 15.000 IVA inclusa e 5.000 euro IVA inclusa per ogni anno successivo per spese di mantenimento/estensione dell'accreditamento, per gli oneri per gli anni 2022, 2023, 2024 che ammonterebbero, rispettivamente, ad euro 15.000, 5.000 e 5.000, andrebbero comunque richieste informazioni in merito ai parametri considerati nella stima dell'onere ivi complessivamente indicato in ragione annua.

Venendo poi alla stima dei costi di ricerca e formazione, ai fini del sostenimento delle attività di ricerca lo sviluppo di nuove metodologie di valutazione, di linee guida, strumenti e conoscenze, per cui la RT ipotizza un investimento costante di euro 500.000 annui da impiegare per finanziare progetti di ricerca e borse di studio, in collaborazione con enti universitari e di ricerca, andrebbero richiesti elementi di conferma in merito all'adeguatezza dei fabbisogni annui previsti, in relazione ai delicati compiti attribuiti all'organismo e in considerazione dell'accelerata evoluzione prevedibile dei sistemi tecnologici e *software* nei prossimi anni.

In tal senso, quanto alla stima delle spese generali per l'avvio dell'organismo, posto che la RT evidenzia che, tenuto conto delle capacità tecniche del servizio certificazione e vigilanza, le stesse potranno trarre beneficio anche da altre iniziative di investimento assunte in ambito "perimetro", asserendo la prudenzialità della stima, per il solo anno 2022, di una spesa *una tantum* di euro 100.000 euro per l'allestimento di spazi e locali, mentre per l'acquisto di postazioni informatiche e per la manutenzione, stima euro 20.000, euro 50.000 ed euro 80.000, rispettivamente, per gli anni 2022, 2023 e 2024, pervenendo ad una valutazione del fabbisogno per il triennio complessiva pari, rispettivamente, a euro 120.000, euro 50.000 ed euro 80.000, andrebbe richiesto un supplemento di informazioni in merito ai parametri considerati degli oneri per il citato investimento, fornendo specifiche indicazioni sui criteri "unitari" considerati a tal fine.

Articolo 5 **(Vigilanza nazionale)**

Il comma 1 stabilisce che l'Agenzia realizza l'attività di vigilanza del mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, con riferimento ai certificati di cybersicurezza ed alle dichiarazioni UE di conformità

emessi nel territorio dello Stato, ai sensi dell'articolo 58, paragrafo 7, lettere a) e b), del Regolamento UE, vigilando sui fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8, del Regolamento.

Si prevede, in particolare, che sull'Agenzia, inoltre, ai sensi dell'articolo 58, paragrafo 7, lettere c), d) ed e), del Regolamento UE, ricadano i seguenti compiti: alla lettera a) l'assistenza ed il sostegno dell'Organismo di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del Regolamento; alla lettera b) il monitoraggio e la vigilanza sulle attività degli organismi di valutazione della conformità pubblici di cui all'articolo 56, paragrafo 5, lettera b), del Regolamento; alla lettera c) ove previsto dal sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera f), del Regolamento, il rilascio dell'autorizzazione degli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, e la limitazione, sospensione o la revoca dell'autorizzazione esistente qualora violino le prescrizioni del Regolamento, dandone notizia all'Organismo di accreditamento.

Il comma 2 prevede che l'Agenzia, nello svolgimento dell'attività di vigilanza di cui al comma 1, operi anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità di vigilanza degli altri Stati membri ai sensi dell'articolo 58, paragrafo 7, lettere a) ed h), del Regolamento UE. L'Agenzia esegue l'attività di vigilanza di cui al comma 1 anche in collaborazione con le Forze dell'ordine.

Il comma 3 dispone che l'Agenzia, nell'attività di vigilanza di cui al comma 1, possa effettuare, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cybersicurezza e degli emittenti le dichiarazioni di conformità UE, indagini ed *audit*, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza, revocare certificati ai sensi del comma 4, irrogare sanzioni pecuniarie ed accessorie ai sensi dell'articolo 10. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

Il comma 4 rileva che nel caso in cui l'Agenzia, in esito alle attività di vigilanza di cui al comma 1, accerti l'emissione di un certificato non conforme, rilasciato ai sensi dell'articolo 56, paragrafi 4, 5, lettera b), o 6, lettere a) e b), del Regolamento, il certificato sia sottoposto a revoca: a) per il livello di affidabilità elevato; b) per il livello di affidabilità di base o sostanziale nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale ai sensi dell'allegato II del decreto legislativo 18 maggio 2018, n. 65, o servizio di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera fff), del decreto legislativo 1° agosto 2003, n. 259, o alla salute o all'incolumità personale; c) se previsto espressamente dallo specifico sistema europeo di certificazione.

Il comma 5 stabilisce che nella fattispecie di cui alla lettera a) del comma 4 l'Agenzia provveda direttamente alla revoca del certificato. Nella fattispecie di cui alla lettera b) del comma 4 l'Agenzia chiede all'organismo emittente il certificato di provvedere alla revoca del certificato entro e non oltre 5 giorni e, in caso di inottemperanza, provvede direttamente entro i successivi 5 giorni. Nella fattispecie di cui alla lettera c) del comma 4 si provvede in base alle regole stabilite dal sistema specifico di certificazione.

Il comma 6 dispone che accertata l'emissione di un certificato non conforme rilasciato ai sensi dell'articolo 56, paragrafi 4, 5, lettera b), o 6, lettere a) e b), del Regolamento, in esito alle attività di vigilanza di cui al comma 1, fatti salvi i casi di revoca di cui alle lettere a), b) o c) del comma 4, l'Agenzia chieda all'organismo che ha emesso il certificato di ripetere in tutto o in parte l'attività di valutazione o integrare l'attività di valutazione con ulteriori verifiche e ricondurre il certificato a conformità entro 120 giorni o revocare il certificato. In caso di mancata riconduzione a conformità o mancata revoca del certificato non conforme da parte dell'organismo, il certificato decade. La riconduzione a conformità o la revoca del certificato sono divulgate ai sensi dell'articolo 54, paragrafo 1, lettera s), del Regolamento UE. È stabilito che le modalità di sostegno ed assistenza dell'Agenzia

all'Organismo di accreditamento per l'attività di vigilanza di cui al comma 1, siano disciplinate da apposita convenzione o protocollo di intesa fra i medesimi soggetti.

Il comma 7 afferma che l'Agenzia, per le prove tecniche nell'ambito delle attività di cui al comma 1, può effettuare valutazioni di sicurezza informatica anche attraverso esperti" esterni" o laboratori di prova abilitati dall'Agenzia, ai sensi dell'articolo 8, comma 4, e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

Il comma 8 prevede che è fatto obbligo agli organismi di valutazione della conformità, ai titolari dei certificati europei di cybersicurezza ed agli emittenti delle dichiarazioni di conformità durante l'attività di vigilanza a cui sono sottoposti, di cooperare con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi. È stabilito che gli stessi operatori mettano a disposizione, su richiesta dell'Agenzia, tutti i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica da parte dell'Agenzia assieme agli strumenti di valutazione eventualmente forniti dal fabbricante o dal fornitore nell'attività di valutazione come indicato nei rapporti di valutazione. L'onere della prova della conformità di certificati e dichiarazioni è in capo agli organismi di valutazione della conformità, ai titolari dei certificati o agli emittenti delle dichiarazioni di conformità.

Il comma 9 afferma che ai sensi dell'articolo 30, commi 4 e 5, della legge n. 234 del 2012, gli oneri derivanti dall'applicazione dei commi 3, 8 e 9 per i controlli effettuati dall'Agenzia e relativi in particolare all'impiego del personale in forza all'Agenzia, della strumentazione utilizzata nelle prove e dei materiali di consumo e per le missioni e spese generali, sono a carico dell'organismo di valutazione della conformità, del titolare del certificato o dell'emittente della dichiarazione UE di conformità sottoposto all'attività di vigilanza. Nel caso in cui l'attività di vigilanza includa ulteriori spese, tra cui l'utilizzo di laboratori di prova esterni ed eventuali spese di trasporto per prodotti prelevati o sequestrati da sottoporre a verifica, le ulteriori spese sono ugualmente a carico del soggetto sottoposto all'attività di vigilanza. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

La RT evidenzia che l'articolo stabilisce le modalità di realizzazione dell'attività di vigilanza del mercato in ambito nazionale.

In particolare, sulla norma ribadisce che, ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della cybersicurezza, con riferimento ai certificati di cybersicurezza ed alle dichiarazioni UE di conformità emessi nel territorio dello Stato, ai sensi dell'articolo 58, paragrafo 7, lettere a) e b), del Regolamento UE, l'Agenzia vigila sui fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di cybersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8, del Regolamento.

In tal senso, conferma che l'Agenzia, ai sensi dell'articolo 58, paragrafo 7, lettere c), d) ed e), del Regolamento UE: a) fatto salvo l'articolo 60, paragrafo 3, assista e sostenga attivamente l'Organismo di Accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità ai fini del Regolamento; b) monitori e vigili sulle attività degli organismi di valutazione della conformità pubblici di cui all'articolo 56, paragrafo 5, lettera b), del Regolamento UE; c) ove previsto dal sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera J), del Regolamento, autorizzi gli organismi di valutazione della conformità a norma dell'articolo 60, paragrafo 3, del Regolamento UE, e disponga la limitazione, la

sospensione o la revoca dell'autorizzazione esistente, qualora gli stessi enti violino le prescrizioni del Regolamento, dandone notizia all'Organismo di Accreditamento.

Rileva che ai sensi del comma 2, rileva che l'Agenzia, nello svolgimento delle predette attività di vigilanza, opera anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità vigilanza degli altri Stati membri ai sensi dell'articolo 58, paragrafo 7, lettere a) e h), del Regolamento. L'Agenzia esegue l'attività di vigilanza di cui al comma 1 anche in collaborazione con le Forze dell'ordine.

Tali disposizioni rivestono carattere ordinamentale e non comportano nuovi o maggiori oneri a carico della finanza pubblica. Con particolare riguardo alla possibile collaborazione con le Forze dell'ordine, tale forma di avvalimento, già prevista dall'articolo 5, comma 5, del decreto-legge n. 82 del 2021, per l'assolvimento dei compiti istituzionali dell'Agenzia, troverà concreta disciplina nelle convenzioni ivi previste e verrà svolta nell'ambito delle risorse già assegnate all'Agenzia e alle stesse Forze dell'ordine, non comportando nuovi o maggiori oneri a carico della finanza pubblica.

Sottolinea che il comma 3 stabilisce che l'Agenzia, nell'attività di vigilanza nazionale, può effettuare indagini ed audit nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cybersicurezza e degli emittenti delle dichiarazioni di conformità UE, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza. Inoltre, è previsto che l'Agenzia può irrogare le sanzioni pecuniarie ed accessorie previste all'articolo 10 dello schema di decreto. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

Certifica che i commi 4-5 dettano disposizioni in tema di revoca dei certificati europei di cybersicurezza.

Afferma che il comma 6 disciplina l'ipotesi di accertamento dell'emissione di un certificato non conforme rilasciato ai sensi dell'articolo 56, paragrafi 4, 5 lettera b), o 6, lettere a) e b), del Regolamento, in esito alle attività di vigilanza di competenza dell'Agenzia. Stabilisce, inoltre, che le modalità di sostegno ed assistenza dell'Agenzia all'Organismo di accreditamento per l'attività di vigilanza di competenza, siano disciplinate da apposita convenzione o protocollo di intesa fra gli stessi.

Con riferimento al comma 7, evidenzia che l'Agenzia, per le prove tecniche nell'ambito delle attività di vigilanza, può effettuare valutazioni di sicurezza informatica anche attraverso esperti esterni o laboratori di prova abilitati dall'Agenzia, ai sensi dell'articolo 8, comma 4, dello schema di decreto, e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

Rileva che il comma 8 stabilisce in capo agli organismi di valutazione della conformità, ai titolari dei certificati europei di cybersicurezza ed agli emittenti delle dichiarazioni di conformità, un obbligo, durante l'attività di vigilanza a cui sono sottoposti, di cooperazione con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi.

Ribadisce che il comma 9 prevede che gli oneri derivanti dall'applicazione dei commi 3, 7 e 8 per i controlli effettuati dall'Agenzia e relativi in particolare all'impiego del personale in forza all'Agenzia, della strumentazione utilizzata nelle prove e dei materiali di consumo e per le missioni e spese generali, siano a carico dell'organismo di valutazione della conformità, del titolare del certificato o dell'emittente della dichiarazione UE di conformità sottoposto all'attività di vigilanza, come previsto dall'articolo 30, commi 4 e 5, della legge 24 dicembre 2012, n. 234. Nel caso in cui l'attività di vigilanza includa ulteriori spese, tra cui l'utilizzo di laboratori di prova esterni ed eventuali spese di trasporto per prodotti prelevati o sequestrati da sottoporre a verifica, le ulteriori spese sono ugualmente a carico del soggetto sottoposto all'attività di vigilanza. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

Al riguardo, per i profili di quantificazione, andrebbe confermato che le attività amministrative e di vigilanza facenti capo all'Autorità, possano essere da espletate dalla medesima nell'ambito delle sole risorse umane e strumentali già previste ai sensi della legislazione vigente. Parimenti, andrebbero richieste conferme in merito alla effettiva possibilità che le forme di collaborazione di cui al comma 2 potranno trovare attuazione da parte dell'Autorità potendo la stessa avvalersi a tal fine delle sole risorse umane e strumentali che sono già previste ai sensi della legislazione vigente.

In merito alle indagini previste al comma 3, posto che il successivo comma 9 pone gli oneri derivanti a carico dei soggetti vigilati, nulla da osservare. Tuttavia per le specifiche modalità di indagine anche tramite l'accesso ai locali la disposizione - peraltro espressamente richiamata al comma 2 - sembrerebbe prefigurare l'indispensabile avvalimento, da parte dell'Agenzia, anche delle forze di polizia, al fine di assicurare l'effettuazione degli accessi e dei prelievi previsti. Pertanto andrebbe chiarito se anche tale avvalimento possa essere messo a carico di tali soggetti.

Sul comma 6, andrebbe richiesta conferma che la stipula di apposite convenzioni o protocolli d'intesa con gli organismi di accreditamento da parte dell'Agenzia per il sostegno e l'assistenza potrà aver luogo senza oneri aggiuntivi per la finanza pubblica.

In relazione al comma 7, posto che la norma in esame prevede espressamente la facoltà per l'Agenzia di ricorrere, per le attività di vigilanza sulla sicurezza informatica, anche ad esperti esterni o laboratori di prova appositamente abilitati ed iscritti nell'elenco tenuto dall'Agenzia, andrebbe confermato che il ricorso a esperti o laboratori possa aver luogo potendo avvalersi delle sole risorse umane e strumentali che sono già previste dalla legislazione vigente.

Articolo 6 ***(Rilascio dei certificati di cybersicurezza)***

Il comma 1 prevede che l'Agenzia rilasci i certificati di cybersicurezza con livello di affidabilità "elevato" tramite l'Organismo di Certificazione della Sicurezza Informatica (OCSI), di cui all'articolo 60, paragrafo 2, del Regolamento, che si può avvalere di esperti od laboratori di prova, ai sensi

dell'articolo 8, comma 4, abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale, ferme restando, per specifici sistemi di certificazione, le possibili modalità di emissione dei certificati alternative ai sensi degli articoli 56, paragrafo 6, lettere a) e b), del Regolamento.

Il comma 2 stabilisce che ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità sostanziale o di base unicamente da parte di un organismo pubblico, ai sensi dell'articolo 56, paragrafo 5, del Regolamento, l'Agenzia rilascia tali certificati attraverso l'organismo di cui al comma 1. Il rilascio può avvenire ad opera di altro organismo di valutazione della conformità pubblico, accreditato dall'Organismo di Accreditamento, monitorato e vigilato dall'Agenzia, ai sensi dell'articolo 58, paragrafo 7, lettera d), del Regolamento, e designato dall'Agenzia ai sensi del provvedimento di cui all'articolo 4, comma 2, salvo diverse disposizioni dello specifico sistema europeo di certificazione.

Il comma 3 prevede che la certificazione della cybersicurezza sia volontaria, salvo diversamente specificato dal diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 56, paragrafo 2 del Regolamento. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può adottare, previa consultazione con i portatori di interesse, regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cybersicurezza ai sensi del decreto legislativo del 15 dicembre 2017, n. 223.

Il comma 4 dispone che ai sensi dell'articolo 30, commi 4 e 5, della legge n. 234 del 2012, gli oneri derivanti dall'applicazione dei commi 1 e 2 per il rilascio dei certificati da parte dell'Agenzia sono a carico del soggetto richiedente la certificazione. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

La RT conferma che la norma contiene disposizioni relative al rilascio dei certificati di cybersicurezza con livello di affidabilità elevato (comma 1) e al rilascio dei certificati con livello di affidabilità sostanziale o di base (comma 2), stabilendo al comma 3 che la certificazione della cybersicurezza è volontaria, salvo diversamente specificato dal diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 56, paragrafo 2 del Regolamento.

Sul comma 4, ribadisce che ivi si prevede che gli oneri derivanti dall'applicazione dei commi 1 e 2 per il rilascio dei certificati da parte dell'Agenzia siano a carico del soggetto richiedente la certificazione, come previsto dall'articolo 30, commi 4 e 5 della legge n. 234 del 2012. Per la determinazione e la corresponsione delle somme di cui al presente comma si fa rinvio all'articolo 13 del presente decreto.

Al riguardo, per i profili di quantificazione, premesso che la disposizione reca norme relative al rilascio dei certificati di cybersicurezza con livello di affidabilità "elevato" (comma 1) e al rilascio dei certificati con livello di affidabilità sostanziale o di "base" (comma 2), stabilendo, al comma 3, che la certificazione della cybersicurezza debba in ogni caso ritenersi "volontaria", salvo diversamente specificato dal diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 56, paragrafo 2 del Regolamento UE, nulla da osservare.

Sul comma 4, posto che ivi si prevede che all'onere della certificazione si dovrà provvedere con oneri che verranno posti a carico del richiedente, nulla da osservare.

Articolo 7 ***(Dichiarazioni UE di conformità)***

Il comma 1 stabilisce che in un sistema di certificazione in cui è autorizzata l'autovalutazione di conformità ai sensi dell'articolo 54, paragrafo 1, lettera e), del Regolamento, i fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema.

Il comma 2 prevede che il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC debba rendere disponibile all'Agenzia, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cybersicurezza ai sensi dell'articolo 54, paragrafo 1, lettera q), del Regolamento, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema. È stabilito che una copia della dichiarazione UE di conformità sia trasmessa all'Agenzia e all'ENISA.

Il comma 3 dispone che ove l'Agenzia accerti la non conformità di una dichiarazione UE di conformità in esito alle attività di vigilanza di cui all'articolo 5, comma 1, sia fatto obbligo al fabbricante o fornitore emittente di revisionare o revocare la dichiarazione UE di conformità entro trenta giorni dandone comunicazione all'Agenzia e all'ENISA, salvo diversa disposizione dello specifico sistema di certificazione.

Il comma 4 prevede che il rilascio di una dichiarazione UE di conformità debba essere volontario, salvo diversamente specificato nel diritto dell'Unione o dal diritto nazionale, ai sensi dell'articolo 53, paragrafo 4 del Regolamento. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può stabilire l'obbligatorietà della dichiarazione UE di conformità nelle fattispecie di cui all'articolo 6, comma 3.

La RT certifica che l'articolo regola l'ipotesi di dichiarazioni UE di conformità rilasciate nel caso di sistemi di certificazione in cui sia autorizzata l'autovalutazione di conformità ai sensi dell'articolo 54, par. 1, lett. e) del Regolamento. In tale ipotesi, i fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema.

Al riguardo, per i profili di quantificazione, ritenuto il tenore ordinamentale delle disposizioni, non ci sono osservazioni.

Articolo 8 ***(Accreditamento ed autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia)***

Il comma 1 prevede che l'Organismo di accreditamento, nello svolgimento dei compiti di cui ai paragrafi 1, 2 e 4 dell'articolo 60 del Regolamento, ed in conformità con le disposizioni dello specifico sistema di certificazione, comunichi all'Agenzia ed all'ufficio unico di collegamento designato per l'Italia ai sensi dell'articolo 10, comma 3, del regolamento (UE) 2019/1020, ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento per la successiva notifica da parte dell'Agenzia alla Commissione europea ai sensi dell'articolo 61 del Regolamento.

La RT evidenzia preliminarmente che la disposizione detta norme relative all'accreditamento e all'autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia.

In particolare, sul comma 1, ribadisce che ivi si prevede l'obbligo, in capo all'Organismo di accreditamento, di comunicare all'Agenzia e all'ufficio unico di collegamento, designato per l'Italia ai sensi dell'articolo 10, par. 3, del regolamento (UE) 2019/1020, ogni aggiornamento relativo agli organismi di valutazione della conformità accreditati in merito nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento per la successiva notifica da parte dell'Agenzia alla Commissione europea.

Al riguardo, non ci sono osservazioni.

Il comma 2 dispone che l'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'Organismo di accreditamento in ordine alle attività di cui al comma 1.

Il comma 3 prevede che qualora un sistema europeo di certificazione stabilisca requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera f), del Regolamento UE, solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'Agenzia a svolgere i compiti previsti da tale sistema.

La RT rileva che la disposizione stabilisce che l'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'Organismo di accreditamento, mentre, il comma 3 stabilisce che, nel caso in cui un sistema europeo di certificazione stabilisca requisiti specifici o supplementari, solo gli organismi di valutazione della conformità che soddisfano i predetti requisiti sono autorizzati dall'Agenzia a svolgere i compiti previsti dal sistema europeo di certificazione.

Al riguardo, per i profili di quantificazione, nulla da osservare.

Il comma 4 dispone che in relazione alle attività di vigilanza nazionale e di rilascio dei certificati, l'Agenzia, con provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, costituisca, aggiorni e renda pubblici due elenchi di esperti e di laboratori di prova da essa abilitati ad operare rispettivamente ai sensi dell'articolo 5, comma 7, ed ai sensi dell'articolo 6, comma 1, a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia. È stabilito che gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati di cui all'articolo 5, comma 7, non possano effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale ai sensi dell'articolo 56, paragrafo 4, o paragrafo 5(b) del Regolamento, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati. Con la medesima procedura di cui al primo periodo, sono individuate le modalità per l'abilitazione e l'eventuale rinnovo, l'inserimento, la sospensione e la cancellazione di esperti e laboratori di prova dai suddetti elenchi.

Il comma 5 prevede che ai sensi dell'articolo 30, commi 4 e 5, della legge n. 234 del 2012, gli oneri derivanti dall'abilitazione di cui al comma 4, le spese per le eventuali attività di autorizzazione di cui al

comma 3, e gli eventuali successivi aggiornamenti sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

La RT conferma che sul comma 4 che la norma si limita a prevedere la costituzione, l'aggiornamento e la pubblicità di un elenco di esperti e un elenco di laboratori di prova abilitati dall'Agenzia ad operare, rispettivamente, ai sensi dell'articolo 5, comma 8 ed ai sensi dell'articolo 6, comma 1, dello schema di decreto, a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia.

Tali elenchi, sono costituiti con provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223. Gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati di cui all'articolo 5, comma 8, dello schema di decreto, non possono effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale ai sensi dell'art. 56, paragrafo 4, o paragrafo 5(b), del Regolamento, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati. Le modalità per l'abilitazione e l'eventuale rinnovo, l'inserimento, la sospensione e la cancellazione di esperti e laboratori di prova dai suddetti elenchi, sono individuate con provvedimento adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del richiamato regolamento adottato con DPCM n. 223 del 2021.

Quindi, sul comma 5, certifica che la norma ivi prevista stabilisce che, ai sensi dell'articolo 30, commi 4 e 5 della legge n. 234 del 2012, gli oneri derivanti dall'abilitazione di cui al comma 3, le spese per le eventuali attività di autorizzazione di cui all'articolo 8, comma 3, dello schema di decreto, e gli eventuali successivi aggiornamenti sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione. Le somme di cui al presente comma sono determinate e sono da corrispondere ai sensi dell'articolo 13.

Al riguardo, per i profili di quantificazione, sul comma 4, andrebbe confermato che l'istituzione e l'aggiornamento degli elenchi di cui si dispone l'istituzione presso l'Agenzia possano essere attività nell'ambito delle sole risorse umane e strumentali per questa già previste ai sensi della legislazione vigente.

Sul punto, venendo anche al comma 5, va sottolineato che ai sensi della norma ivi prevista, i soli oneri riconducibili all'attività istruttoria finalizzata al rilascio della dall'abilitazione (comma 3), nonché quelli relativi a spese per le eventuali attività di autorizzazione e gli eventuali successivi aggiornamenti, sono posti a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione.

Pertanto, andrebbe richiesta una conferma in merito alle spese di tenuta e aggiornamento dell'elenco da parte dell'Agenzia a valere delle sole risorse previste ai sensi dalla legislazione vigente.

Articolo 9

(Attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza)

Il comma 1 prevede che allo scopo di elevare il livello nazionale di cybersicurezza, l'Agenzia possa realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di *software*, e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale.

Il comma 2 stabilisce che l'Agenzia monitora gli sviluppi nel campo della certificazione della cybersicurezza, anche consultando i portatori di interesse nazionale del settore e scambiando informazioni, esperienze e buone pratiche con la Commissione europea e le altre autorità nazionali della cybersicurezza.

Il comma 3 conferma che la norma dispone conformemente all'articolo 57 del Regolamento ed in assenza di un sistema europeo di certificazione, che l'Agenzia può introdurre sistemi di certificazione nazionali della cybersicurezza, per prodotti TIC, servizi TIC o processi TIC.

La RT precisa che l'articolo contiene disposizioni in materia di attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza, prevedendo che l'Agenzia possa realizzare progetti di ricerca, ivi inclusi quelli per lo sviluppo di *software*, e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale con il fine di elevare il livello nazionale di cybersicurezza.

Certifica che tale disposizione riveste carattere meramente ordinamentale e non comporta nuovi o maggiori oneri a carico della finanza pubblica. A tal proposito, rappresenta che la realizzazione di progetti di ricerca è già prevista dall'articolo 7, comma 1, lettera r), del decreto-legge n. 82 del 2021, che dispone che l'Agenzia, perseguendo obiettivi di eccellenza, supporti negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca, nonché del sistema produttivo nazionale, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e che possa promuovere, sviluppare e finanziare specifici progetti e iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. Tali funzioni, pertanto, verranno svolte nell'ambito delle risorse, di cui all'articolo 18 del decreto-legge n. 82 del 2021, già assegnate all'Agenzia.

Al riguardo, per i profili di quantificazione, si rinvia all'articolo 4.

CAPO III
SANZIONI, RECLAMI E RICORSI GIURISDIZIONALI

Articolo 10
(Quadro sanzionatorio)

Il comma 1 stabilisce che l'Agenzia, anche ai sensi dell'articolo 7, comma 1, lettera e), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, in caso di violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, ai sensi dell'articolo 58, paragrafo 8, lettera f), e dell'articolo 65 del Regolamento UE irroghi sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. Si applica, in quanto compatibile, la disciplina della legge 24 novembre 1981, n. 689.

Il comma 2 prevede che salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che emette un certificato di cybersicurezza non conforme sia punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. È previsto che in caso di omessa revoca di un certificato da parte dell'organismo su richiesta dell'Agenzia ai sensi dell'articolo 5, comma 5, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

Il comma 3 dispone che, salvo che il fatto costituisca reato, il fabbricante o fornitore che emette una dichiarazione UE di conformità volontaria non conforme sia punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. È stabilito che in caso di omessa revisione o revoca di dichiarazione UE di conformità volontaria o obbligatoria ai sensi dell'articolo 7, comma 3, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

Il comma 4 prevede che salvo che il fatto costituisca reato, in caso di obbligatorietà di una dichiarazione UE di conformità, ai sensi dell'articolo 7, comma 4, o di un certificato di cybersicurezza, ai sensi dell'articolo 6, comma 3, il fabbricante o fornitore che mette a disposizione sul mercato un prodotto TIC o servizio TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza del certificato di cybersicurezza obbligatorio, è punito con la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. È previsto che alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC si avvale di un processo TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza di certificato di cybersicurezza obbligatorio.

Il comma 5 afferma che nei casi di cui al comma 4 oppure ove, in esito ad un accertamento di non conformità ai sensi dei commi 4, 5 o 6 dell'articolo 5, sia revocato o decada un certificato obbligatorio per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già immessi sul mercato o per l'inibizione del servizio;

Il comma 6 prevede che salvo che il fatto costituisca reato, il fabbricante che non ottemperi a quanto prescritto al comma 5 per il richiamo di prodotti già immessi sul mercato sia assoggettato alla sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. È stabilito che nel caso in cui il fabbricante non ottemperi al richiamo di prodotti dal mercato, l'Agenzia, trascorsi sei mesi dalla scadenza fissata, può provvedere, al sequestro dei prodotti in questione dal mercato, a spese del fabbricante.

Il comma 7 stabilisce che salvo che il fatto costituisca reato, il fornitore che non ottemperi a quanto prescritto al comma 5 per l'inibizione del servizio dal mercato sia assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro.

Il comma 8 dispone che salvo che il fatto costituisca reato, Il titolare di un certificato europeo di cybersicurezza che non notifichi, ai sensi dell'articolo 56, paragrafo 8, del Regolamento, eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC o processi

TIC certificati è punito con la sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità emittente un certificato di cybersicurezza il suo titolare ovvero il fornitore o fabbricante emittente una dichiarazione UE di conformità, che dovesse rilevare o venire a conoscenza della presenza di vulnerabilità nel prodotto TIC, servizio TIC o processo TIC certificato o dichiarato conforme, che non siano state riscontrate durante il processo di valutazione, e non ottemperari agli obblighi riguardanti il modo in cui segnalare e trattare le vulnerabilità previste per lo specifico sistema di certificazione ai sensi dell'articolo 54, paragrafo 1, lettera m), del Regolamento.

Il comma 9 prevede che salvo che il fatto costituisca reato, il fabbricante o fornitore che non renda disponibile, per il periodo stabilito ai sensi dell'articolo 54, paragrafo 1, lettera q), del Regolamento, la dichiarazione UE di conformità o la documentazione tecnica o tutte le altre informazioni pertinenti o non trasmetta una copia della dichiarazione UE di conformità all'Agenzia o ad ENISA ai sensi dell'articolo 53, paragrafo 3, del Regolamento ovvero non renda disponibili pubblicamente una o più delle informazioni previste ai sensi dell'articolo 55 del Regolamento o non rispetti il formato o le procedure di aggiornamento delle stesse informazioni ai sensi dell'articolo 54, paragrafo 1, lettera v), del Regolamento o pubblichi informazioni non corrette sui certificati detenuti o sulle dichiarazioni UE di conformità emesse, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fornitore o fabbricante che non comunichi la revisione o la revoca di una dichiarazione UE di conformità ai sensi dell'articolo 7, comma 3, del presente decreto.

Il comma 10 afferma che salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottemperari agli obblighi di divulgazione dei certificati europei di cybersicurezza rilasciati, modificati o revocati come previsto nell'ambito dello specifico sistema di certificazione, ai sensi dell'articolo 54, paragrafo 1, lettera s), del Regolamento, nonché secondo le modalità di cui all'articolo 5, comma 6, sia assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. È stabilito che alla medesima sanzione sia assoggettato l'organismo di valutazione della conformità autorizzato dall'Agenzia ai sensi dell'articolo 60, paragrafo 3, del Regolamento, che non specifichi nella procedura per i reclami definita ai sensi dell'articolo 11, comma 2, l'inoltro degli stessi per conoscenza anche all'Agenzia.

Il comma 11 dispone che salvo che il fatto costituisca reato, nel caso di accertamento di esercizio di organismo di valutazione della conformità senza autorizzazione di cui all'articolo 60, paragrafo 3, del Regolamento si applichi la sanzione del pagamento di una somma da 120.000 euro a 600.000 euro e al soggetto non possono essere rilasciate ulteriori autorizzazioni nei successivi tre anni dall'accertamento della violazione. Se l'autorizzazione è scaduta da meno di un anno la sanzione è compresa tra 30.000 euro e 150.000 euro ed il soggetto può richiedere il rilascio di nuova autorizzazione.

Il comma 12 afferma che salvo che i fatti costituiscano reato, il richiedente di una certificazione che nell'ambito dello svolgimento dell'attività di valutazione e di rilascio dei certificati, scientemente, fornisce dati, informazioni o documentazione falsi o ometta informazioni necessarie per espletare la certificazione, in violazione dell'articolo 54, paragrafo 1, lettera h), e dell'articolo 56, paragrafo 7, del Regolamento, è assoggettato alla sanzione del pagamento di una somma da 90.000 euro a 450.000 euro. È previsto che alla medesima sanzione sia assoggettato il soggetto che, scientemente, durante le verifiche di vigilanza, a cui è sottoposto, ai sensi dell'articolo 5, comma 5, fornisce dati, informazioni o documentazione falsi.

Il comma 13 evidenzia che salvo che il fatto costituisca reato, il fabbricante che violi le condizioni di utilizzo degli eventuali marchi o etichette previste da un sistema europeo di certificazione, ai sensi dell'articolo 54, paragrafo 1, lettera i), del Regolamento, sia assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

Il comma 14 prevede che salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottemperari agli eventuali obblighi riguardanti la conservazione dei registri di cui

all'articolo 54, paragrafo 1, lettera n), del Regolamento, sia assoggettato alla sanzione del pagamento di una somma da 45.000 euro a 225.000 euro.

Il comma 15 afferma che l'Agenzia può impartire ordini o intimare diffide ai soggetti che operano in contrasto al quadro europeo di certificazione. È previsto che ai soggetti che non ottemperino nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 euro ad 1.000.000 di euro. Se le violazioni riguardano provvedimenti adottati dall'Agenzia nei confronti di soggetti con fatturato pari almeno a 200.000.000 euro, si applica a ciascun soggetto interessato una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e non superiore all' 1,5 per cento del fatturato, restando comunque fermo il limite massimo di 5.000.000 di euro. Come riferimento per il fatturato si assume il valore realizzato dallo stesso soggetto nell'esercizio precedente a quello in cui sia stato impartito l'ordine o sia stata intimata la diffida.

Il comma 16 dispone che fermo restando il limite massimo di 5.000.000 di euro per la sanzione, i valori minimi e massimi delle sanzioni pecuniarie dal comma 2 al comma 15, siano triplicati, se la violazione ha riguardato un certificato relativo ad un prodotto TIC, un servizio TIC o un processo TIC rilasciato nell'ambito di un sistema di certificazione destinato, ai sensi dell'articolo 54, paragrafo 1, lettere a) o b), del Regolamento, all'utilizzo con le finalità o nell'ambito di un servizio essenziale ai sensi dell'allegato II del decreto legislativo 18 maggio 2018, n. 65, o di un servizio di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera fff), del decreto legislativo 1° agosto 2003, n. 259.

Il comma 17 prevede che i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie siano definiti con successivo provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223. È stabilito che nelle more dell'adozione del provvedimento di definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della legge 24 novembre 1981, n. 689.

Il comma 18 stabilisce che fermo restando il limite massimo di 5.000.000 di euro per la sanzione, le sanzioni amministrative pecuniarie previste ai commi dal 2 al 14, siano rivalutate ogni cinque anni con provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, in misura pari all'indice ISTAT dei prezzi al consumo previo arrotondamento all'unità di euro secondo il seguente criterio: se la parte decimale è inferiore a 50 centesimi l'arrotondamento va effettuato per difetto, se è uguale o superiore a 50 centesimi l'arrotondamento va effettuato per eccesso. È stabilito che l'importo della sanzione pecuniaria rivalutato secondo i predetti criteri si applichi esclusivamente per le violazioni commesse successivamente alla data di entrata in vigore del provvedimento che lo prevede.

Il comma 19 prevede che l'autorizzazione di un organismo di valutazione della conformità ad operare nel sistema europeo di certificazione ai sensi dell'articolo 60, paragrafo 3, del Regolamento, ove prevista, sia sospesa per 6 mesi o revocata nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio. È previsto che in caso di revoca dell'autorizzazione, il trasgressore non può ottenere nuova autorizzazione nei successivi cinque anni dal provvedimento di revoca.

Il comma 20 dispone che l'Agenzia notifichi alla Commissione europea il quadro sanzionatorio di cui al presente articolo entro sessanta giorni dall'entrata in vigore del presente decreto e provvede poi a dare notifica delle eventuali modifiche entro sessanta giorni successivi alle stesse.

La RT certifica che l'articolo definisce il sistema delle sanzioni applicabili per la violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, ai sensi dell'articolo 58, paragrafo 8, lettera J), e dell'articolo 65 del Regolamento UE.

Come anticipato in premessa, l'articolo 18, comma 2, lettera c), della legge di delega n. 53 del 2021, in deroga ai limiti previsti dall'articolo 32, comma 1, lettera d),

della legge 24 dicembre 2012, n. 234, stabilisce che le sanzioni amministrative pecuniarie non devono essere inferiori nel minimo a 15.000 euro e non devono essere superiori nel massimo a 5.000.000 di euro.

Rileva, al riguardo, il comma 17 dell'articolo 10 dello schema di decreto prevede che con successivo provvedimento dell'Agenzia, adottato secondo la procedura di cui all'articolo 5, comma 3, alinea, del DPCM 9 dicembre 2021, n. 223, saranno definiti i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie previste dal presente decreto. Nelle more dell'adozione del provvedimento di definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della L. 24 novembre 1981, n. 689.

Ai sensi dell'articolo 18, comma 2, lettera c), della legge n. 53 del 2021 e dell'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021, l'Agenzia, in caso di violazione dei predetti obblighi può irrogare sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. La predetta attività sanzionatoria genera introiti per l'Agenzia che saranno riutilizzati per costituire una dotazione variabile per le attività di ricerca e formazione.

Il comma 3 dell'articolo non comporta nuovi o maggiori oneri per la finanza pubblica in quanto trattasi di sanzioni di nuova istituzione.

Infatti, si ritiene utile rappresentare che l'articolo 21 del decreto legislativo 18 maggio 2018, n. 65 detta l'apparato sanzionatorio per la violazione degli obblighi previsti dalla direttiva (UE) 2016/1148; ai sensi dell'articolo 7, comma 1, lettera d), del D.L. n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale è individuata quale autorità nazionale competente NIS (art. 8, par. 1 della direttiva (UE) 2016/1148) ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto legislativo n. 65 del 2018.

Il regolamento (UE) 2019/881, invece - oggetto del presente schema di decreto legislativo prevede, all'articolo 58, par. 7, lettera f), tra le funzioni delle autorità nazionali di certificazione della cybersicurezza, quella di "irrogare sanzioni conformemente al diritto nazionale, a norma dell'articolo 65, e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente regolamento".

Nella sua qualità di autorità nazionale di certificazione della cybersicurezza, l'Agenzia svolge la predetta funzione.

Gli ambiti previsti dai citati atti europei (direttiva (UE) 2016/1148 e regolamento (UE) 2019/881) sono diversi e prevedono obblighi distinti, pertanto, le attività svolte dall'Agenzia in tali ambiti sono distinte e non sussiste, dunque, sovrapposizione tra le sanzioni previste dall'articolo 10 del presente schema di decreto legislativo e l'articolo 21 del decreto legislativo n. 65/2018.

Ciò risulta, peraltro, evidente dalle fattispecie di sanzioni di cui all'articolo 21 del d.lgs n. 65 del 2018, che prevedono inosservanza di obblighi riguardanti l'adozione di misure di sicurezza o notifica di incidenti in capo a fornitori di servizi essenziali o servizi digitali, mentre l'articolo 10 del presente schema di decreto legislativo prevede obblighi in capo a diversi soggetti riguardanti la gestione dei certificati europei di

cybersicurezza e le dichiarazioni UE di conformità associate a prodotti, servizi e processi TIC.

Le sanzioni introdotte con il presente schema di decreto legislativo costituiscono, dunque, nuove sanzioni — non precedentemente irrogate — per inosservanza degli obblighi introdotti dal regolamento (UE) 2019/881, successivo alla direttiva (UE) 2016/1148, e che investe un ambito distinto rispetto all'ambito trattato dalla direttiva.

Al riguardo, per i profili di quantificazione, ritenuto il tenore avente mero rilievo ordinamentale delle disposizioni in esame e in considerazione del carattere "eventuale" delle maggiori entrate derivanti dalla irrogazione delle sanzioni, nulla da osservare.

Si rinvia all'articolo 13.

Articolo 11

(Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità)

Il comma 1 riconosce alle persone fisiche e giuridiche hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di cybersicurezza o all'Agenzia se il reclamo riguarda un certificato europeo di cybersicurezza rilasciato dall'organismo di certificazione dell'Agenzia o da suo organismo di valutazione della conformità che agisce in conformità all'articolo 56, paragrafo 6, del Regolamento. È stabilito che l'Agenzia, ai sensi dell'articolo 58, paragrafo 7, lettera f), del Regolamento, tratta inoltre i reclami degli stessi in relazione alle dichiarazioni UE di conformità di cui all'articolo 7.

Il comma 2 prevede che avverso le decisioni degli organismi di valutazione della conformità diversi dall'organismo di certificazione ai sensi dell'articolo 6, comma 1, può essere proposta procedura di reclamo a tal fine indicata dagli stessi organismi. È stabilito che nel caso di autorizzazione ai sensi dell'articolo 60, paragrafo 3, del Regolamento, la procedura di reclamo indicata dall'organismo preveda l'inoltro del reclamo da parte del reclamante oltretutto all'organismo anche per conoscenza all'Agenzia.

Il comma 3 stabilisce che avverso le decisioni dell'Agenzia riguardanti le certificazioni oppure le dichiarazioni UE di conformità rilasciate ai sensi dell'articolo 53 del Regolamento può essere proposta procedura di reclamo. È previsto che il reclamante formuli istanza all'Agenzia, identificando il certificato di cybersicurezza o la dichiarazione UE di conformità oggetto del reclamo, le ragioni del reclamo e le azioni correttive che ritiene necessarie.

Il comma 4 prevede che l'Agenzia, a seguito di un reclamo ai sensi del comma 3, informi il reclamante dello stato del procedimento e della decisione adottata e informa il reclamante del diritto a un ricorso giurisdizionale effettivo. È stabilito che l'Agenzia risponde ai reclami entro novanta giorni dal ricevimento dell'istanza. In caso di mancata risposta ad un reclamo inoltrato all'Agenzia entro i termini previsti, lo stesso è da intendersi rigettato.

La RT si limita a certificare che l'articolo contiene disposizioni in materia di reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità.

La disposizione ha carattere ordinamentale e, pertanto, non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Al riguardo, per i profili di quantificazione, nulla da osservare.

Articolo 12 ***(Ricorso all'autorità giudiziaria)***

Il comma 1 prevede che fatti salvi eventuali ricorsi amministrativi o altri ricorsi extragiudiziali, le persone fisiche e giuridiche hanno diritto a un ricorso giurisdizionale effettivo per quanto riguarda: a) le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cybersicurezza detenuto da tali persone fisiche e giuridiche; b) il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformità.

Il comma 2 stabilisce che i procedimenti a norma del presente articolo sono presentati dinanzi al Tribunale Amministrativo Regionale del Lazio per quanto riguarda i ricorsi contro l'Agenzia ed al Tribunale Amministrativo del luogo ove è ubicata la sede degli altri organismi di valutazione della conformità per i ricorsi contro tali organismi.

La RT certifica che la norma descrive le modalità per i ricorsi giurisdizionali in relazione ai certificati europei di cybersicurezza.

La disposizione ha carattere ordinamentale e, pertanto, non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Al riguardo, per i profili di quantificazione, non ci sono osservazioni.

CAPO IV **DISPOSIZIONI FINANZIARIE**

Articolo 13 ***(Destinazione dei proventi derivanti dalle attività dell'Agenzia)***

Il comma 1 prevede che le attività di vigilanza di cui all'articolo 5, comma 1, di certificazione di cui all'articolo 6, comma 1, di autorizzazione di cui all'articolo 8, comma 3, di abilitazione di cui all'articolo 8, comma 4, sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi. I relativi proventi sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione degli appositi capitoli dell'Agenzia. Con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del Direttore generale dell'Agenzia, sono determinate le tariffe e modalità di riscossione.

La RT conferma che la norma contiene disposizioni relative alla destinazione dei proventi derivanti dall'attività dell'Agenzia.

Il comma 1, in tal senso, stabilisce che le attività di vigilanza (art. 58.7 del Regolamento e articolo 5 dello schema di decreto), di certificazione (art. 56.5.(a) e art. 56.6) del Regolamento e articolo 6, comma 1 dello schema di decreto) e di autorizzazione ed abilitazione di esperti, di laboratori di prova, ed organismi di valutazione della conformità (art. 60.3 del Regolamento e articolo 8 dello schema di decreto) sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi. I relativi proventi sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e

delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione degli appositi capitoli dell'Agenzia.

Con decreto del Presidente del Consiglio dei ministri sono determinate le tariffe e modalità di riscossione.

Al riguardo, per i profili di quantificazione, posto che la norma si limita a prevedere il versamento al bilancio dello Stato dei proventi relativi all'applicazione delle tariffe e ai fini della riassegnazione dei relativi importi a valere della dotazione di spesa prevista per l'Agenzia, nulla da osservare.

Il comma 2 dispone che le spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza di cui all'articolo 5, comma 1, sono calcolate ai sensi del decreto di cui al comma 1.

Il comma 3 prevede che gli introiti derivanti dalle sanzioni pecuniarie di cui all'articolo 10 sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione dei capitoli del bilancio dell'Agenzia destinati alle attività di ricerca e formazione concernenti la certificazione della cybersicurezza di prodotti TIC, servizi TIC e processi TIC di cui all'articolo 9, comma 1.

La RT ribadisce sul comma 2 stabilisce che le spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza di cui all'articolo 5, comma 1, dello schema di decreto, sono calcolate ai sensi del comma 1.

Quanto al comma 3, infine, si stabilisce che gli introiti derivanti dalle sanzioni pecuniarie di cui all'articolo 10 dello schema di decreto, sono versati ad apposito capitolo del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione dei capitoli del bilancio dell'Agenzia destinati alle attività e ai progetti di ricerca, ivi inclusi quelli per lo sviluppo di software, e di formazione concernenti la certificazione della cybersicurezza di prodotti TIC, servizi TIC e processi TIC di cui all'articolo 9, comma 1.

Al riguardo, per i profili di quantificazione, non ci sono osservazioni.

Articolo 14 ***(Ulteriori disposizioni finanziarie)***

Il comma 1 prevede che agli oneri derivanti dall'articolo 4, comma 3, pari a 657.500 euro per l'anno 2022, 592.500 euro per l'anno 2023 e 637.500 euro annui a decorrere dall'anno 2024 si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234.

Il comma 2 dispone che le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi all'articolo 4, comma 3, sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1 della legge 28 dicembre 2015, n. 208.

Il comma 3 stabilisce che dall'attuazione del presente decreto, ad esclusione dell'articolo 4, comma 3, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

Il comma 4 dispone che il Ministro dell'economia e delle finanze sia autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati in attuazione del presente articolo e dell'articolo 13.

La RT certifica che posto che gli introiti previsti all'articolo 13 non sono sufficienti per garantire l'operatività dell'Agenzia, stabilisce che agli oneri per le attività che la stessa dovrà svolgere nell'esercizio dei suoi compiti in ambito nazionale di certificazione della cybersicurezza, individuate all'articolo 4, comma 3, e stimati in complessivi euro 657.500 per il 2022, euro 592.500 per l'anno 2023 e per euro 637.500 dal 2024, si farà fronte facendo ricorso al fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234, come previsto dall'articolo 1 della medesima legge n. 53 del 2021.

Ciò, in considerazione del fatto che l'individuazione dell'autorità nazionale di certificazione della cybersicurezza, e l'attribuzione alla stessa di adeguate risorse, costituisce adempimento di obblighi europei e che, a tal fine, è stata conferita una delega al Governo con l'articolo 18 della citata legge n. 53 del 2021.

Sul comma 2 evidenzia che la norma stabilisce che le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi all'articolo 4, comma 3, sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dei commi da 512 a 520, dell'articolo 1, della legge 28 dicembre 2015, n. 208 e successive modificazioni.

Quanto al comma 3 rileva che la norma ivi prevista dispone che dall'attuazione del presente decreto, ad esclusione dall'articolo 4, comma 3, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l'Agenzia provvederà con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

Ai sensi del comma 4, il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati in attuazione del presente articolo e dell'articolo 13.

Al riguardo, per i profili di copertura, sul comma 1, posto che alla compensazione degli oneri specificamente previsti dall'articolo 4, comma 3, si provvede a valere della dotazione prevista in bilancio in relazione al fondo per l'attuazione della normativa europea¹, andrebbero richieste conferme in merito alle disponibilità ivi esistenti per il triennio 2022/2024 e a decorrere, libere da impegni già perfezionati o in via di

¹ Capitolo 2815 iscritto nello stato di previsione del ministero dell'economia e delle finanze del bilancio 2022/2024, recante uno stanziamento annuo di 213,2; 215,2 e 216,2 milioni per le annualità del triennio.

perfezionamento, nonché rassicurazioni in merito alla adeguatezza delle rimanenti risorse a fronte del recepimento previsto in relazione alla normativa comunitaria.

Quanto al comma 3, dal momento che ivi è riportata la clausola di invarianza per cui dall'attuazione del presente decreto, ad esclusione dell'articolo 4, comma 3, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che l'Agenzia provvederà con le risorse umane, strumentali e finanziarie previste a legislazione vigente, va rammentato che il comma 6-*bis* dell'articolo 17 della legge di contabilità prescrive che in presenza di siffatte clausole, la RT debba essere completa dell'illustrazione dei dati ed elementi informativi idonei a comprovarne l'effettiva sostenibilità.

CAPO V DISPOSIZIONI FINALI

Articolo 15

(Successiva attuazione nazionale dei sistemi europei di certificazione)

L'articolo prevede che ai nuovi sistemi europei di certificazione che sono adottati dalla Commissione europea ai sensi dell'articolo 49, paragrafo 7, del Regolamento e che non siano autonomamente applicabili nel quadro di certificazione nazionale vigente, sia data attuazione modificando o integrando il provvedimento di cui all'articolo 4, comma 2, in ogni aspetto operativo necessario per dare piena attuazione al nuovo sistema europeo di certificazione.

La RT stabilisce che ai nuovi sistemi europei di certificazione, che sono adottati dalla Commissione europea ai sensi dell'articolo 49, paragrafo 7, del Regolamento, e che non siano autonomamente applicabili nel quadro di certificazione nazionale vigente, sia data attuazione modificando o integrando il provvedimento di cui all'articolo 4, comma 2, in ogni aspetto operativo necessario per dare piena attuazione al nuovo sistema europeo di certificazione.

L'articolo contiene disposizioni di carattere ordinamentale e, pertanto, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

Al riguardo, per i profili di quantificazione, nulla da osservare.