Certificazione di sicurezza dei prodotti ICT in attuazione del regolamento UE sulla cibersicurezza
Atto del Governo 388

Informazioni sugli atti di riferimento

Atto del Governo:	388	
Titolo:	Schema di decreto legislativo recante norme di adeguamento della normativa nazionale alle disposizioni del titolo III "Quadro di certificazione della cibersicurezza" del regolamento (UE) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza")	
Norma di delega:	Articoli 1 e 18 della legge 22 aprile 2021, n. 53	
Numero di articoli:		
	Senato	**Camera**
Date:		
presentazione:	6 maggio 2022	6 maggio 2022
annuncio:	11 maggio 2022	9 maggio 2022
assegnazione:	7 maggio 2022	7 maggio 2022
termine per l'espressione del parere:	16 giugno 2022	16 giugno 2022
Commissioni competenti :	1^ Affari Costituzionali e 5^ Bilancio	I Affari Costituzionali e IX Trasporti riunite e V bilancio
Rilievi di altre commissioni:	2^ Giustizia, 8^ Lavori pubblici, comunicazioni e 14^ Politiche Unione europea	XIV Politiche dell'Unione europea (Assegnato il 7 maggio 2022 ai sensi ex art.126,co.2 - Termine il 16 giugno 2022)

Premessa

Lo schema di decreto legislativo in esame (A.G. 388) attua la delega prevista dall'articolo 18 della **legge di delegazione europea 2019-2020** (legge 22 aprile 2021, n. 53) volta all'adeguamento della normativa nazionale alle disposizioni del **regolamento (UE) n. 2019/881** del 17 aprile 2019, relativo all'Agenzia dell'Unione europea per la cibersicurezza (European Union Agency for Network and Information Security — ENISA) e al quadro europeo della certificazione.

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

Si ricorda che i **regolamenti dell'Unione europea** sono atti giuridici definiti nell'articolo 288 del trattato sul funzionamento dell'Unione europea (TFUE). Sono di applicazione generale, vincolanti in tutti i loro elementi e **direttamente applicabili** in tutti i Paesi membri, senza dovere essere trasposti in una legge nazionale. Tuttavia, in alcuni casi - come in quello in esame - è lo stesso regolamento che rinvia alla adozione di norme nazionali per la sua piena applicabilità.

In particolare, al fine di dare attuazione al regolamento sulla cibersicurezza - 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.**

Il regolamento sulla cibersicurezza (UE) n. 2019/881

Il regolamento UE sulla cibersicurezza (UE) 2019/881 (di seguito, il Regolamento) ha l'obiettivo di rafforzare la cibersicurezza dell'Unione e introduce:

- una nuova disciplina dell'Agenzia UE per la cibersicurezza;
- 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 cibersicurezza, centro di competenze in materia di sicurezza informatica che ha sede ad Atene. 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** da parte del provvedimento in esame, istituisce il **quadro europeo di certificazione della cibersicurezza**, ovvero un meccanismo volto a istituire un sistema europeo comune di **certificazione della cibersicurezza** 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 cibersicurezza, specificando che i prodotti, servizi e processi TIC 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. I certificati sono rilasciati da organismi di valutazione della conformità (articolo 56, par. 4), operanti al livello nazionale (articolo 60).

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

Gli Stati membri sono incaricati di **designare autorità nazionali di certificazione** (articolo 58).

Al livello europeo, invece, opera il Gruppo europeo per la certificazione della cibersicurezza (articolo 62), composto da rappresentanti delle autorità nazionali.

Il Titolo IV (articoli 66-69) contiene alcune disposizioni finali.

Il Regolamento, e segnatamente l'articolo 69, paragrafo 2, prevede per la sua completa applicazione, l'adozione da parte di ciascun Paese membro di adempimenti per l'attuazione nazionale degli articoli 58, 60, 61, 63, 64 e 65 del medesimo regolamento **entro due anni** dalla sua entrata in vigore (entro cioè il 28 giugno 2021).

Tra l'altro, si prevede:

- l'istituzione di una **autorità nazionale di certificazione della cibersicurezza** (art. 58, par. 1), 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** (art 65) per permettere alle autorità nazionali di far rispettare il regolamento europeo ed i successivi sistemi di certificazione adottati nell'Unione Europea.

Per quanto riguarda la prima previsione, si segnala che l'**Agenzia per la cibersicurezza nazionale** (**ACN**) ha assunto già la funzione di autorità nazionale di certificazione della cibersicurezza in virtù di quanto disposto dal decreto-legge 14 giugno 2021, n. 82 (art. 7, comma 1, lett. *e*).

Come riferisce la relazione illustrativa del provvedimento istitutivo dell'ACN, i primi effetti concreti sull'ordinamento dei singoli Stati membri avverranno soltanto attraverso la **successiva adozione di sistemi europei di certificazione** della cibersicurezza elaborati per **specifici ambiti** (quali certificazioni in base allo standard *Common Criteria*, servizi *cloud*, reti 5G) con atti di esecuzione della Commissione Europea (art. 49, par. 7). Con la pubblicazione del piano di sviluppo della Commissione Europea (art. 47) si prevede l'adozione sistemi di certificazione specifici anche per i dispositivi IoT (*Internet of Things*), e per gli IACS (*Industrial automation and control systems*).

Per ogni ulteriore approfondimento sul quadro generale della politica UE in materia di Cibersicurezza si rimanda a: Consiglio europeo, Cibersicurezza: la risposta dell'UE alle minacce informatiche; sulla normativa in materia certificazione si rimanda a: Commissione europea, The EU cybersecurity certification framework.

La disposizione di delega (art. 18, L. 53/2021)

L'**articolo 18** della legge n. 53 del 2021 (legge di delegazione europea 2019-2020) detta i princìpi e criteri direttivi per l'adeguamento della normativa nazionale alle disposizioni del titolo III, Quadro di certificazione della cibersicurezza, del Regolamento (UE) 2019/881.

In particolare, il **comma 1** ha delegato il Governo ad adottare, **entro dodici mesi dalla data di entrata in vigore** della stessa legge di delegazione n. 53 del 2021 (8 maggio 2021), uno o più decreti legislativi per provvedere all'adeguamento della normativa nazionale al suddetto Regolamento.
Il rinvio alle procedure di cui all'articolo 31 della legge n. 234 del 2012, che comprendono anche il meccanismo di **scorrimento automatico**, è contenuto nell'articolo 1 della legge n. 53 del 2021 che, a differenza delle precedenti leggi di delegazione europea (si veda ad esempio l'articolo 1 della legge n. 117 del 2019), fa **riferimento non soltanto al recepimento delle direttive** indicate in allegato, **ma anche** a**ll'attuazione degli "altri atti dell'Unione europea** di cui agli articoli da 3 a 29", tra i quali rientra appunto il Regolamento, previsto dall'articolo 18.
Il richiamato articolo **31** della legge **234/2012** 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**. Il presente schema è stato assegnato il 7 maggio 2022, con **termine per l'espressione del parere 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**.

Nel dettaglio, l'articolo 1 della legge n. 53 del 2021, rubricato Delega al Governo per il recepimento delle direttive e l'attuazione degli altri atti dell'Unione europea, al comma 1 delega il Governo ad adottare, secondo i termini, le procedure, i princìpi e i criteri direttivi di cui agli articoli 31 e 32 della legge 24 dicembre 2012, n. 234, nonché secondo quelli specifici dettati dalla stessa legge di delegazione europea **e tenendo conto delle eccezionali conseguenze** economiche e sociali derivanti dalla pandemia di **COVID-19**, i decreti legislativi per il recepimento delle direttive europee e l'attuazione degli altri atti dell'Unione europea di cui agli articoli da 3 a 29 e all'allegato A.
Al comma 2 dispone che gli schemi dei decreti legislativi (relativi sia al recepimento delle direttive che all'attuazione degli altri atti UE) siano **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** dei competenti organi parlamentari.

Il **comma 2** indica i seguenti **princìpi e criteri direttivi specifici** a cui il Governo si dovrà attenere:

- designare il Ministero dello sviluppo economico quale «**autorità nazionale di certificazione della cibersicurezza**» 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 di fatto superato con l'affidamento all'**Agenzia per la cibersicurezza nazionale** della funzione di autorità nazionale di certificazione della cibersicurezza ad opera del decreto-legge 14 giugno 2021, n. 82 (art. 7, comma 1, lett. *e)*;
- individuare l'organizzazione e le modalità per lo svolgimento dei compiti e l'esercizio dei poteri della medesima autorità competente, ovvero:

  - **supervisionare e far applicare le regole** previste nei sistemi europei di certificazione della cibersicurezza per il controllo della conformità dei prodotti, servizi e processi TIC con i requisiti dei certificati europei di cibersicurezza rilasciati; controllare la conformità agli obblighi e far applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti, servizi o processi TIC che sono stabiliti in Italia e che effettuano un'autovalutazione della conformità; assistere e sostenere gli organismi nazionali di accreditamento nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione; autorizzare gli organismi di valutazione della conformità o limitare, sospendere o revocare l'autorizzazione esistente in caso di violazione delle prescrizioni del regolamento; trattare i reclami delle persone fisiche o giuridiche in relazione ai certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o ai certificati europei di cibersicurezza; redigere una relazione sintetica annuale; cooperare con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche; sorvegliare gli sviluppi che presentano un interesse nel campo della certificazione della cibersicurezza (articolo 58, par. 7, regolamento (UE) 2019/881);

- il **rilascio dei certificati europei** da parte della stessa autorità nazionale di certificazione della cibersicurezza, di un organismo pubblico accreditato o di un organismo di valutazione della conformità. Ciò avviene qualora lo preveda lo stesso sistema europeo di certificazione della cibersicurezza "in casi debitamente giustificati" (articolo 56, par. 5, regolamento (UE) 2019/881) o qualora il sistema medesimo richieda un livello di affidabilità elevato (articolo 56, par. 6). Si ricorda che ai sensi dell'articolo 58, par. 4, gli Stati membri sono tenuti ad assicurare che le autorità nazionali di certificazione mantengano "rigorosamente separate" le attività di rilascio di certificati europei di cibersicurezza da quelle invece relative alla vigilanza;

- definire il 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 cibersicurezza. Il presente criterio direttivo attua la norma di cui all'articolo 65 del regolamento (UE) 2019/881, la quale incarica gli Stati membri di stabilire sanzioni "effettive, proporzionate e dissuasive", che dovranno essere notificate alla Commissione europea.
- prevedere che il Ministero dello sviluppo economico (ora l'Autorità nazionale per la cibersicurezza) in quanto autorità nazionale di certificazione della cibersicurezza, possa **revocare i certificati** rilasciati sul territorio nazionale da organismi di valutazione della conformità o organismi pubblici accreditati come organismi di valutazione della conformità. Tale potere di revoca è previsto dall'articolo 58, par. 7 e 8, del regolamento (UE) 2019/881, come descritto in precedenza. 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 ad 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. Tale possibilità di revoca viene meno, per espressa previsione della lettera d) del comma 2 della norma in commento, nel caso in cui i singoli sistemi europei di certificazione contengano disposizioni diverse. La lettera d) cita l'articolo 49 del regolamento (UE) 2019/881, che disciplina l'*iter* di approvazione del sistema europeo di certificazione della cibersicurezza. La proposta di sistema è redatta dall'ENISA, su richiesta della Commissione europea, previa consultazione di tutti i pertinenti portatori di interessi. E' istituito un gruppo di lavoro *ad hoc* e l'ECCG presta assistenza e consulenza specialistica. La proposta elaborata dall'ENISA ad esito del processo sopra descritto può quindi essere adottata dalla Commissione europea nella forma di atti di esecuzione. Ogni sistema europeo di certificazione adottato è soggetto a revisione su base quinquennale.

Contenuto

L'A.G. 388 si compone di **15 articoli** suddivisi in **5 Capi**.

Il **Capo I** reca **disposizioni di carattere generale** (**artt. 1-3**).

Il **Capo II** definisce le procedure di **certificazione della cibersicurezza** disciplinando diffusamente i compiti e gli obblighi in tale ambito dell'Autorità nazionale per la cibersicurezza, dei fabbricanti o fornitori dei prodotti ICT e degli Organismi di valutazione (**artt. 4-10**).

Le **sanzioni, i controlli e i ricorsi giurisdizionali** relativi alla violazione delle procedure di certificazione sono oggetto del **Capo III** (**artt. 9-12**).

Infine, il **Capo IV** reca **disposizioni finanziarie** (**artt. 13 e 14**) e il **Capo V** le disposizioni finali (**art. 15**).

Disposizioni generali (artt. 1-3)

L'**articolo 1, comma 1**, dello schema di decreto legislativo definisce l'oggetto e l'ambito di applicazione dello stesso decreto, consistente nell'adozione di misure volte ad adeguare la normativa nazionale al nuovo quadro europeo di certificazione della cibersicurezza, introdotto mediante le disposizioni del Titolo III del regolamento (UE) 2019/881 (definito come il Regolamento).

Come evidenziato in premessa, si tratta dell'ambito di intervento determinato dalla delega contenuta 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 cibersicurezza 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 cibersicurezza, con riferimento al quadro europeo di certificazione;

b) modalità di cooperazione dell'autorità nazionale di certificazione della cibersicurezza 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**, restano fuori 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 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 d.lgs. n. 196 del 2003).

Si 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 cibersicurezza (European Union Agency for Network and Information Security — 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. Alcune definizioni derivano dal regolamento (CE) 765/2008 riguardante la vigilanza del mercato dell'Unione Europea, altre dal regolamento (UE) n. 1025/2012 sulla normazione europea.

In particolare, si richiamano di seguito alcune definizioni parzialmente innovative rispetto a quelle del regolamento (UE) 2019/881 (art. 2):

- 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)** introduce la definizione di «**organismo di certificazione**» quale organismo di valutazione della conformità che **emette certificati europei di cibersicurezza** 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, siano dotati di personalità giuridica e siano terzi e indipendenti dall'organizzazione o dai prodotti TIC, servizi TIC o processi TIC che tali organismi sono chiamati a valutare.

Entrambe le definizioni di cui alle lettere p) e q) richiamano il termine "organismo di valutazione della conformità", così come definito a sua volta nel regolamento (CE) 765/2008 quale "organismo che svolge attività di valutazione della conformità, fra cui tarature, prove, certificazioni e ispezioni".

Dal confronto tra la definizione UE e quella nazionale si evince come le funzioni di competenza dell'organismo di valutazione della conformità siano state attribuite, in parte, ai laboratori di prova (per le verifiche documentali e/o prove) e, in altra parte, agli organismi di certificazione (per l'emissione certificati europei di cibersicurezza).

- alla **lettera z)** specifica il significato del termine «**certificato europeo di cibersicurezza**» quale documento rilasciato da un **organismo di certificazione** (laddove il Regolamento parla genericamente di "organismo pertinente") 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.

Certificazione (artt. 4-9)

L'**articolo 4** dello schema di decreto legislativo interviene in merito all'**autorità nazionale di certificazione della cibersicurezza,** disciplinando le modalità con cui sono definite l'organizzazione e le procedure per lo svolgimento dei compiti ad essa affidati.

Tale autorità (**comma 1**) è individuata nell'**Agenzia per la cibersicurezza nazionale**, come già previsto dagli articoli 7, comma 1, lettera *e)*, e 16, comma 12, lettera *b)*, del **decreto-legge n. 82 del 2021** (recante disposizioni urgenti in materia di cibersicurezza, definizione dell'architettura nazionale di cibersicurezza e istituzione dell'Agenzia per la cibersicurezza nazionale, ai cui *dossier* e *tema* si rinvia per ogni approfondimento) 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 cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. «regolamento sulla cibersicurezza»), di seguito Regolamento.

L'articolo 7 del **decreto-legge n. 82 del 2021** disciplina le funzioni dell'Agenzia per la cibersicurezza nazionale e, al comma 1, lettera *e*), la individua espressamente quale Autorità nazionale di certificazione della cibersicurezza, ai sensi dell'articolo 58 del Regolamento (UE) 2019/881.

L'articolo 58 della normativa europea prevede, infatti, al paragrafo 1, che ciascuno Stato membro provvede a designare una o più autorità nazionali di certificazione della cibersicurezza site nel suo territorio oppure in altro Stato membro che a ciò consenta, affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.

Conseguentemente, l'articolo 7, comma 1, lettera *e)*, dispone che all'Agenzia sono attribuite le **funzioni in materia di sicurezza cibernetica già esercitate dal MISE** e che, nello svolgimento dei suoi compiti, essa:

a. **accredita** le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, ai sensi dell'articolo 60, paragrafo 1, del Regolamento (UE) 2019/881 (a mente del quale, gli organismi di valutazione della conformità sono accreditati da organismi nazionali di accreditamento, previa verifica del rispetto dei requisiti indicati nell'allegato al regolamento stesso);
b. **delega** i predetti Ministeri, attraverso tali strutture accreditate, al rilascio del **certificato europeo di sicurezza cibernetica**, ai sensi dell'articolo 56, paragrafo 6, lett. *b)*, il quale dispone che, ove un sistema europeo di certificazione della cibersicurezza richieda un livello di affidabilità «elevato», il certificato europeo di cibersicurezza nell'ambito di tale sistema è rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza oppure da un organismo di valutazione della conformità - in tal caso, sulla base di una delega generale rilasciata a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

L'articolo 16 del decreto-legge n. 82 del 2021, richiamato anch'esso dall'art. 4 dello schema di decreto legislativo in esame, ha apportato delle modifiche alla **legge n. 53 del 2021** (legge di delegazione europea 2019-2020), inserendovi il richiamo espresso all'Agenzia per la cibersicurezza nazionale.

Nello specifico, le modifiche hanno interessato l'articolo 4, comma 1, lettera *b)*, e l'articolo 18.

- L'articolo 4, comma 1, lettera *b)*, della legge n. 53 del 2021 elenca, tra i princìpi e criteri direttivi che il Governo deve osservare per l'attuazione della direttiva (UE) 2018/1972 (istitutiva del Codice europeo delle comunicazioni elettroniche), anche l'obbligo di rispettare il principio di stabilità dell'attuale riparto di competenze, in sede di assegnazione delle nuove competenze affidate all'AGCOM (quale Autorità nazionale indipendente di regolamentazione del settore) e alle altre autorità amministrative competenti. A seguito della citata modifica, la disposizione menziona ora, quali esempi di tali autorità amministrative competenti, non solo il MISE, ma **anche l'Agenzia per la cibersicurezza nazionale**.
- L'articolo 18 reca, a sua volta, princìpi e criteri direttivi per l'adeguamento della normativa nazionale alle disposizioni del Titolo III (Quadro di certificazione della cibersicurezza) del regolamento (UE) 2019/881: con la modifica apportata dall'articolo 16 del decreto-legge n. 82 del 2021, è ora previsto che **ogni riferimento al MISE, ovunque ricorra, è da intendersi riferito all'Agenzia per la cibersicurezza nazionale**, stante l'avvenuto trasferimento di attribuzioni di cui si è già detto.

Il **comma 2** reca la disciplina delle modalità di definizione dell'organizzazione e dei compiti dell'Autorità.

Al 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 Regolamento di organizzazione e funzionamento dell'Agenzia per la cibersicurezza nazionale):

- **l'organizzazione e le procedure** per lo svolgimento dei compiti che le competono in veste di Autorità nazionale di certificazione della cibersicurezza;
- le **modalità applicative** delle attività svolte, in ambito sia nazionale che internazionale, dall'Autorità (articoli 4 – 9, v. *infra*), nonché in sede di reclamo sui certificati di cibersicurezza e sulle dichiarazioni UE di conformità (articolo 11, v. *infra*);
- la **rigorosa separazione** tra le attività dell'Agenzia relative al rilascio di certificati europei di cibersicurezza (articolo 6, comma, v. *infra*) e le attività di vigilanza (articolo 5, v. *infra*), 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.

L'articolo 4, comma 4, del d.P.C.M. n. 223 del 2021 definisce le **Divisioni** quali strutture istituite, di norma all'interno dei Servizi, per la gestione di un insieme omogeneo di tematiche e macro-processi. Le Divisioni di maggiore complessità (il cui numero non può essere superiore a trenta) costituiscono articolazioni di livello dirigenziale non generale ed è previsto che, in sede di prima applicazione delle disposizioni del decreto-legge e fino alla rideterminazione della dotazione organica, non possono esserne istituite più di ventiquattro.

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

L'articolo 62 del Regolamento europeo sulla cibersicurezza disciplina la struttura e le funzioni dell'**ECCG**. Esso è composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o di altre autorità nazionali competenti (con la precisazione che ogni membro dell'ECCG non può rappresentare più di due Stati), mentre i portatori di interessi e le parti terze interessate possono essere invitati a presenziare alle riunioni e a partecipare ai suoi lavori. Le funzioni di presidenza e di segretario dell'ECCG sono svolte dalla **Commissione**, con l'assistenza dell'**ENISA** (European Union Agency for Cybersecurity), come previsto dall'articolo 8, paragrafo 1, lettera *e)*.

All'ECCG sono affidati i seguenti **compiti**:

a. **consigliare e coadiuvare la Commissione** nell'attuazione della disciplina, in particolare per quanto riguarda il programma di lavoro progressivo dell'Unione, le questioni relative alla politica in materia di certificazione della cibersicurezza, il coordinamento degli approcci strategici e la preparazione dei sistemi europei di certificazione della cibersicurezza;

b. **assistere, consigliare e collaborare con il gruppo consultivo ENISA** in relazione alla preparazione di una proposta di sistema europeo di certificazione della cibersicurezza ai sensi dell'articolo 49, nonché adottare il relativo parere;
c. **chiedere all'ENISA** di preparare proposte di sistemi, in casi debitamente giustificati, ai sensi dell'articolo 48, paragrafo 2;
d. **adottare pareri** indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza;
e. **esaminare gli sviluppi** che presentano un interesse in materia di certificazione della cibersicurezza e **scambio di informazioni e buone pratiche** sui sistemi europei di certificazione della cibersicurezza;
f. **agevolare la cooperazione** tra le autorità nazionali di certificazione della cibersicurezza attraverso lo sviluppo della capacità e lo scambio di informazioni, in particolare mediante la definizione di metodi per un efficiente **scambio di informazioni** in relazione a tutti gli aspetti della certificazione della cibersicurezza;
g. sostenere l'attuazione dei meccanismi di **valutazione *inter pares*** in conformità delle regole fissate da un sistema europeo di certificazione della cibersicurezza (articolo 54, paragrafo 1, lettera *u*);
h. **agevolare l'allineamento** dei sistemi europei di certificazione della cibersicurezza alle norme riconosciute a livello internazionale, rivedendo tra l'altro i sistemi europei di certificazione della cibersicurezza esistenti e, ove opportuno, rivolgendo **raccomandazioni** all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale.

L'articolo 66 del Regolamento europeo prevede, a sua volta, che la Commissione sia assistita da un **comitato** istituito ai sensi del Regolamento (UE) n. 182/2011, il quale stabilisce le regole e i princìpi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione. È espressamente previsto, al proposito, che trovi applicazione l'articolo 5, paragrafo 4, lettera b), di tale Regolamento, che, nell'ambito della procedura d'esame degli atti adottati dalla Commissione da parte dei comitati, impedisce alla Commissione stessa di adottare il progetto di atto di esecuzione nel caso in cui l'atto di base preveda come condizione necessaria l'espressione di un **parere** da parte del comitato, e questo non sia stato espresso.

Il **comma 3**, infine, reca le **autorizzazioni di spesa** per gli anni da 2022 in poi, 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 (v. *infra*);
- 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, cui si rinvia.

L'**articolo 5** dello schema di decreto legislativo 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 cibersicurezza, con riferimento ai certificati di cibersicurezza 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.

Le disposizioni appena richiamate stabiliscono, infatti, che le Autorità nazionali di certificazione della cibersicurezza, tra gli altri compiti:

- **supervisionano e fanno applicare le regole** previste nei sistemi europei di certificazione della cibersicurezza per il controllo della conformità dei prodotti ICT, servizi ICT e processi ICT con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti (lettera *a*) e
- **controllano la conformità** agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti ICT, servizi ICT o processi ICT che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità (lettera *b*).

Per **prodotto ICT** si intende un elemento o un gruppo di elementi di una rete o di un sistema informativo; per **servizio ICT** si intende un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi; per **processo ICT**, infine, si intende un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC.

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

cibersicurezza e sugli organismi di valutazione della conformità, ai sensi dell'articolo 58, paragrafo 8, del Regolamento.

L'articolo 58 elenca, al paragrafo 8, i **poteri** di cui ciascuna autorità nazionale di certificazione della cibersicurezza deve almeno disporre:

a. **richiedere** agli organismi di valutazione della conformità, ai titolari di certificati europei della cibersicurezza e agli emittenti di dichiarazioni UE di conformità di fornire le eventuali **informazioni necessarie** all'esecuzione dei suoi compiti;
b. condurre **indagini**, sotto forma di verifiche contabili, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità allo scopo di verificarne l'osservanza della normativa;
c. **adottare misure appropriate**, nel rispetto del diritto nazionale, per accertare che gli organismi di valutazione della conformità, i titolari di certificati europei di cibersicurezza e gli emittenti di dichiarazioni UE di conformità si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;
d. ottenere **accesso ai locali** degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersicurezza al fine di svolgere indagini in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri;
e. **revocare**, conformemente al diritto nazionale, i certificati europei di cibersicurezza rilasciati dalle autorità nazionali di certificazione della cibersicurezza o dagli organismi di valutazione della conformità, qualora tali certificati non siano conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;
f. irrogare **sanzioni** conformemente al diritto nazionale e chiedere la cessazione immediata delle violazioni degli obblighi di cui al presente 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),* 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)* che segue, nonché all'articolo 60, paragrafo 3, del Regolamento, a mente del quale, qualora i sistemi europei di certificazione della cibersicurezza stabiliscano requisiti specifici o supplementari, solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'autorità nazionale di certificazione della cibersicurezza a svolgere i compiti previsti da tali sistemi;
b. **monitoraggio e vigilanza** sulle attività degli organismi di valutazione della conformità pubblici di cui all'articolo 56, paragrafo 5, lettera *b)*, del Regolamento. Tale disposizione fa riferimento alla procedura di rilascio dei certificati europei di cibersicurezza, stabilendo che, in casi debitamente giustificati, un sistema europeo di certificazione della cibersicurezza può prevedere che essi possano essere rilasciati unicamente da un ente pubblico, da individuarsi in un'autorità nazionale di certificazione della cibersicurezza (lettera *a*) oppure in un organismo pubblico accreditato come organismo di valutazione della conformità (lettera *b*);
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 cibersicurezza (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.

La **cooperazione con altre autorità di vigilanza del mercato** competenti è prevista dall'articolo 58, paragrafo 7, lettera *a),* del Regolamento, con riferimento all'attività consistente nel supervisionare e far applicare le regole previste nei sistemi europei di certificazione della cibersicurezza in materia di controllo della conformità dei prodotti ICT, servizi ICT e processi ICT con i requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori.
La successiva lettera *h)* prevede, invece, in generale, la **cooperazione con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche**, anche mediante lo scambio di informazioni sugli eventuali prodotti ICT, servizi ICT e processi ICT non conformi ai requisiti del Regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza.

Sempre nello svolgimento dell'attività di vigilanza ai sensi del comma 1, all'Agenzia è consentito (**comma 3):**

- effettuare **indagini ed *audit*** nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti le dichiarazioni di conformità UE;
- ottenere informazioni anche tramite **l'accesso ai locali** degli organismi di valutazione della conformità o dei titolari dei certificati europei di cibersicurezza;
- **revocare certificati** ai sensi del successivo comma 4;
- **irrogare sanzioni** pecuniarie ed accessorie ai sensi dell'articolo 10 (v. *infra*);
- **prelevare prodotti.**

A tal fine, è espressamente sancito l'**obbligo**, per gli organismi di valutazione della conformità, per i titolari dei certificati europei di cibersicurezza 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.

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, cui si rinvia) e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

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).*

L'articolo 56, paragrafo 4, autorizza gli organismi di valutazione della conformità al rilascio dei certificati europei di cibersicurezza che fanno riferimento a un livello di **affidabilità «di base» o «sostanziale»** sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza adottato dalla Commissione.
In **deroga** a ciò, il paragrafo 5 prevede che, in casi debitamente giustificati, un sistema europeo di certificazione della cibersicurezza possa riservare il rilascio di tali certificati esclusivamente ad un ente pubblico, che è individuato, alla lettera *b)*, in un organismo pubblico accreditato come organismo di valutazione della conformità.
Il paragrafo 6 ha ad oggetto, invece, il rilascio di certificati europei di cibersicurezza che attestino un livello di **affidabilità «elevato»,** nell'ambito di un sistema europeo di certificazione della cibersicurezza che lo richieda. In tal caso, il certificato deve essere rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza oppure, nei due casi che seguono, da un organismo di valutazione della conformità:

- **previa approvazione** dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo certificato europeo di cibersicurezza rilasciato da un organismo di valutazione della conformità; o
- sulla base di una **delega generale** del compito di rilasciare tali certificati europei di cibersicurezza a un organismo di valutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

Si ricorda che, a mente dell'articolo 52, i sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti ICT, i servizi ICT e i processi ICT uno o più dei seguenti **livelli di affidabilità**: «di base», «sostanziale» o «elevato». Il livello di affidabilità è commisurato al livello del **rischio** associato al previsto uso del prodotto ICT, servizio ICT o processo ICT, in termini di probabilità e impatto di un incidente.
Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di **affidabilità «di base»** assicura che i prodotti ICT, i servizi ICT e i processi ICT per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.
Un certificato europeo di cibersicurezza che si riferisca al livello di **affidabilità «sostanziale»** assicura che i prodotti ICT, servizi ICT e processi ICT per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti ICT, i servizi ICT o i processi ICT attuano correttamente le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

Un certificato europeo di cibersicurezza che si riferisca al livello di **affidabilità «elevato»** assicura che i prodotti ICT, i servizi ICT e i processi ICT per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno le seguenti: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti ICT, i servizi ICT o i processi ICT attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.

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 ad un prodotto ICT, servizio ICT o processo ICT che ha comportato un **concreto e dimostrato pregiudizio**:
  - ad 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);
  - ad un **servizio di comunicazione elettronica** come definito ai sensi dell'articolo 2, comma 1, lettera *fff),* del decreto legislativo n. 259 del 2003 (c.d. 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 ed in generale, **se previsto** espressamente dallo specifico sistema europeo di certificazione. Conseguentemente, si seguiranno 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 cibersicurezza (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.

Infine, 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.

Tale previsione costituisce applicazione dell'**articolo 30, commi 4 e 5, della legge n. 234 del 2012** (legge sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa europea; per ogni approfondimento, si rinvia al relativo tema), i quali prevedono, rispettivamente, che:

- gli oneri relativi a prestazioni e a controlli da eseguire da parte di uffici pubblici, ai fini dell'attuazione delle disposizioni dell'Unione europea di cui alla legge di delegazione europea per l'anno di riferimento e alla legge europea per l'anno di riferimento, **sono posti a carico dei soggetti interessati**, secondo tariffe prestabilite, pubbliche e determinate sulla base del costo effettivo del servizio reso;

- le **entrate** derivanti dalle tariffe così determinate sono attribuite, nei limiti previsti dalla legislazione vigente, alle amministrazioni che effettuano le prestazioni e i controlli, mediante riassegnazione ai sensi del regolamento di cui al d.P.R. n. 469 del 1999 (recante norme di semplificazione del procedimento per il versamento di somme all'entrata e la riassegnazione alle unità previsionali di base per la spesa del bilancio dello Stato, con particolare riferimento ai finanziamenti dell'Unione europea).

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 (v. *infra*).

L'**articolo 6** reca la disciplina per il **rilascio dei certificati di cibersicurezza.**

Con riferimento ai certificati di cibersicurezza con livello di affidabilità **elevato**, 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, cui si rinvia), 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 (v. *supra*).

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, su cui v. *supra*), 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;
- **monitorato** e **vigilato** dall'Agenzia;
- **designato** dall'Agenzia ai sensi del provvedimento di cui all'articolo 4, comma 2 (v. *supra*).

Il **comma 3** - riportando fedelmente il contenuto dell'articolo 56, comma 2, del Regolamento - stabilisce che la certificazione della cibersicurezza 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 cibersicurezza 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**, infine, facendo anch'esso riferimento all'articolo 30, commi 4 e 5, della legge n. 234 del 2012 (v. *supra*) e precisando che le somme sono determinate e da corrispondere ai sensi dell'articolo 13 (v. *infra*), 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 cibersicurezza 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.

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 cibersicurezza (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.

Come già per la certificazione di cibersicurezza, è specificato che il rilascio di una dichiarazione UE di conformità è; **volontario**, salvo diversamente specificato nel diritto dell'Unione o dal diritto nazionale e che, in mancanza di un diritto dell'Unione armonizzato, l'Agenzia può stabilire l'obbligatorietà della dichiarazione UE di conformità nelle fattispecie di cui al precedente articolo 6, comma 3.

L'**articolo 8** regolamenta la procedura di **accreditamento ed 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 ed 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.

Il citato **articolo 61** prevede che, per ciascun sistema europeo, le autorità nazionali di certificazione della cibersicurezza notificano alla Commissione gli **organismi** di valutazione della conformità che sono stati **accreditati** e, se del caso, **autorizzati** a rilasciare certificati europei di cibersicurezza ai livelli di affidabilità di cui all'articolo 52 del Regolamento (v. *supra*). Le autorità nazionali di certificazione della cibersicurezza notificano, altresì, alla Commissione, senza indebito ritardo, ogni successiva modifica degli stessi.
Un anno dopo l'entrata in vigore di un sistema europeo di certificazione della cibersicurezza, la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un **elenco** degli organismi di valutazione della conformità notificati nell'ambito di tale sistema. Laddove la Commissione dovesse ricevere una notifica dopo lo scadere di tale periodo, essa provvede a pubblicare, nella *Gazzetta ufficiale dell'Unione europea,* le modifiche del predetto elenco, entro due mesi dalla data di ricevimento della notifica.
Un'autorità nazionale di certificazione della cibersicurezza può presentare alla Commissione una **richiesta di rimozione** di un organismo di valutazione della conformità già notificato, e la Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricevimento della richiesta dell'autorità nazionale.

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, è previsto 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 (secondo la già citata procedura di cui all'articolo 5, comma 3, alinea, del d.P.C.M. n. 223 del 2021), costituisce, aggiorna e rende 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, su cui v. *supra* -, 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 norma dell'articolo 30, commi 4 e 5, della legge n. 234 del 2012, v. *supra* - a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione. Le somme sono determinate e sono da corrispondere ai sensi dell'articolo 13 (v. *infra*).

Allo scopo di **elevare il livello nazionale di cibersicurezza**, 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 ed internazionale.

L'Agenzia **monitora**, altresì, **gli sviluppi** nel campo della certificazione della cibersicurezza, 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 cibersicurezza.

Nel caso in cui manchi un sistema europeo di certificazione, l'Agenzia **può introdurre sistemi di certificazione nazionali della cibersicurezza** per prodotti ICT, servizi ICT o processi ICT, conformemente all'articolo 57 del Regolamento.

L'articolo 57 appena citato dispone che i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti ICT, servizi ICT e processi ICT non coperti da un sistema europeo di certificazione della cibersicurezza **restano in vigore**.
Al contrario, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti ICT, servizi ICT e processi ICT coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato dalla Commissione. Resta fermo che i certificati esistenti rilasciati nell'ambito di sistemi nazionali di certificazione della cibersicurezza e coperti da un sistema europeo di certificazione della cibersicurezza restano validi fino alla loro data di scadenza.
Gli Stati membri **non** introducono nuovi sistemi nazionali di certificazione della cibersicurezza per prodotti ICT, servizi ICT e processi ICT già coperti da un sistema europeo di certificazione della cibersicurezza in vigore.
In ogni caso, al fine di **evitare la frammentazione** del mercato interno, gli Stati membri informano la Commissione e l'ECCG di ogni intenzione di elaborare nuovi sistemi nazionali di certificazione della cibersicurezza.

Sanzioni, reclami e ricorsi giurisdizionali (artt. 10-12)

L'**articolo 10** – disposizione di apertura del **Capo III**, relativo alla disciplina delle sanzioni, dei reclami e dei ricorsi giurisdizionali – reca il **quadro sanzionatorio** di riferimento, stabilendo al **comma 1** che l'Agenzia, in caso di violazione degli obblighi del quadro europeo di certificazione della cibersicurezza, irroga **sanzioni pecuniarie ed 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 si è 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.

L'articolo 58, paragrafo 8, lettera *f)*, attribuisce all'autorità nazionale il potere di irrogare sanzioni conformemente al diritto nazionale e chiedere la cessazione immediata delle violazioni degli obblighi di cui al Regolamento.
L'articolo 65 dispone che gli Stati membri stabiliscono le sanzioni applicabili in caso di violazione della normativa e dei sistemi europei di certificazione della cibersicurezza e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere **effettive**, **proporzionate** e **dissuasive**. Gli Stati membri notificano senza indugio tali norme e misure alla Commissione e provvedono poi a dare notifica delle eventuali modifiche successive.

Di seguito, l'elenco degli **illeciti** tipizzati con le relative **sanzioni**.

- Salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che **emette un certificato di cibersicurezza 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 (comma 2).
- 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 (comma 3).
- 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 cibersicurezza, ai sensi dell'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 cibersicurezza 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 cibersicurezza obbligatorio. In tali casi, 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 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 (commi 4 e 5).

- 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 (comma 6).
- Salvo che il fatto costituisca reato, 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 (comma 7).
- Salvo che il fatto costituisca reato, il titolare di un certificato europeo di cibersicurezza che **non notifichi**, ai sensi dell'articolo 56, paragrafo 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 cibersicurezza 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 (comma 8).
- 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 (comma 9).
- Salvo che il fatto costituisca reato, l'organismo di valutazione della conformità che **non ottempera agli obblighi di divulgazione** dei certificati europei di cibersicurezza 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 specifichi nella procedura per i reclami definita ai sensi dell'articolo 11, comma 2, l'inoltro degli stessi per conoscenza anche all'Agenzia (comma 10).
- 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 ed il soggetto può richiedere il rilascio di nuova autorizzazione (comma 11).
- 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. 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, fornisce dati, informazioni o documentazione falsi (comma 12).
- Salvo che il fatto costituisca reato, il fabbricante che **viola 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, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro (comma 13).

- 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 (comma 14).
- 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 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 (comma 15).

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 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 n. 65 del 2018, o di un **servizio di comunicazione elettronica** ai sensi dell'articolo 2, comma 1, lettera *fff)*, del decreto 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.

Infine, 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.

L'**articolo 11** disciplina la **procedura dei reclami** sui certificati di cibersicurezza 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:

1. l'**emittente** di un certificato europeo di cibersicurezza, o
2. l'**Agenzia**, se il reclamo riguarda un certificato europeo di cibersicurezza 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.

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 e, nel caso di autorizzazione ai sensi dell'articolo 60, paragrafo 3, del Regolamento, la procedura di reclamo indicata dall'organismo prevede l'inoltro del reclamo da parte del reclamante, oltreché all'organismo, anche per conoscenza all'Agenzia.

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**. Il reclamante formula istanza all'Agenzia, identificando il certificato di cibersicurezza o la dichiarazione UE di conformità oggetto del reclamo, le ragioni del reclamo e le azioni correttive che ritiene necessarie (comma 3).

In tale ultima ipotesi, l'Agenzia informa il reclamante dello stato del procedimento e della decisione adottata, nonché del diritto a un ricorso giurisdizionale effettivo.

L'Agenzia risponde ai reclami entro **novanta giorni** dal ricevimento dell'istanza ed il silenzio è da intendersi alla stregua di un **rigetto**.

L'**articolo 12** disciplina la presentazione dei **ricorsi giurisdizionali** in materia di certificati europei di cibersicurezza e dichiarazioni UE di conformità. Si tratta di una disposizione finalizzata a dare 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:

a. le **decisioni** assunte dall'Agenzia per la cibersicurezza nazionale - **ACN** (in qualità di autorità nazionale di certificazione della cibersicurezza 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 cibersicurezza detenuto da tali persone fisiche e giuridiche;
   Si valuti l'opportunità di chiarire se il rilascio improprio faccia riferimento al rilascio di un certificato europeo di cibersicurezza (o dichiarazione UE di conformità) non conforme, come definito dall'articolo 3, lettera aa) del Regolamento.
b. 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 in esame.

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, si ricorda che ai sensi dell'articolo **135,** lettera **h-bis) c.p.a.**, introdotta dal decreto-legge n. 82 del 2021 (*Disposizioni urgenti in materia di cibersicurezza, definizione dell'architettura nazionale di cibersicurezza e istituzione dell'Agenzia per la cibersicurezza 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 cibersicurezza nazionale". *Si valuti pertanto l'opportunità di coordinare la disposizione alla luce di quanto già previsto dall'art. 135, lettera h-bis) c.p.a.*

Con riguardo al riferimento ai ricorsi "al TAR del luogo ove è ubicata la sede degli altri organismi di valutazione della conformità per i ricorsi contro (le decisioni di) tali organismi", la disposizione sembrerebbe stabilire un criterio di competenza territoriale per quanto concerne la giurisdizione del giudice amministrativo. S*i valuti in proposito l'opportunità di un approfondimento sui profili connessi al riparto di giurisdizione anche avendo riguardo alle attività svolte in concreto da tali organismi.*

Per quanto riguarda inoltre la formulazione del testo, si valuti l'opportunità di riferire la presentazione dinanzi al giudice dei "ricorsi" invece che dei "procedimenti", come ora indicato nel comma 2 e di modificare di conseguenza la parte restante della disposizione.

Disposizioni finanziarie e finali (artt. 13-15)

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 cibersicurezza.

La disposizione attua lo specifico criterio di delega di cui alla lettera c) del comma 2 dell'articolo 18 della L. 53/2021.

In base al citato criterio, gli introiti derivanti dall'irrogazione delle sanzioni devono 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 cibersicurezza. E' noto tuttavia che in base all'articolo 16, comma 12, lettera b) del decreto-

legge 14 giugno 2021, n. 82, i riferimenti al Ministero dello sviluppo economico in tutti i criteri di delega sono sostituiti con i riferimenti alla nuova Agenzia per la cibersicurezza nazionale, a cui il medesimo decreto ha affidato la funzione di autorità nazionale di certificazione della cibersicurezza,

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 cibersicurezza, 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 24 dicembre 2012, n. 234

In proposito merita ricordare che ai sensi dell'**articolo 1 della legge n. 53 del 2021** (legge di delegazione europea 2019-2020), le eventuali spese non contemplate da leggi vigenti e che non riguardano l'attività ordinaria delle amministrazioni statali o regionali possono essere previste nei soli limiti occorrenti per l'adempimento degli obblighi derivanti dall'esercizio delle deleghe di cui allo stesso articolo 1, comma 1. Alla relativa copertura, nonché alla copertura delle minori entrate eventualmente derivanti dall'attuazione delle deleghe, laddove non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, si provvede mediante riduzione del fondo per il recepimento della normativa europea di cui all'articolo 41-bis della citata legge n. 234 del 2012. Qualora la dotazione del predetto fondo si rivelasse insufficiente, i decreti legislativi dai quali derivino nuovi o maggiori oneri sono emanati solo successivamente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie. In relazione alla copertura individuata, la relazione tecnica spiega che l'individuazione dell'autorità nazionale di certificazione della cibersicurezza 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.

Il comma 2 dispone che le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi (art. 4, co. 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.

Si ricorda che il Piano triennale per l'informatica nella pubblica amministrazione fissa gli obiettivi e individua i principali interventi di sviluppo e gestione dei sistemi informativi delle p.a. (art. 14-bis del D.Lgs. 82/2005 Codice dell'amministrazione digitale CAD). Il Piano è redatto dall'AgID, che ne cura anche la verifica dell'attuazione, e approvato dal Presidente del Consiglio, o dal ministro delegato per l'informatizzazione. Con il decreto del Ministro per l'innovazione tecnologica e la transizione digitale del 24 febbraio 2022è stato approvato il Piano triennale per l'informatica nella pubblica amministrazione 2021-2023 che prosegue e integra le linee di azione del Piano 2020-2022 del Piano 2019-2021 e del Piano 2017-2019.

Il comma 3 stabilisce che dall'attuazione del decreto legislativo **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, 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 in esame - 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.

Si ricorda che il provvedimento di cui si prefigura un eventuale aggiornamento, previsto ai sensi dell'articolo 4, co. 2, dello schema in esame, individua l'organizzazione e le procedure per lo svolgimento dei compiti dell'Agenzia quale autorità nazionale di certificazione della cibersicurezza, nonché la definizione delle modalità applicative delle attività previste dal decreto in esame.

Quadro normativo

In materia di certificazione della sicurezza informatica, **a livello nazionale** vige il DPCM 30 ottobre 2003 (pubblicato nella *Gazzetta Ufficiale* 27 aprile 2004, n. 98), che 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 DPCM 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 (articolo 3) una procedura di valutazione e la relativa certificazione.

Il medesimo DPCM 30 ottobre 2003 (art. 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.

L'OCSI sovrintende alle attività operative di valutazione e certificazione nell'ambito dello Schema nazionale attraverso:

- la predisposizione di regole tecniche in materia di certificazione sulla base delle norme e direttive nazionali, comunitarie ed 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 princìpi 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.

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

Ai sensi del DPCM 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 Perimetro sono tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il DPCM 14 aprile 2021, n. 81

Inoltre, i soggetti inclusi nel perimetro, ai sensi dell'articolo 1, comma 6, del decreto legge n. 105/2019 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 DPR 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. 105/2019, nonché i criteri tecnici per l'individuazione delle categorie di beni, sistemi e servizi ICT (da effettuarsi con DPCM) che saranno oggetto della valutazione del CVCN nel caso in cui siano destinati agli *asset* "strategici". Tali categorie sono state individuate con il DPCM 15 giugno 2021

Il decreto-legge 14 giugno 2021, n. 82, che ha ridefinito l'architettura nazionale di cibersicurezza e istituito l'**Agenzia per la cibersicurezza nazionale**, ha trasferito il CVCN presso l'Agenzia e la sua operatività è assicurata dal 30 giugno 2022.

Il 25 maggio 2022 è stata presentata dal Governo la **Strategia Nazionale di cibersicurezza 2022-2026** e l'annesso Piano di implementazione, approvati il 18 maggio 2022 dal Comitato Interministeriale per la Cybersicurezza, presieduto dal Presidente del Consiglio. La Strategia, che fissa gli obiettivi e gli strumenti di intervento in materia di sicurezza cibernetica, prevede, tra l'altro il potenziamento delle capacità del CVCN.

A seguito della crisi in Ucraina sono state adottate alcuni disposizioni di urgenza finalizzate alla **diversificazione delle dotazioni informatiche delle pubbliche amministrazioni** (D.L. 21/2022, art. 29).

Si prevede 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 ad una **circolare** dell'Agenzia per la cibersicurezza nazionale l'individuazione delle **categorie di prodotti** destinate alla sicurezza dei dispositivi (antivirus, antimalware, 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 cibersicurezza nazionale ha emanato la circolare 21 aprile 2022, n. 4336, relativa alla "Diversificazione di prodotti e servizi tecnologici di sicurezza informatica".

Più in generale in materia di sicurezza informatica si veda la pagina Sicurezza cibernetica del portale della documentazione della Camera dei deputati.

Rispetto delle competenze legislative costituzionalmente definite

Il provvedimento appare riconducibile in via prevalente alla materia "sicurezza dello Stato" di competenza legislativa esclusiva dello Stato ai sensi dell'articolo 117, secondo comma, lettera d) della Costituzione.

Compatibilità con la normativa dell'Unione europea

Documenti all'esame delle istituzioni dell'Unione europea

È prossima all'adozione da parte delle Istituzioni legislative UE la proposta di direttiva, cosiddetta **direttiva NIS2** (NIS, *Network and Information Security*), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, presentata dalla Commissione europea nel dicembre 2020.

Sulla proposta il 13 maggio 2022 il Consiglio e il Parlamento europeo sono giunti a un accordo, che necessita dell'approvazione formale.

La proposta di direttiva NIS 2 stabilisce il quadro di riferimento per le **misure** di **gestione** dei rischi di **cibersicurezza** e gli obblighi di **segnalazione** in una serie di settori che comprende, tra l'altro, l'energia, i trasporti, la salute e le infrastrutture digitali.

In particolare, stabilisce **norme minime** e meccanismi per la **cooperazione** tra le **autorità competenti** di ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza, e prevedendo mezzi di **ricorso** e **sanzioni** per garantirne l'applicazione.

La proposta prevede l'istituzione di una **rete europea** delle organizzazioni di collegamento per le crisi informatiche **EU-CyCLONe**, volta a sostenere la gestione coordinata degli incidenti di cibersicurezza su vasta scala.

Mentre ai sensi della precedente direttiva NIS la responsabilità di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali spettava agli Stati membri, la nuova direttiva NIS 2 introduce la regola della **soglia di dimensione**. Ciò significa che tutti i **soggetti di medie e grandi dimensioni** che operano nei settori o forniscono i servizi contemplati dalla direttiva dovrebbero rientrare nel suo ambito di applicazione.

Il testo concordato in via provvisoria contiene disposizioni per garantire la proporzionalità, un livello più elevato di gestione dei rischi e parametri di criticità definiti per determinare i soggetti interessati.

Il nuovo regime esclude dalla sua applicazione i soggetti operanti in settori quali la difesa o la sicurezza nazionale, la pubblica sicurezza, l'attività di contrasto e la giustizia. Sono altresì esclusi **Parlamenti** e **banche centrali**. La NIS2 dovebbe invece applicarsi agli enti della pubblica amministrazione a livello centrale e regionale, gli Stati membri possono decidere che si applichi a tali enti anche a livello locale.

Unitamente alla riforma della direttiva NIS la Commissione europea ha presentato una proposta di direttiva sulla **resilienza dei soggetti critici** che riscrive il regime contenuto nella direttiva 2008/114/CE, relativa all'individuazione e alla designazione delle **infrastrutture critiche europee** e alla valutazione della necessità di migliorarne la protezione

Il nuovo regime riguarda **soggetti critici** in una serie di settori come: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali e spazio.

Lo scopo della proposta è dotare tali soggetti della capacità di prevenire, proteggersi, rispondere, resistere e riprendersi in caso di catastrofi naturali, atti terroristici o emergenze sanitarie come la COVID-19.

Secondo la proposta gli Stati membri dovranno dotarsi di una **strategia** per rafforzare la resilienza dei soggetti critici, effettuare una **valutazione** dei **rischi** almeno ogni **quattro anni** e individuare i soggetti critici che forniscono **servizi essenziali**.

I soggetti critici dovrebbero individuare i rischi rilevanti in grado di perturbare in modo significativo la fornitura di servizi essenziali, adottare misure adeguate per garantire la propria resilienza e notificare gli eventi perturbatori alle autorità competenti.

La proposta di direttiva stabilisce inoltre norme per l'individuazione dei soggetti critici di particolare rilevanza europea. Un soggetto critico è considerato tale di particolare rilevanza europea quando fornisce un servizio essenziale a o in più di un terzo degli Stati membri. In questi casi, la Commissione può essere invitata a organizzare una missione di consulenza per valutare le misure predisposte dal soggetto interessato per adempiere ai propri obblighi.

Senato: Dossier n. 555
Camera: Atti del Governo n. 388
25 maggio 2022

Senato	Servizio Studi del Senato	Studi1@senato.it - 066706-2451	SR_Studi
Camera	Servizio Studi Dipartimento Istituzioni	st_istituzioni@camera.it - 066760-3855	CD_istituzioni
	Servizio Studi Dipartimento Trasporti	st_trasporti@camera.it - 066760-2614	CD_trasporti
	Servizio Studi Dipartimento Bilancio	st_bilancio@camera.it - 066760-2233	CD_bilancio