

## COMMISSIONI RIUNITE

### I (Affari costituzionali, della Presidenza del Consiglio e interni) e IX (Trasporti, poste e telecomunicazioni)

#### S O M M A R I O

##### ATTI DEL GOVERNO:

Schema di decreto legislativo recante norme di 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 n. 388 (*Esame, ai sensi dell'articolo 143, comma 4, del Regolamento, e rinvio*) ..... 3

##### ATTI DEL GOVERNO

*Giovedì 26 maggio 2022. — Presidenza della presidente della IX Commissione Raffaella PAITA.*

##### **La seduta comincia alle 14.20.**

**Schema di decreto legislativo recante norme di 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 n. 388.**

*(Esame, ai sensi dell'articolo 143, comma 4, del Regolamento, e rinvio).*

Le Commissioni iniziano l'esame dello schema di decreto in titolo.

Raffaella PAITA, *presidente e relatrice per la IX Commissione*, avverte, anzitutto, che, come specificato anche nelle convocazioni, alla luce di quanto stabilito dalla

Giunta per il Regolamento nella riunione del 4 novembre 2020, i deputati possono partecipare all'odierna seduta in videoconferenza, in quanto non sono previste votazioni sul provvedimento.

Fa presente quindi che le Commissioni riunite I e IX sono chiamate a esaminare, ai fini del parere al Governo, lo schema di decreto legislativo recante norme di 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 n. 388).

Dichiara dunque di riferire sul quadro regolatorio di riferimento e sulle disposizioni generali dello schema di decreto.

Lo schema di decreto attua la delega prevista dall'articolo 18 della legge di delegazione europea 2019-2020 – legge n. 523 del 2021 – volta all'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 2019/881 del 17 aprile 2019, relativo all'Agenzia dell'Unione euro-

pea per la cybersicurezza (*European Union Agency for Network and Information Security – ENISA*) e al quadro europeo della certificazione di cui al titolo III del medesimo regolamento.

Il provvedimento dà attuazione ad alcune disposizioni del titolo III del regolamento, relative alla certificazione della cybersicurezza dei prodotti, dei servizi e dei processi relativi alle tecnologie dell'informazione e della comunicazione (ICT).

Ricorda che i regolamenti dell'Unione europea sono atti giuridici definiti nell'articolo 288 del trattato sul funzionamento dell'Unione europea (TFUE). Sono atti di applicazione generale, vincolanti in tutti i loro elementi e direttamente applicabili in tutti i Paesi membri, senza dover essere trasposti in una legge nazionale. Tuttavia, in alcuni casi – come in quello in esame – è lo stesso regolamento che rinvia all'adozione di norme nazionali per la sua piena applicabilità. In particolare, al fine di dare attuazione al regolamento sulla cybersicurezza – principalmente con riferimento agli articoli 58, 60, 61, 63, 64 e 65 dello stesso – è necessario che ciascuno Stato membro adotti alcuni interventi normativi a livello nazionale.

Per quanto riguarda il regolamento UE sulla cybersicurezza (UE) 2019/881, che ha l'obiettivo di rafforzare la cybersicurezza dell'Unione, esso introduce una nuova disciplina dell'Agenzia dell'Unione europea per la cybersicurezza e un sistema comune di certificazione delle tecnologie dell'informazione e delle comunicazioni (ICT).

Il regolamento è diviso in quattro parti. Il Titolo I – articoli 1 e 2 – contiene disposizioni generali (oggetto, ambito di applicazione e definizioni).

Il Titolo II – articoli da 3 a 45 – è dedicato a delineare la nuova regolamentazione dell'ENISA, Agenzia dell'Unione europea per la cybersicurezza, centro di competenze in materia di sicurezza informatica che ha sede ad Atene. Essa collabora con l'UE e con i Paesi membri per prevenire, rilevare e contrastare i problemi di sicurezza dell'informazione. Fornisce in tal senso consigli e soluzioni per il settore pubblico e privato. Fra le sue attività rientrano: 1)

l'organizzazione di esercitazioni di crisi informatiche in tutta Europa; 2) l'assistenza per lo sviluppo di strategie nazionali di sicurezza informatica; 3) la promozione della cooperazione fra le squadre di pronto intervento informatico e lo sviluppo di capacità. L'ENISA pubblica altresì relazioni e studi sulle questioni di sicurezza informatica e nuove tecnologie.

Il Titolo III – articoli da 46 a 65 – oggetto di attuazione con il provvedimento in esame, istituisce il quadro europeo di certificazione della cybersicurezza, ovvero un meccanismo volto a istituire un sistema europeo comune di certificazione della cybersicurezza e ad attestare che i prodotti, servizi e processi ICT valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati, o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita.

In particolare, l'articolo 51 descrive gli obiettivi di sicurezza dei sistemi europei.

L'articolo 52 ne illustra i livelli di affidabilità e l'articolo 54 ne elenca gli elementi.

L'articolo 56 disciplina la certificazione della cybersicurezza, specificando che i prodotti, servizi e processi ITC certificati ricorrendo ad un sistema europeo di certificazione sono considerati conformi ai requisiti di tale sistema. La certificazione è volontaria, salvo quando diversamente specificato dal diritto dell'Unione o degli Stati membri.

L'articolo 57 specifica che eventuali sistemi nazionali di certificazione della cybersicurezza che risultino coperti da un sistema europeo cessano di produrre effetti a decorrere dalla data di entrata in vigore del sistema europeo medesimo.

L'articolo 58 prevede l'istituzione di un'Autorità nazionale di certificazione della cybersicurezza, con il compito di far rispettare nel proprio territorio nazionale le disposizioni del Titolo III e dei successivi sistemi europei di certificazione adottati nell'Unione ed il compito di emissione dei certificati di livello elevato; la definizione

di un quadro sanzionatorio per permettere alle Autorità nazionali di far rispettare il regolamento europeo e i successivi sistemi di certificazione adottati nell'Unione europea.

Per quanto riguarda il primo profilo, segnala come l'Agenzia per la cybersicurezza nazionale (ACN) abbia già assunto la funzione di Autorità nazionale di certificazione della cybersicurezza in virtù di quanto disposto dall'articolo 7, comma 1, lettera e), del decreto-legge n. 82 del 2021.

L'articolo 60 stabilisce che tali certificati siano rilasciati da organismi di valutazione della conformità operanti al livello nazionale.

Ai sensi dell'articolo 62, a livello sovranazionale, opera il Gruppo europeo per la certificazione della cybersicurezza, composto da rappresentanti delle Autorità nazionali.

Il Titolo IV (articoli 66-69) contiene alcune disposizioni finali. In particolare, l'articolo 69, paragrafo 2, prevede per la sua completa applicazione, l'adozione, da parte di ciascun Paese membro, degli adempimenti per l'attuazione degli articoli 58, 60, 61, 63, 64 e 65 entro due anni dall'entrata in vigore del medesimo regolamento (entro cioè il 28 giugno 2021).

Con riferimento al quadro normativo interno in cui si colloca il provvedimento, ricorda che in materia di certificazione della sicurezza informatica, il decreto del Presidente del Consiglio dei ministri 30 ottobre 2003 definisce lo schema nazionale per la valutazione e la certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione. Lo schema reca l'insieme delle procedure e delle regole nazionali necessarie per la valutazione e certificazione, conformemente ai criteri europei o agli standard internazionali.

L'articolo 2, comma 2, del d.P.C.M. specifica che le procedure relative allo schema nazionale devono essere osservate « dall'organismo di certificazione, dai laboratori per la valutazione della sicurezza, nonché da tutti coloro, persone fisiche, giuridiche e qualsiasi altro organismo o associazione, cui competono le decisioni in ordine alla

richiesta, acquisizione, progettazione, realizzazione, installazione ed impiego di sistemi e prodotti nel settore della tecnologia dell'informazione, per i quali la sicurezza costituisce uno dei requisiti e che necessitano di una certificazione di sicurezza ». Vengono regolate, all'articolo 3, una procedura di valutazione e la relativa certificazione.

Il medesimo d.P.C.M., all'articolo 4, individua nell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCTI), poi accorpato nella nuova Direzione Generale per le Tecnologie delle Comunicazioni e la Sicurezza Informatica – Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (DGCTSI-ISCTI) del Ministero dello sviluppo economico, l'Organismo di Certificazione della Sicurezza Informatica (OCSI). L'OCSI gestisce lo schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione e sovrintende alle attività operative di valutazione e certificazione attraverso: la predisposizione di regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie e internazionali di riferimento; il coordinamento delle attività nell'ambito dello Schema nazionale in armonia con i criteri ed i metodi di valutazione; la predisposizione delle Linee Guida per la valutazione di prodotti, traguardi di sicurezza, profili di protezione e sistemi, ai fini del funzionamento dello Schema; la divulgazione dei principi e delle procedure relative allo Schema nazionale; l'accreditamento, la sospensione e la revoca dell'accreditamento degli LVS; la verifica del mantenimento dell'indipendenza, imparzialità, affidabilità, competenze tecniche e capacità operative da parte degli LVS accreditati; l'approvazione dei Piani di Valutazione; l'ammissione e l'iscrizione delle valutazioni; l'approvazione dei Rapporti Finali di Valutazione; l'emissione dei Rapporti di Certificazione sulla base delle valutazioni eseguite dagli LVS; l'emissione e la revoca dei Certificati; la definizione, l'aggiornamento e la diffusione, almeno su base semestrale, di una lista di prodotti,

sistemi e profili di protezione certificati e in corso di certificazione; la predisposizione, la tenuta e l'aggiornamento dell'elenco degli LVS accreditati; la promozione delle attività per la diffusione della cultura della sicurezza nel settore della tecnologia dell'informazione; la formazione, abilitazione e addestramento dei Certificatori, personale dipendente dell'Organismo di Certificazione, nonché dei Valutatori, dipendenti degli LVS e Assistenti, ai fini dello svolgimento delle attività di valutazione; la predisposizione, tenuta e aggiornamento dell'elenco dei Certificatori, Valutatori e Assistenti.

Il decreto-legge n. 105 del 2019 – che definisce il perimetro di sicurezza cibernetica nazionale – ha affidato al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, il compito di effettuare la valutazione di beni, sistemi e servizi ICT destinati a essere impiegati su infrastrutture ICT che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato.

Ai sensi del d.P.C.M. 31 luglio 2020, n. 131, i soggetti pubblici e privati – che offrono tali servizi o funzioni – sono individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici, interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro, dalle amministrazioni competenti nei rispettivi settori.

I soggetti inclusi nel perimetro di sicurezza cibernetica, così individuati, sono tenuti a predisporre annualmente l'elenco degli *asset* ritenuti « strategici » per la fornitura dei servizi essenziali e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali *asset*, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT (*Computer Security Incident Response Team*) attivo presso la Presidenza del Consiglio.

Le misure di sicurezza, che i soggetti inclusi nel predetto perimetro sono tenuti ad adottare e le modalità di notifica degli

incidenti sono state definite con il d.P.C.M. 14 aprile 2021, n. 81.

Inoltre, i soggetti inclusi nel perimetro, ai sensi dell'articolo 1, comma 6, del decreto-legge n. 105 del 2019 sono tenuti a comunicare al CVCN l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri *asset* « strategici » e appartenenti a determinate categorie individuate sulla base di specifici criteri tecnici. Il CVCN, entro un tempo massimo di 60 giorni dalla comunicazione, indica al soggetto incluso nel perimetro eventuali condizioni a cui i fornitori dovranno attenersi e *test* di *hardware* e *software* che dovranno essere eseguiti. Eventuali condizioni e i *test* sono inseriti nei bandi di gara e contratti con clausole che condizionano il contratto al rispetto delle condizioni e all'esito favorevole dei *test* disposti dal CVCN. I *test* possono essere effettuati presso i laboratori del CVCN o presso laboratori di prova accreditati dallo stesso CVCN e devono essere conclusi nel termine di sessanta giorni.

Con il D.P.R. 5 febbraio 2021, n. 54, sono state definite procedure, modalità e termini di funzionamento del CVCN, le procedure per la verifica del rispetto delle disposizioni del decreto-legge n. 105 del 2019, nonché i criteri tecnici per l'individuazione delle categorie di beni, sistemi e servizi ICT (da effettuarsi con d.P.C.M.) che saranno oggetto della valutazione del CVCN nel caso in cui siano destinati agli *asset* « strategici ». Tali categorie sono state individuate con il d.P.C.M. 15 giugno 2021.

Il già citato decreto-legge n. 82 del 2021, che ha ridefinito l'architettura nazionale di cybersicurezza e istituito l'Agenzia per la cybersicurezza nazionale, ha trasferito il CVCN presso l'Agenzia e la sua operatività è assicurata dal 30 giugno 2022.

Ricorda inoltre che il Governo, il 16 maggio 2022, ha approvato la Strategia Nazionale di cybersicurezza 2022-2026, che fissa gli obiettivi e gli strumenti di intervento in materia di sicurezza cibernetica, e prevede, tra l'altro il potenziamento delle capacità del CVCN.

Rileva altresì come, a seguito della crisi in Ucraina, siano state adottate alcune disposizioni di urgenza finalizzate alla diver-

sificazione delle dotazioni informatiche delle pubbliche amministrazioni (decreto-legge n. 21 del 2022, articolo 29). Si prevede che le pubbliche amministrazioni provvedano alla diversificazione dei prodotti informatici in uso, al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici. Si tratta dei rischi legati all'eventualità che le aziende produttrici di tali prodotti informatici, legate alla Federazione Russa, non siano in grado di fornire servizi e aggiornamenti atti a prevenire i rischi medesimi, a seguito della crisi in Ucraina, anche al fine di prevenire possibili pregiudizi per la sicurezza nazionale nello spazio cibernetico.

Inoltre, si demanda a una circolare dell'Agenzia per la cybersicurezza nazionale l'individuazione delle categorie di prodotti destinate alla sicurezza dei dispositivi (antivirus, anti-*malware*, EDR) ovvero alla protezione delle reti (*firewall*). Nella circolare sono indicate, altresì, le principali raccomandazioni procedurali (ferma restando la responsabilità di ciascuna amministrazione) nonché le categorie di prodotti e servizi, ivi incluse le relative aziende produttrici o fornitrici. In attuazione di tale disposizione, l'Agenzia per la cybersicurezza nazionale ha emanato la circolare 21 aprile 2022, n. 4336, relativa alla « Diversificazione di prodotti e servizi tecnologici di sicurezza informatica ».

Per ciò che attiene alla disposizione di delega in forza della quale è stato predisposto lo schema di decreto legislativo in esame, ricorda che il già citato articolo 18 della legge n. 53 del 2021 (legge di delegazione europea 2019-2020) detta i principi e criteri direttivi per l'adeguamento della normativa nazionale alle disposizioni del titolo III, « Quadro di certificazione della cybersicurezza » del regolamento (UE) 2019/881.

In particolare, il comma 1 del citato articolo 18 ha delegato il Governo ad adottare, entro dodici mesi dalla data di entrata in vigore della stessa legge di delegazione, uno o più decreti legislativi per provvedere all'adeguamento della normativa nazionale al suddetto regolamento.

Al riguardo fa presente che l'articolo 1 della citata legge n. 53 del 2021 rinvia alle

procedure di cui all'articolo 31 della legge n. 234 del 2012, relativamente non soltanto al recepimento delle direttive indicate in allegato alla medesima legge n. 53, ma anche all'attuazione degli « altri atti dell'Unione europea di cui agli articoli da 3 a 29 », tra i quali rientra appunto il regolamento 2019/881. Il richiamato articolo 31 della legge n. 234 del 2012 prevede che la legge di delegazione europea indichi le direttive in relazione alle quali sugli schemi dei decreti legislativi di recepimento è acquisito il parere delle competenti Commissioni parlamentari. In tal caso gli schemi dei decreti legislativi sono trasmessi, dopo l'acquisizione degli altri pareri previsti dalla legge, alla Camera dei deputati e al Senato della Repubblica affinché su di essi sia espresso il parere delle competenti Commissioni parlamentari (entro quaranta giorni dalla data di trasmissione dell'atto). Qualora il termine per l'espressione del parere parlamentare scada nei trenta giorni che precedono la scadenza dei termini di delega o successivamente, questi ultimi sono prorogati di tre mesi.

Fa presente che lo schema di decreto in esame è stato assegnato il 7 maggio 2022, e che il termine per l'espressione del parere parlamentare è fissato al 16 giugno 2022 (dunque successivamente al termine per l'adozione dei decreti legislativi, previsto per l'8 maggio 2022): di conseguenza, il termine per l'esercizio della delega è prorogato di tre mesi, dall'8 maggio all'8 agosto 2022.

Il comma 2 del richiamato articolo 18 specifica i seguenti principi e criteri direttivi a cui il Governo si dovrà attenere. In primo luogo, designare il Ministero dello sviluppo economico quale « autorità nazionale di certificazione della cybersicurezza » ai sensi del paragrafo 1 dell'articolo 58 del regolamento (UE) 2019/881; ogni Stato membro dovrà individuare una o più Autorità e comunicarne l'identità alla Commissione europea; le Autorità sono incaricate di compiti di vigilanza e devono essere indipendenti dai soggetti sui quali vigilano in termini di organizzazione, decisioni di finanziamento, struttura giuridica e processo decisionale; tale principio è stato, peraltro,

di fatto superato con l'affidamento all'Agenzia per la cybersicurezza nazionale della funzione di Autorità nazionale di certificazione della cybersicurezza ad opera del già citato articolo 7, comma 1, lettera *e*), del decreto-legge n. 82 del 2021.

In secondo luogo, individuare l'organizzazione e le modalità per lo svolgimento dei compiti e l'esercizio dei poteri della medesima Agenzia per la cybersicurezza nazionale, i quali sono: *a*) supervisionare e far applicare le regole previste nei sistemi europei di certificazione della cybersicurezza per il controllo della conformità dei prodotti, servizi e processi ITC con i requisiti dei certificati europei di cybersicurezza rilasciati; *b*) controllare la conformità agli obblighi e far applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti, servizi o processi ITC che sono stabiliti in Italia e che effettuano un'autovalutazione della conformità; *c*) assistere e sostenere gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione; *d*) autorizzare gli organismi di valutazione della conformità o limitare, sospendere o revocare l'autorizzazione esistente in caso di violazione delle prescrizioni del regolamento; *e*) ricevere i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cybersicurezza rilasciati dalle autorità nazionali di certificazione della cybersicurezza o ai certificati europei di cybersicurezza; *f*) redigere una relazione sintetica annuale; *g*) cooperare con le altre Autorità nazionali di certificazione della cybersicurezza o con altre autorità pubbliche; *h*) sorvegliare gli sviluppi che presentano un interesse nel campo della certificazione della cybersicurezza (articolo 58, paragrafo 7 del regolamento (UE) 2019/881); *i*) rilasciare i certificati europei, qualora lo preveda lo stesso sistema europeo di certificazione della cybersicurezza « in casi debitamente giustificati » (articolo 56, paragrafo 5 del regolamento (UE) 2019/881) o qualora il sistema medesimo richieda un livello di affidabilità elevato (articolo 56, paragrafo 6). Ricorda che ai sensi dell'articolo 58, paragrafo 4, del citato regolamento gli Stati membri

sono tenuti ad assicurare che le Autorità nazionali di certificazione mantengano « rigorosamente separate » le attività di rilascio di certificati europei di cybersicurezza da quelle invece relative alla vigilanza.

Gli altri criteri direttivi previsti dal comma 2 del citato articolo 18 della legge di delegazione europea riguardano, in primo luogo, la definizione del sistema delle sanzioni applicabili, stabilendo in particolare che le sanzioni amministrative pecuniarie devono essere non inferiori nel minimo a 15.000 euro né superiori nel massimo a 5.000.000 di euro; gli introiti derivanti dall'irrogazione delle sanzioni saranno versati all'entrata del bilancio dello Stato per essere riassegnati ad apposito capitolo dello stato di previsione del Ministero dello sviluppo economico per finalità di ricerca e formazione in materia di certificazione della cybersicurezza. In secondo luogo, la previsione che il Ministero dello sviluppo economico (ora l'Autorità nazionale per la cybersicurezza), in quanto autorità nazionale di certificazione della cybersicurezza, possa revocare i certificati rilasciati sul territorio nazionale da organismi di valutazione della conformità o organismi pubblici accreditati come organismi di valutazione della conformità; i certificati oggetto di possibile revoca sono quelli rilasciati ai sensi dell'articolo 56, paragrafi 4 e 5, lettera *b*), del regolamento (UE) 2019/881, ovvero quelli rilasciati da organismi di valutazione della conformità e che corrispondono a un livello di affidabilità « di base » o « sostanziale » ma anche quelli che, « in casi debitamente giustificati », siano rilasciati da un organismo pubblico accreditato come organismo di valutazione della conformità.

Passando a illustrare il contenuto dello schema di decreto legislativo, che si compone di 15 articoli, suddivisi in 5 Capi, il Capo I reca disposizioni di carattere generale (articoli 1-3), il Capo II definisce le procedure di certificazione della cybersicurezza disciplinando diffusamente i compiti e gli obblighi in tale ambito dell'Autorità nazionale per la cybersicurezza, dei fabbricanti o fornitori dei prodotti ICT e degli Organismi di valutazione (articoli 4-10), il

Capo III disciplina le sanzioni, i controlli e i ricorsi giurisdizionali relativi alla violazione delle procedure di certificazione (articoli 9-12), il Capo IV reca disposizioni finanziarie (articoli 13 e 14), mentre il Capo V reca le disposizioni finali (articolo 15).

L'articolo 1, comma 1, definisce l'oggetto e l'ambito di applicazione del decreto, consistente nell'adozione di misure volte ad adeguare la normativa nazionale al nuovo quadro europeo di certificazione della cybersicurezza, introdotto mediante le disposizioni del Titolo III del regolamento (UE) 2019/881. Come evidenziato in premessa, si tratta dell'ambito di intervento determinato dalle disposizioni di delega contenute nell'articolo 18, comma 1, della legge di delegazione europea 2019-2020.

All'interno di tale ambito di intervento, il comma 2 specifica quali sono le finalità principali del decreto legislativo, coerentemente con i criteri direttivi: *a)* individuazione dell'organizzazione dell'autorità nazionale di certificazione della cybersicurezza in Italia in base ai compiti ed ai poteri ad essa attribuiti in materia di vigilanza in ambito nazionale e di rilascio dei certificati di cybersicurezza, con riferimento al quadro europeo di certificazione; *b)* modalità di cooperazione dell'Autorità nazionale di certificazione della cybersicurezza con le altre Autorità pubbliche nazionali ed europee (competenti in materia di vigilanza del mercato) con l'Organismo di accreditamento nazionale designato in Italia; *c)* definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

Ai sensi del comma 3, sono escluse dall'ambito di applicazione del decreto le disposizioni specifiche riguardanti le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale, coerentemente con quanto previsto dall'articolo 1, paragrafo 2, del regolamento, che fa salve le competenze degli Stati membri in questi settori, anche in considerazione del carattere specifico della

politica di sicurezza e di difesa di ciascuno Stato membro (considerando n. 43).

L'articolo 2 dispone che il trattamento dei dati personali derivante dall'applicazione del decreto legislativo sia effettuato, in accordo con il regolamento europeo per la protezione dei dati personali (regolamento (UE) 2016/679, *General Data Protection Regulation* – GDPR) e con il vigente Codice per la protezione dei dati personali (di cui al decreto legislativo n. 196 del 2003).

Ricorda che, ai sensi dell'articolo 41 del regolamento (UE) 2019/881, il trattamento dei dati personali da parte dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA) è soggetto al regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati e resta conseguentemente fuori dall'ambito di applicazione del GDPR (ai sensi dell'articolo 2, paragrafo 3, dello stesso GDPR).

L'articolo 3, in aggiunta alle definizioni contenute nel regolamento (UE) 2019/881, introduce e adegua una serie di definizioni valide ai fini del decreto legislativo.

Richiama di seguito alcune definizioni parzialmente innovative rispetto a quelle di cui all'articolo 2 del regolamento (UE) 2019/881. La lettera *p)* reca la definizione di « 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. La lettera *q)* introduce la definizione di « organismo di certificazione » quale organismo di valutazione della conformità che emette certificati europei di cybersicurezza in base alle norme armonizzate europee ed agli *standard* di riferimento; si tratta di organismi che per essere accreditati devono soddisfare i requisiti indicati nell'Allegato del Regolamento: tra gli altri requisiti, si prevede che siano istituiti a norma del diritto interno, che siano dotati di personalità giuridica e siano terzi e indipendenti dall'organizzazione o dai pro-

dotti ITC, servizi ITC o processi ITC che tali organismi sono chiamati a valutare. La lettera z) specifica il significato del termine « certificato europeo di cybersicurezza » quale documento rilasciato da un organismo di certificazione (laddove il regolamento parla genericamente di « organismo pertinente ») che attesta che un determinato prodotto ITC, servizio ITC o processo ITC è stato oggetto di una valutazione di conformità ai requisiti stabiliti da un sistema europeo di certificazione.

Valentina CORNELI (M5S), *relatrice per la I Commissione*, ricollegandosi a quanto già affermato dalla presidente e correlatrice Paita, rileva che l'articolo 4 interviene in merito all'Autorità nazionale di certificazione della cybersicurezza, disciplinando le modalità con cui sono definite l'organizzazione e le procedure per lo svolgimento dei compiti ad essa affidati.

Tale autorità, al comma 1, è individuata nell'Agenzia per la cybersicurezza nazionale, come già previsto dagli articoli 7, comma 1, lettera e), e 16, comma 12, lettera b), del decreto-legge n. 82 del 2021, e nel rispetto di quanto previsto dall'articolo 58, paragrafo 1, del regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (cosiddetto « regolamento sulla cybersicurezza »).

Il comma 2 reca la disciplina delle modalità di definizione dell'organizzazione e dei compiti dell'Autorità. In proposito, è previsto che sia la stessa Agenzia a disciplinare, mediante proprio provvedimento adottato dal Direttore generale, sentito il Vice direttore generale, ai sensi dell'articolo 5, comma 3, del d.P.C.M. n. 223 del 2021 (recante il regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale): l'organizzazione e le procedure per lo svolgimento dei compiti che le competono in veste di Autorità nazionale di certificazione della cybersicurezza; le modalità applicative delle attività svolte, in ambito sia nazionale sia internazionale, dall'Autorità (articoli 4-9), nonché in sede di reclamo sui certificati di cyber-

sicurezza e sulle dichiarazioni UE di conformità (articolo 11); la rigorosa separazione tra le attività dell'Agenzia relative alle sue funzioni di vigilanza (articolo 5) e quelle di rilascio dei certificati europei di cybersicurezza (articolo 6), nonché lo svolgimento indipendente di tali attività, nell'ambito di due distinte Divisioni istituite ai sensi dell'articolo 4, comma 4, del già citato d.P.C.M. n. 223 del 2021.

Il comma 2, ultimo periodo, dispone che l'Agenzia partecipa con proprio personale alle attività internazionali del Gruppo europeo di certificazione della cybersicurezza (ECCG) e del comitato *ad hoc* ai sensi degli articoli 62 e 66 del regolamento (UE) 2019/881.

Il comma 3 reca le autorizzazioni di spesa per gli anni dal 2022, per consentire lo svolgimento dei compiti attribuiti all'Agenzia, in materia di: realizzazione e gestione dei sistemi informativi; formazione del personale tecnico e amministrativo; ricerca e innovazione; realizzazione e aggiornamento di laboratori interni; abilitazione di laboratori di prova ed esperti; autorizzazione di organismi di valutazione della conformità; vigilanza, accreditamento, rinnovo ed estensione dell'organismo di certificazione della sicurezza informatica di cui all'articolo 6, comma 1; missioni nazionali ed internazionali; spese generali.

Nel dettaglio, è autorizzata la spesa di 657.500 euro per il 2022, 592.500 euro per il 2023 e 637.500 euro annui a decorrere dal 2024. A tali oneri si provvede mediante corrispondente riduzione del Fondo per il recepimento della normativa europea (di cui all'articolo 41-*bis* della legge n. 234 del 2012), come disposto dall'articolo 14, comma 1 dello schema di decreto.

L'articolo 5 elenca e disciplina le attività di vigilanza svolte in ambito nazionale dall'Agenzia.

Ai sensi del comma 1, l'Agenzia vigila sul mercato nazionale per garantire la 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) 2019/881. Per svolgere l'attività di vigilanza del mercato in ambito nazionale, l'Agenzia vigila, altresì, sui fornitori e fabbricanti che emettono 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.

Il comma 1, ultimo periodo, introduce poi tre ulteriori attività che l'Agenzia svolge, ai sensi, rispettivamente, dell'articolo 58, paragrafo 7, lettere *c*), *d*) ed *e*), del citato regolamento, il cui contenuto viene sostanzialmente riprodotto: *a*) assistenza e sostegno attivo all'organismo di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità; tale competenza è esercitata fatto salvo quanto stabilito alla lettera *b*), nonché all'articolo 60, paragrafo 3, del regolamento, qualora i sistemi europei di certificazione della cybersicurezza stabiliscano requisiti specifici o supplementari; solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'Autorità nazionale di certificazione della cybersicurezza a svolgere i compiti previsti da tali sistemi; *b*) monitoraggio e vigilanza sulle attività degli organismi pubblici di valutazione della conformità di cui all'articolo 56, paragrafo 5, lettera *b*), del regolamento; tale disposizione fa riferimento alla procedura di rilascio dei certificati europei di cybersicurezza, stabilendo che, in casi debitamente giustificati, un sistema europeo di certificazione della cybersicurezza può prevedere che essi possano essere rilasciati unicamente da un ente pubblico, da individuarsi in un'Autorità nazionale di certificazione della cybersicurezza oppure in un organismo pubblico accreditato come organismo di valutazione della conformità; *c*) nel caso in cui un sistema di certificazione preveda che gli organismi di valutazione della conformità devono possedere requisiti specifici o supplementari, volti a garantirne la competenza tecnica nella valutazione dei requisiti di cybersicurezza (articolo 54, paragrafo 1, lettera *f*) del regolamento), autorizzazione dei soli organismi di valutazione

della conformità che – a norma dell'articolo 60, paragrafo 3, del Regolamento – soddisfano detti requisiti, nonché limitazione, sospensione o revoca dell'autorizzazione già esistente, qualora sussistano violazioni del regolamento, dando di ciò notizia all'organismo di accreditamento.

Il comma 2 prevede che, nello svolgimento dell'attività di vigilanza di cui al comma 1, l'Agenzia può anche collaborare con le 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*) e *h*) del regolamento, nonché con le Forze dell'ordine.

Sempre nello svolgimento dell'attività di vigilanza ai sensi del comma 1, all'Agenzia è consentito, ai sensi del comma 3: di effettuare indagini nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cybersicurezza e degli emittenti le dichiarazioni di conformità UE; di ottenere informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di cybersicurezza; di revocare certificati ai sensi del comma 4; di irrogare sanzioni pecuniarie ed accessorie ai sensi dell'articolo 10; di prelevare prodotti.

A tal fine, è espressamente sancito l'obbligo, per gli organismi di valutazione della conformità, per i titolari dei certificati europei di cybersicurezza e per gli emittenti delle dichiarazioni di conformità, di cooperare con l'Agenzia quando sono sottoposti ad attività di verifica sui certificati e sulle dichiarazioni UE emessi. Su richiesta dell'Agenzia, essi mettono a disposizione tutti i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica, assieme agli strumenti di valutazione eventualmente forniti dal fabbricante o dal fornitore. Resta fermo che 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.

I commi da 4 a 6 disciplinano specificamente le ipotesi e la procedura di revoca dei certificati di cui l’Agenzia, all’esito dell’attività di vigilanza, accerti la non conformità alle disposizioni del regolamento.

Innanzitutto, il comma 4 individua tali certificati in quelli emessi ai sensi dell’articolo 56 del regolamento, paragrafi 4, 5, lettera *b*), e 6, lettere *a*) e *b*). Il procedimento di revoca si articola diversamente a seconda della natura del certificato in questione: se si tratta di un certificato rilasciato per il livello di affidabilità elevato, la revoca è disposta in ogni caso e l’Agenzia vi provvede direttamente; per il livello di affidabilità di base o sostanziale, invece, la revoca è disposta solo nel caso in cui il certificato non conforme sia relativo a un prodotto ICT, servizio ICT o processo ICT che ha comportato un concreto e dimostrato pregiudizio: a un servizio essenziale ai sensi dell’allegato II del decreto legislativo n. 65 del 2018 (il riferimento è al settore dell’energia, ai trasporti, al settore bancario, alle infrastrutture dei mercati finanziari, al settore sanitario, alla fornitura e distribuzione di acqua potabile ed alle infrastrutture digitali); a un servizio di comunicazione elettronica come definito ai sensi dell’articolo 2, comma 1, lettera *fff*), del decreto legislativo n. 259 del 2003 (Codice delle comunicazioni elettroniche), e cioè i servizi, forniti di norma a pagamento su reti di comunicazioni elettroniche, di accesso a internet, di comunicazione interpersonale e di trasmissione di segnali come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva; alla salute o all’incolumità personale: in tal caso, il comma 5 prevede un’interlocuzione tra l’Agenzia e l’organismo che ha emesso il certificato. In prima battuta, infatti, è l’Agenzia a chiedere all’organismo emittente di provvedere alla revoca del certificato entro e non oltre 5 giorni; in caso di inottemperanza, l’Agenzia provvede direttamente alla revoca entro i successivi 5 giorni; il potere di revoca sussiste, infine e in generale, se previsto espressamente dallo specifico sistema europeo di certificazione. Conseguentemente, si segui-

ranno le regole appositamente stabilite dal sistema.

Una volta accertata l’emissione di un certificato non conforme, all’Agenzia è, tuttavia, consentito attivare una specifica procedura volta alla sanatoria del certificato stesso. Infatti, il comma 6 stabilisce che, fatti salvi i casi di revoca appena elencati, l’Agenzia chiede 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 in base alle modalità stabilite nel sistema europeo di certificazione della cybersicurezza (ai sensi dell’articolo 54, paragrafo 1, lettera *s*), del regolamento) ed è specificato che le modalità di sostegno ed assistenza dell’Agenzia all’Organismo di accreditamento per l’attività di vigilanza nazionale sono disciplinate da apposita convenzione o protocollo di intesa fra i medesimi soggetti.

Per l’effettuazione delle prove tecniche necessarie nell’ambito delle attività di vigilanza di cui al comma 1, il comma 7 prevede, altresì, la possibilità per l’Agenzia di 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.

Il comma 9 reca la copertura finanziaria, disponendo che agli 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 – provvede l’organismo di valutazione della conformità, il titolare del certificato o l’emittente della dichiarazione UE di conformità sottoposto all’attività di vigilanza.

Anche le eventuali ulteriori spese legate all’attività di vigilanza, tra cui le spese per l’utilizzo di laboratori di prova esterni e per il trasporto di prodotti prelevati o sequestrati da sottoporre a verifica, sono a carico del soggetto sottoposto all’attività di vigilanza. Tutte le somme dovute dal soggetto controllato sono determinate e sono da corrispondere ai sensi dell’articolo 13.

L’articolo 6 reca la disciplina per il rilascio dei certificati di cybersicurezza.

Con riferimento ai certificati di cybersicurezza con livello di affidabilità elevato, il comma 1 stabilisce che l’Agenzia provvede al relativo rilascio tramite l’Organismo di Certificazione della Sicurezza Informatica (OCSI). A tal fine, l’OCSI può avvalersi di esperti o di 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. Restano ferme, per specifici sistemi di certificazione, le possibili modalità di emissione dei certificati alternative ai sensi dell’articolo 56, paragrafo 6, lettere *a*) e *b*), del regolamento, vale a dire ad opera di un organismo di valutazione della conformità che agisca sulla base di una delega generale al rilascio dei certificati oppure previa approvazione dell’Autorità nazionale di certificazione per ogni certificato rilasciato. Anche nel caso di certificati con livello di affidabilità sostanziale o di base, ove uno specifico sistema di certificazione ne preveda il rilascio unicamente da parte di un organismo pubblico (ai sensi dell’articolo 56, paragrafo 5, del regolamento), l’Agenzia provvede attraverso l’OCSI.

Il comma 2 consente, comunque – salvo che lo specifico sistema europeo di certificazione disponga diversamente – il rilascio ad opera di altro organismo di valutazione della conformità pubblico, che sia: accreditato dall’organismo di accreditamento; mo-

nitorato e vigilato dall’Agenzia; designato dall’Agenzia ai sensi del provvedimento di cui all’articolo 4, comma 2.

Il comma 3 – riportando fedelmente il contenuto dell’articolo 56, comma 2, del regolamento – stabilisce che la certificazione della cybersicurezza è volontaria, salvo che sia diversamente specificato dal diritto dell’Unione o dal diritto nazionale. Inoltre, nel caso in cui il diritto dell’Unione non sia armonizzato, autorizza l’Agenzia ad 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 n. 223 del 2017 (che disciplina la procedura d’informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell’informazione).

Il comma 4, facendo anch’esso riferimento all’articolo 30, commi 4 e 5, della legge n. 234 del 2012 e precisando che le somme sono determinate e da corrispondere ai sensi dell’articolo 13, pone gli oneri derivanti dall’applicazione dei commi 1 e 2 per il rilascio dei certificati da parte dell’Agenzia a carico del soggetto richiedente la certificazione.

L’articolo 7 definisce e disciplina le dichiarazioni UE di conformità. Esse trovano applicazione all’interno di un sistema europeo di certificazione della cybersicurezza che abbia autorizzato l’autovalutazione di conformità (articolo 54, paragrafo 1, lettera *e*), del regolamento) e consentono ai fornitori o fabbricanti di prodotti ICT, servizi ICT o processi ICT di 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 si prevede che il fabbricante o fornitore di prodotti ICT, servizi ICT o processi ICT è tenuto a rendere disponibile all’Agenzia, per il periodo stabilito nel sistema europeo di certificazione della cybersicurezza (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 ICT o servizi ITC al sistema. Una copia della dichiarazione UE di conformità è trasmessa, altresì, all'Agenzia e all'ENISA. Nel caso in cui l'Agenzia, all'esito dello svolgimento dell'attività di vigilanza di cui all'articolo 5, comma 1, accerti la non conformità di una di tali dichiarazioni, il fabbricante o il fornitore che l'ha prodotta deve revisionarla o revocarla entro trenta giorni, dandone comunicazione all'Agenzia e all'ENISA. Sono comunque fatte salve le diverse disposizioni dello specifico sistema di certificazione.

L'articolo 8 regola la procedura di accreditamento e autorizzazione degli organismi di valutazione della conformità, nonché di abilitazione dei laboratori di prova e degli esperti dell'Agenzia.

Il comma 1 impegna l'organismo di accreditamento a comunicare all'Agenzia e all'ufficio unico di collegamento designato per l'Italia (ai sensi dell'articolo 10, paragrafo 3, del regolamento (UE) 2019/1020, sulla vigilanza del mercato e sulla conformità dei prodotti) ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento. L'organismo di accreditamento vi provvede nello svolgimento dei propri compiti in materia di accreditamento degli organismi di valutazione della conformità (ai sensi dell'articolo 60, paragrafi 1, 2 e 4, del regolamento) e in conformità con quanto previsto dallo specifico sistema di certificazione. Tale adempimento è finalizzato alla successiva notifica, da parte dell'Agenzia, alla Commissione europea, ai sensi dell'articolo 61 del Regolamento.

Ai sensi del comma 2, l'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'organismo di accreditamento relative alle attività di cui al comma 1, con la precisazione, contenuta al comma 3, che, qualora un sistema europeo di certificazione stabilisca requisiti specifici o supplementari, solo gli organismi di valutazione della conformità che li soddisfano sono autorizzati dall'Agenzia a svolgere i compiti previsti da tale sistema.

Il comma 4 disciplina la procedura di abilitazione dei laboratori di prova e degli esperti dell'Agenzia.

Nel dettaglio, si prevede che, in relazione alle attività di vigilanza nazionale e di rilascio dei certificati, l'Agenzia, con provvedimento adottato dal Direttore generale, sentito il Vice direttore generale, costituisce, aggiorna e rende pubblici due elenchi di esperti e di laboratori di prova da essa abilitati a operare – rispettivamente, ai sensi dell'articolo 5, comma 7, e ai sensi dell'articolo 6, comma 1 – a supporto della propria attività di vigilanza e rilascio dei certificati.

Allo stesso modo, 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. Gli esperti e i laboratori di prova così abilitati non possono comunque effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità sostanziale o di base in ambito nazionale, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati.

Anche in questo caso, 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 posti a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione.

Allo scopo di elevare il livello nazionale di cybersicurezza, l'articolo 9 consente all'Agenzia di 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 e internazionale.

L'Agenzia monitora, altresì, 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. Nel caso in cui manchi un sistema europeo di certificazione, l'Agenzia può introdurre sistemi di certificazione nazionali della cybersicurezza per prodotti ICT, servizi ICT o processi ICT, conformemente all'articolo 57 del regolamento.

L'articolo 10 prevede le disposizioni sulle sanzioni, i reclami e i ricorsi giurisdizionali.

Il comma 1 stabilisce che l'Agenzia, in caso di violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, irroga sanzioni pecuniarie e accessorie, chiedendo la cessazione immediata della violazione. Si applica, in quanto compatibile, la disciplina di cui alla legge n. 689 del 1981. Tale potere è esercitato ai sensi dell'articolo 7, comma 1, lettera *e*), del decreto-legge n. 82 del 2021 (con cui, come già detto, sono state trasferite all'Agenzia tutte le funzioni, anche sanzionatorie, prima spettanti al MiSE), nonché dell'articolo 58, paragrafo 8, lettera *f*), e dell'articolo 65 del regolamento.

Ai sensi del comma 2, salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che emette un certificato di cybersicurezza non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. 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.

In base al comma 3, salvo che il fatto costituisca reato, il fabbricante o fornitore che emette una dichiarazione UE di conformità volontaria non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. 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.

In base ai commi 4 e 5, 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 del-

l'articolo 6, comma 3, il fabbricante o fornitore che mette a disposizione sul mercato un prodotto ICT o servizio ICT 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.

Alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto ICT o di un servizio ICT si avvale di un processo ICT privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza di certificato di cybersicurezza obbligatorio.

In tali casi, oppure ove, in esito a 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 ICT o di un servizio ICT, 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.

In base al comma 6, salvo che il fatto costituisca reato, il fabbricante che non ottempera a quanto prescritto al comma 5 per il richiamo di prodotti già immessi sul mercato è assoggettato alla sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. 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.

Salvo che il fatto costituisca reato, il comma 7 prevede che il fornitore che non ottempera a quanto prescritto al comma 5 per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro.

Salvo che il fatto costituisca reato, il comma 8 prevede che il titolare di un certificato europeo di cybersicurezza che non notifichi, ai sensi dell'articolo 56, pa-

ragrafo 8, del regolamento, eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza dei prodotti ICT, servizi ICT o processi ICT 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 o 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 ICT, servizio ICT o processo ICT certificato o dichiarato conforme, che non siano state riscontrate durante il processo di valutazione, e non ottemperi 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.

Ai sensi del comma 9, 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 pubblici 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.

In base al comma 10, salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottempera

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, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità autorizzato dall'Agenzia ai sensi dell'articolo 60, paragrafo 3, del regolamento, che non specifici nella procedura per i reclami definita ai sensi dell'articolo 11, comma 2, l'inoltro degli stessi per conoscenza anche all'Agenzia.

Secondo il comma 11, 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 applica 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 e il soggetto può richiedere il rilascio di nuova autorizzazione.

Ai sensi del comma 12, 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, fornisca 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. Alla medesima sanzione è assoggettato il soggetto che, scientemente, durante le verifiche di vigilanza a cui è sottoposto, ai sensi dell'articolo 5, comma 5, fornisca dati, informazioni o documentazione falsi.

Salvo che il fatto costituisca reato, il comma 13 prevede che il fabbricante che viola le condizioni di utilizzo degli even-

tuali marchi o etichette previste da un sistema europeo di certificazione, ai sensi dell'articolo 54, paragrafo 1, lettera *i*), del regolamento, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro.

In base al comma 14, salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che non ottempera agli eventuali obblighi riguardanti la conservazione dei registri di cui all'articolo 54, paragrafo 1, lettera *n*), del Regolamento, è assoggettato alla sanzione del pagamento di una somma da 45.000 euro a 225.000 euro.

Il comma 15 prevede che l'Agenzia può impartire ordini o intimare diffide ai soggetti che operano in contrasto al quadro europeo di certificazione. Ai soggetti che non ottemperano nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 euro a 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.

Ai sensi del comma 16, è stabilito 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, sono triplicati, se la violazione ha riguardato un certificato relativo a un prodotto ITC, un servizio ITC o un processo ITC 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 n. 65 del 2018, o di un servizio di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera *fff*), del de-

creto legislativo n. 259 del 2003. Quanto ai criteri di graduazione nell'irrogazione delle sanzioni pecuniarie, essi sono definiti con successivo provvedimento dell'Agenzia, adottato dal Direttore generale, sentito il Vice direttore generale (secondo la procedura, già vista, di cui all'articolo 5, comma 3, alinea, del d.P.C.M. n. 223 del 2021).

Nelle more dell'adozione di tale provvedimento, ai sensi del comma 17 si applicano i criteri di cui all'articolo 11 della legge n. 689 del 1981.

È altresì stabilito, al comma 18, 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 sono rivalutate ogni cinque anni con provvedimento dell'Agenzia, adottato come sopra, 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. L'importo della sanzione pecuniaria rivalutato secondo i predetti criteri si applica esclusivamente per le violazioni commesse successivamente alla data di entrata in vigore del provvedimento che lo prevede.

Ai sensi del comma 19, nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio, 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, è sospesa per 6 mesi o revocata. In caso di revoca, 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 provveda poi a dare notifica delle eventuali modifiche entro sessanta giorni successivi alle stesse.

L'articolo 11 disciplina la procedura dei reclami sui certificati di cybersicurezza e

sulle dichiarazioni UE di conformità. Le autorità competenti a ricevere i reclami proposti dalle persone fisiche e giuridiche sono, ai sensi del comma 1: l'emittente di un certificato europeo di cybersicurezza, o l'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.

L'Agenzia, inoltre, tratta i reclami proposti in relazione alle dichiarazioni UE di conformità di cui all'articolo 7.

L'articolo 12 disciplina la presentazione dei ricorsi giurisdizionali in materia di certificati europei di cybersicurezza e dichiarazioni UE di conformità, dando attuazione all'articolo 64 del regolamento, il quale prevede il diritto a un ricorso giurisdizionale effettivo.

In particolare, il comma 1 prevede che le persone fisiche e giuridiche hanno diritto di presentare ricorso giurisdizionale – « fatti salvi eventuali ricorsi amministrativi o altri ricorsi extragiudiziali » – avverso: le decisioni assunte dall'Agenzia per la cybersicurezza nazionale – ACN (in qualità di autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58, paragrafo 1, del regolamento) ovvero dagli organismi di valutazione della conformità (laboratori di prova o organismi di certificazione) in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cybersicurezza detenuto da tali persone fisiche e giuridiche; il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformità ai sensi dell'articolo 11 dello schema di decreto.

Il comma 2 stabilisce che i ricorsi contro le decisioni assunte dall'Agenzia sono presentati dinanzi al TAR Lazio, mentre i ricorsi avverso le decisioni degli altri organismi di valutazione della conformità dinanzi al TAR del luogo ove è ubicata la sede di tali organismi. Con riguardo alle decisioni o al mancato o parziale accoglimento di un reclamo da parte dell'Agenzia, ricorda che ai sensi dell'articolo 135, lettera *h-bis*) del codice del procedimento

amministrativo, introdotta dal decreto-legge n. 82 del 2021 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), risultano già devolute « salvo ulteriori previsioni di legge » alla competenza funzionale inderogabile del TAR Lazio, sede di Roma, le « controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale ».

Con riguardo alla previsione che stabilisce la presentazione al TAR del luogo ove è ubicata la sede degli altri organismi di valutazione della conformità dei ricorsi contro le decisioni di tali organismi, la disposizione sembrerebbe stabilire un criterio di competenza territoriale per quanto concerne la giurisdizione in materia del giudice amministrativo.

L'articolo 13 disciplina le modalità di assegnazione e gestione degli introiti derivanti dalle attività di vigilanza e di certificazione dell'Agenzia, nonché dalle sanzioni.

Il comma 1 stabilisce che le attività di vigilanza nazionale (articolo 5, comma 1), di certificazione (articolo 6, comma 1), di autorizzazione (articolo 8, comma 3), di abilitazione dei laboratori di prova (articolo 8, comma 4) sono sottoposte a tariffa, che viene calcolata sulla base dei costi effettivi dei servizi resi.

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.

Il 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, sono calcolate ai sensi del comma 1.

Il comma 3 stabilisce che gli introiti derivanti dall'irrogazione delle sanzioni di cui all'articolo 10, versati in apposito capitolo dell'entrata del bilancio statale, sono riassegnati sul capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze e destinati ad alimentare le attività di ricerca e formazione

concernenti la certificazione della cybersicurezza. La disposizione attua lo specifico criterio di delega di cui alla lettera *c*) del comma 2 dell'articolo 18 della legge n. 53 del 2021.

L'articolo 14 specifica le modalità di copertura delle spese di funzionamento dell'Agenzia per le nuove attività discendenti dal regolamento europeo, posto che, come chiarito nella relazione tecnica al provvedimento, gli introiti previsti dall'articolo 13 non sono sufficienti a garantire l'operatività dell'Agenzia.

In particolare, il comma 1 dispone che agli oneri per le attività che l'Agenzia 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 provvederà facendo ricorso al Fondo per il recepimento della normativa europea (di cui all'articolo 41-*bis* della legge n. 234 del 2012).

Il comma 2 dispone che le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi (articolo 4, comma 3) debbano essere 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 decreto legislativo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e che l'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente, fatto salvo il ricorso al fondo 41-*bis* di cui al comma 1 per la copertura dei costi di cui all'articolo 4, comma 3.

Il comma 4 autorizza il Ministro dell'economia e delle finanze ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati in attuazione delle disposizioni finanziarie qui riassunte.

L'articolo 15 stabilisce una clausola di adeguamento del quadro nazionale di certificazione della sicurezza informatica definito dal decreto – e dal provvedimento di cui all'articolo 4, comma 2, per le parti di maggior dettaglio – nel caso in cui un nuovo sistema europeo di certificazione adottato dalla Commissione europea non risulti direttamente applicabile nel quadro vigente. In tal caso si prevede, infatti, che l'Agenzia ne possa dare attuazione semplicemente integrando o modificando il provvedimento di cui al comma 2 dell'articolo 4. Ricorda che il provvedimento di cui si prefigura un eventuale aggiornamento, previsto ai sensi dell'articolo 4, comma 2, dello schema di decreto, individua 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 previste dal decreto.

Per quel che concerne il rispetto delle competenze legislative costituzionalmente definite, rileva come il provvedimento sia riconducibile in via prevalente alla materia « sicurezza dello Stato », attribuita alla competenza legislativa esclusiva statale dall'articolo 117, secondo comma, lettera *d*), della Costituzione.

Raffaella PAITA, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

**La seduta termina alle 14.25.**