dossier

XIX Legislatura

14 luglio 2026

Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti

Atto del Governo n. 422

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO STUDI
TEL. 06 6706-2451 - ✉ studi1@senato.it – 𝕏 @SR_Studi

Dossier n. 736

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-9475 - ✉ st_istituzioni@camera.it – 𝕏 @CD_istituzioni

Dipartimento Trasporti
Tel. 06 6760-2614 - ✉ st_trasporti@camera.it – 𝕏 @CD_trasporti

Progetti di legge n. 422

I N D I C E

Articolo 1 *(Modifiche al decreto legislativo n. 123 del 2022)* 5

Articolo 2 *(Modifiche all'articolo 35 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82)* 12

Articolo 3 *(Modifiche all'articolo 7 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)* 15

Articolo 4 *(Clausola di invarianza finanziaria)* 19

LE RECENTI INIZIATIVE LEGISLATIVE DELL'UNIONE EUROPEA IN MATERIA DI CYBERSICUREZZA 20

Articolo 1
(Modifiche al decreto legislativo n. 123 del 2022)

L'**articolo** estende ai **servizi di sicurezza gestiti** il sistema europeo di **certificazione** della *cybersicurezza*. L'articolo attua una delega contenuta nella legge di delegazione europea per il 2025. Al fine di adeguare la normativa nazionale a quella dell'Unione europea, l'articolo in esame novella in più punti il decreto legislativo n. 123 del 2022.

Lo schema di decreto legislativo in esame si pone l'obiettivo di dare attuazione alla delega di cui all'**articolo 16** della legge n. 36 del 2026 (legge di delegazione europea per il 2025). Tale articolo reca una delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2025/37 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che modifica il regolamento (UE) 2019/881 per quanto riguarda i **servizi di sicurezza gestiti**.

Secondo la definizione data dalla richiamata normativa unionale (**art. 14 *bis*** del regolamento (UE) 2019/881) un servizio di sicurezza gestito è:
"un servizio prestato a un terzo consistente nello svolgimento di attività, o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di *cybersicurezza*, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica".
La relazione illustrativa evidenzia che i servizi di sicurezza gestiti svolgono un ruolo importante nella prevenzione, nel rilevamento e nella risposta agli incidenti di *cybersicurezza*. Tali servizi sono considerati soggetti "essenziali" o "importanti" ai sensi della direttiva (UE) 2022/2555 (c.d. **direttiva NIS 2**).

Attualmente, la normativa la principale normativa nazionale in materia è rappresentata dal **decreto legislativo n. 123 del 2022** (norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «Quadro di certificazione della *cybersicurezza*» del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la *cybersicurezza*, e alla certificazione della *cybersicurezza* per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013).

L'**articolo 1** dello schema di decreto legislativo in esame si compone di **un comma** a sua volta suddiviso in **sette lettere** (**a-g**). L'articolo novella in più punti il citato **decreto legislativo n. 123 del 2022**.

L’articolo dà attuazione al principio e criterio direttivo di cui all’**articolo 16, comma 2, lettera a)** della citata legge di delega (legge n. 36 del 2026).

Si analizzeranno di seguito le novelle apportate a tale testo dalle varie lettere del citato **articolo 1**, **comma 1:**

- la **lettera a)** novella in più punti l’**articolo 3**, **comma 1**, del decreto legislativo n. 123 del 2022. Nello specifico:

1. si prevede l’introduzione della nuova lettera **a-bis)** che fornisce una definizione di “**servizio di sicurezza gestito**”. Come evidenziato dalla relazione illustrativa, tale definizione è mutuata integralmente dal regolamento (UE) 2019/881;
2. si novella il contenuto della **lettera d)** che definisce la nozione di “**messa a disposizione sul mercato**”. La novella mira ad includere in tale nozione anche la fornitura di un **servizio di sicurezza gestito;**
3. si novella il contenuto della **lettera f)** che definisce la nozione di “**ritiro**”. La novella mira ad includere in tale nozione anche i provvedimenti volti ad impedire la messa a disposizione sul mercato di un **servizio di sicurezza gestito** all’interno della catena della fornitura;
4. si novella il contenuto della **lettera g)** che definisce la nozione di “**vigilanza del mercato**”. La novella mira ad includere in tale nozione anche le attività svolte dalle autorità competenti al fine di garantire che i **servizi di sicurezza gestiti** siano conformi ai requisiti stabiliti dal **quadro europeo di certificazione** e non pregiudichino la salute, la sicurezza o qualsiasi altro aspetto volto a garantire la protezione del pubblico interesse;
5. si novella il contenuto della **lettera u)** che definisce la nozione di “**dichiarazione UE di conformità**”. La novella mira a prevedere che tale nozione ricomprenda anche un riferimento ai **servizi di sicurezza gestiti**;
6. si novella la **lettera z)** al fine di inserire un riferimento ai **servizi di sicurezza gestiti** nei “**certificati europei di *cybersicurezza***”. In particolare, si prevede che tali certificati possano essere rilasciati, previa valutazione da un organismo di certificazione che attesti la valutazione di conformità ai requisiti stabiliti dal sistema europeo di certificazione, anche in riferimento ai **servizi di sicurezza gestiti**.

- la **lettera b)** novella in più punti l'**articolo 5** del decreto legislativo n. 123 del 2022 in relazione alla disciplina delle **attività di vigilanza del mercato**. Nello specifico:

1. si novella il **comma 4**, **lettera b)**, del citato articolo. Il testo, come modificato, prevede che nel caso in cui l'Agenzia per la *cybersicurezza* nazionale (ACN o Agenzia) all'esito delle sue attività di vigilanza accerti l'emissione di certificati **non conformi** per il **livello base** o **sostanziale** li sottoponga a **revoca**. Tale circostanza si verifica a condizione che il certificato non conforme sia relativo ad **un prodotto TIC** (tecnologia dell'informazione e della comunicazione), **servizio TIC**, **processo TIC** o **servizio di sicurezza gestito** (fattispecie quest'ultima non presente nella normativa attualmente vigente) che ha comportato un **concreto** e **dimostrato** pregiudizio a un **soggetto essenziale** secondo la definizione della nozione presente nell'**articolo 6**, **commi 1** e **2**, del decreto legislativo n. 138 del 2024. Si rimanda al seguente dossier per approfondimenti sul punto;
2. si novella il **comma 5**, **secondo periodo**. La novella prevede che nei casi previsti dal **comma 4, lettera b)** (vedi sopra), l'**Agenzia** chiede al soggetto che ha emesso il certificato di provvedere alla sua revoca entro e non oltre 5 giorni, **dandone contestuale notifica** all'**Agenzia** stessa;
3. si novella il **comma 6**. La novella conferisce all'ACN la possibilità di chiedere al soggetto che ha emesso un certificato non conforme 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 un termine stabilito dalla stessa ACN** ma, in ogni caso, **non superiore** a 120 giorni. Il testo vigente, invece, prevede che la richiesta di riesame da parte dell'Agenzia debba concludersi entro 120 giorni;
4. si novella il **comma 9**. La novella espunge il rinvio fatto da tale comma a sé stesso. L'intervento normativo, come evidenziato anche dalla relazione illustrativa, mira a correggere un **errore materiale**. Nello specifico il **comma 9** (di per sé non oneroso) reca la copertura finanziaria per gli oneri derivanti dall'attuazione dell'attività di vigilanza del mercato dell'ACN secondo quanto previsto dai **commi 3** e **8** del medesimo articolo. Si veda il seguente *dossier* per approfondimenti.

- la **lettera c)** novella l'**articolo 6**, **comma 1**, del decreto legislativo n. 123 del 2022. Tale comma definisce le modalità per l'emissione da parte dell'ACN dei certificati di cybersicurezza a livello nazionale per il livello di

affidabilità elevato. La novella estende la possibilità per l'ACN, tramite l'organismo di certificazione della sicurezza informatica (OCSI) di rilasciare anche certificati di livello **sostanziale** e **base** (ex **art. 56** del regolamento (UE) 2025/37/2025);

- la **lettera d)** novella in diversi punti l'**articolo 7** del decreto legislativo n. 123 del 2022. Nello specifico:

1) viene novellato il **comma 1** inserendo la possibilità per i fornitori o fabbricanti di **servizi di sicurezza gestiti** di rilasciare, sotto la **propria responsabilità,** dichiarazioni UE di conformità di **livello base** per dimostrare il rispetto di requisiti tecnici previsti nel sistema. Il testo attualmente vigente consente tale facoltà ai soli fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC;
2) viene novellato il **comma 2** estendendo ai fabbricanti o fornitori di **servizi di sicurezza gestiti**, il dovere di rendere disponibile all'ACN la dichiarazione di conformità, la relativa documentazione e altre informazioni pertinenti. Copia della dichiarazione UE di conformità è trasmessa all'ACN e a ENISA (Agenzia europea per la *cybersicurezza*).

- la **lettera e)**, novella l'**articolo 9**, **comma 3**, del decreto legislativo n. 123 del 2022. Nello specifico, il testo novellato consente all'ACN di introdurre sistemi di certificazione nazionali della *cybersicurezza*, per **servizi di sicurezza gestiti**, attualmente tale facoltà è limitata ai prodotti TIC, servizi TIC o processi TIC. Si ricorda che, ai sensi dell'**articolo 9, comma 3**, del citato decreto legislativo, l'ACN può agire solo conformemente all'**articolo 57** del regolamento UE 37/2025 e in assenza di un sistema europeo di certificazione;

- la **lettera f)** novella in più punti l'**articolo 10** del decreto legislativo n. 123 del 2022. Tale articolo definisce il quadro sanzionatorio in relazione al mancato rispetto degli obblighi del quadro europeo di certificazione della *cybersicurezza*. Nello specifico:

1. viene novellato il **comma 1** dell'articolo. Si prevede che alla disciplina dei poteri sanzionatori dell'ACN sia applicabile, in quanto compatibile, l'**articolo 17, comma 4-*quater***, del decreto-legge n. 82 del 2021. Tale rinvio sostituisce quello vigente che rimanda alla legge n.689 del 1981. Il citato **articolo 17, comma 4-*quater***, dispone che la disciplina del procedimento sanzionatorio amministrativo dell'ACN sia definito con un regolamento che stabilisce, in particolare, termini e modalità per l'accertamento, la

contestazione e la notificazione delle violazioni della normativa in materia di *cybersicurezza* e l'irrogazione delle relative sanzioni di competenza dell'Agenzia ai sensi del presente decreto e delle altre disposizioni che assegnano poteri accertativi e sanzionatori all'Agenzia;

2. si novella il **comma 4** che modifica il quadro sanzionatorio estendendo ai fabbricanti e ai fornitori di servizi di **sicurezza gestiti** che immettono sul mercato prodotti privi di dichiarazione UE di conformità obbligatoria, con dichiarazione non conforme o in assenza di certificato di *cybersicurezza* obbligatorio le previsioni rivolte ai produttori o fornitori di servizi TIC. Fatto salvo che il fatto costituisca reato, la sanzione consiste nel pagamento di una somma **non inferiore a 30.000€** e **non superiore a 150.000€**;
3. viene novellato il **comma 5**. La modifica estende ai servizi di sicurezza gestiti i poteri inibitori dell'ACN. In particolare, nei casi di cui al **comma 4** (vedi sopra) o in seguito all'esito di un accertamento di conformità, si abbia la revoca di un certificato obbligatorio per la messa a disposizione sul mercato di un prodotto o un servizio TIC o di un servizio di sicurezza gestito, l'ACN dispone il **ritiro** del prodotto o l'**inibizione** del servizio. I costi sono a carico esclusivamente del fabbricante o del fornitore. L'ACN indica i tempi e le modalità per il ritiro dei prodotti dal mercato e l'inibizione dei servizi;
4. viene novellato il **comma 8**, che estende alla sicurezza dei servizi di sicurezza gestiti, gli obblighi di notifica per i titolari dei certificati UE di *cybersicurezza* che abbiano riscontrato in essi eventuali vulnerabilità o irregolarità. A meno che il fatto non costituisca un reato, la sanzione per il titolare che non procede a notificare consiste nel pagamento di una somma compresa tra i **60.000€** e **300.000€**. Inoltre, si estende ai **servizi di sicurezza gestiti** la previsione secondo cui alla medesima sanzione sono sottoposti gli organismi di valutazione della conformità che hanno emesso un certificato di *cybersicurezza* ovvero i rispettivi titolari, fornitori o fabbricanti emittenti una dichiarazione UE di conformità, che dovessero rilevare o venire a conoscenza della presenza di vulnerabilità;

Il **decreto legislativo n. 123 del 2022** definisce gli obblighi di notifica attraverso un rinvio all'**articolo 56**, **paragrafo 8**, del regolamento (UE) 2019/881. Nello specifico, i titolari di un certificato europeo di *cybersicurezza* sono tenuti ad informare l'autorità nazionale di certificazione della *cybersicurezza*, ove sia questa a rilasciare il certificato europeo di

cybersicurezza, o l'organismo di certificazione del rilevamento di eventuali vulnerabilità o irregolarità. In quest'ultimo caso, l'organismo di certificazione trasmette le informazioni così ricevute, senza indebiti ritardi, all'autorità nazionale di certificazione della *cybersicurezza* interessata.
Come accennato, in Italia l'Autorità nazionale di certificazione della *cybersicurezza* (NCCA) ai sensi del decreto-legge n. 82 del 2021 e del regolamento (UE) 2019/881 è l'ACN. L'attività di certificazione viene svolta dall'Organismo di certificazione della sicurezza informatica – **OCSI** (istituito dall'**articolo 4, comma 1**, del decreto del Presidente del Consiglio dei Ministri del 30 ottobre 2003). Dal **primo luglio 2022** l'**OCSI** è incardinato all'interno dell'ACN in seguito al trasferimento di competenze in materia di certificazione della *cybersicurezza* di cui all'**articolo 7**, **comma 1**, **lettera e)**, del citato decreto-legge n. 82 del 2021. Tale disposizione è stata attuata dal con il decreto del Presidente del Consiglio dei Ministri del 15 giugno 2022

5. viene novellato il **comma 16**. La novella estende ai **servizi di sicurezza gestiti** la previsione che **triplica** il limite minimo e massimo delle sanzioni (nel limite di 5.000.000€) nel caso in cui le violazioni riguardino sistemi di certificazione rilasciati, tra l'altro, nell'ambito di un servizio erogato da un "**soggetto essenziale**". Tale nozione viene definita attraverso un rinvio esplicito all'**articolo 6**, **comma 1**, del decreto legislativo n. 138 del 2024 (recepimento della direttiva (UE) 2022/2555 – c.d. NIS 2 -, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione). La relazione illustrativa evidenzia come tale novella sia necessaria ad adeguare pienamente la normativa al contenuto della direttiva NIS 2. In particolare, la relazione osserva che la normativa attualmente vigente rinvia al decreto legislativo 18 maggio 2018, n. 65 (attualmente abrogato) che recepiva la direttiva NIS 1 (Direttiva UE 2016/1148). Per approfondimenti sulla nozione di "**soggetti essenziali**" si rinvia al seguente dossier.

- la **lettera g)** novella in più punti l'**articolo 13** del decreto legislativo n. 123 del 2022. Nello specifico:

1. viene novellato il **comma 1** dell'articolo che definisce la destinazione dei proventi derivanti dalle **tariffe** relative allo svolgimento delle attività di vigilanza, certificazione, autorizzazione e di abilitazione dell'ACN. La normativa vigente prevede che tali proventi siano versati su un apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del MEF, sul pertinente capitolo dello stato di previsione della spesa del medesimo ministero al fine di

incrementare la dotazione degli appositi capitoli dell'ACN. La modifica che il presente schema di decreto legislativo intende apportare prevede che i proventi riassegnati con decreto del MEF confluiscano, invece, nel capitolo dello stato di previsione della spesa di cui all'**articolo 18** del decreto legge n. 82 del 2021. Tale articolo prescrive che il citato capitolo serva a finanziare l'organizzazione e il funzionamento dell'ACN (articoli da **5** a **7** del decreto-legge). Attualmente, il citato **articolo 18** assegna a tale capitolo una dotazione di **110.000.000 euro** per l'anno 2026 e **122.000.000 euro** annui a decorrere dall'anno 2027. A queste risorse vanno aggiunte quelle trasferite dalle amministrazioni le cui funzioni sono state compresse in seguito all'entrata in funzione dell'ACN. Tali risorse sono trasferite, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili delle singole amministrazioni.

La relazione annuale dell'ACN al Parlamento relativa al 2025, stimava in poco più di **124 milioni** di euro la propria dotazione per il 2026 e in poco più di **135 milioni** quella per il 2027 e il 2028. Si osservi che il disegno di legge di assestamento per il 2026 (A.C. 3006) all'esame delle Camere nel momento di pubblicazione di questo *dossier*, fissa in poco meno di **137 milioni di euro** (capitolo 1672) la somma da assegnare all'ACN senza rilevare mutamenti rispetto alle previsioni iniziali.

2. viene novellato il **comma 3**. La novella opera nella stessa direzione del punto precedente prevedendo che gli introiti derivanti dalle **sanzioni pecuniarie** di cui all'articolo 10 del decreto legislativo n. 123 del 2022 (vedi *supra*) siano versati nel medesimo capitolo dello stato di previsione della spesa di cui all'**articolo 18** del decreto legge n. 82 del 2021. La novella, inoltre, specifica che tali introiti debbano essere destinati alle attività di ricerca e formazione concernenti la certificazione della *cybersicurezza* di prodotti TIC, servizi TIC, processi TIC o **servizi di sicurezza gestiti**.

Articolo 2
(Modifiche all'articolo 35 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82)

L'**articolo 2** apporta modifiche all'articolo 35, commi 4 e 5, del decreto legislativo n. 82/2005, cd. codice dell'amministrazione digitale (CAD), in materia di dispositivi sicuri e procedure per la generazione della firma qualificata.

L'**articolo 2** modifica l'**articolo 35** del **decreto legislativo n. 82/2005**, il quale reca il codice dell'amministrazione digitale (CAD).
Una prima modifica incide sul comma 4 del citato articolo 35 del CAD.
Il **previgente comma 4** dell'articolo 35 statuiva che i dispositivi sicuri di firma dovessero essere dotati di certificazione di sicurezza ai sensi dello **schema nazionale** (di cui al successivo comma 5).
Tale previsione è divenuta obsoleta con l'intervenuta attuazione del regolamento UE n. 881 del 2019 (cd. *Cybersecurity Act*) per mezzo del regolamento di esecuzione UE n. 482 del 2024.
Da siffatta normativa dell'Unione europea consegue che tutti i sistemi nazionali di certificazione della cybersicurezza, nonché le procedure correlate per i prodotti e i processi TIC, cessino di produrre effetti decorsi dodici mesi dall'entrata in vigore del citato regolamento n. 482.
Pertanto lo schema nazionale di certificazione, di cui tratta la disposizione, ha cessato di produrre i suoi effetti (il 27 febbraio 2026). Gli subentra lo **schema europeo di certificazione della cybersicurezza**.
La nuova formulazione prevede così che le certificazioni di sicurezza richieste siano quelle previste dall'**articolo 30** del **regolamento eIDAS.**

Il regolamento europeo n. 910/2014, cd. regolamento eIDAS (*Electronic IDentification, Authentication and trust Services*) mira a fornire una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni, onde incrementare la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di *e-business* e commercio elettronico nell'Unione Europea.
L'articolo 30 del regolamento eIDAS disciplina la certificazione dei dispositivi per la creazione di una firma elettronica qualificata.
I paragrafi 1 e 2 stabiliscono che siano gli Stati a designare gli organismi, pubblici o privati, idonei a certificare la conformità dei dispositivi e a notificarne nomi e indirizzi alla Commissione. Quest'ultima è tenuta a diffondere tali informazioni agli altri Stati membri.

Il paragrafo 3 elenca i due elementi alternativi su cui si basa la certificazione di conformità:

a) un processo di valutazione di sicurezza, condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici;

b) un processo diverso da quello di cui alla lettera *a)*, a condizione che utilizzi livelli di sicurezza comparabili e che l'organismo di cui al paragrafo 1 notifichi tale processo alla Commissione. Detto processo può essere utilizzato solo in assenza delle norme di cui alla lettera *a)*, ovvero quando è in corso un processo di valutazione di sicurezza di cui alla medesima lettera.

Mediante atti di esecuzione, prosegue il paragrafo 3, la Commissione adotta un elenco di norme per la valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui alla lettera *a)*.

Il paragrafo 4, infine, conferisce alla Commissione il potere di adottare atti delegati riguardanti la fissazione di criteri specifici che gli organismi designati debbono soddisfare.

In attuazione del paragrafo 4 dell'articolo 30 del regolamento eIDAS, la Commissione ha adottato la decisione di esecuzione n. 650/2016, del 25 aprile 2016.

Nell'Allegato della decisione sono elencate le norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione, applicabili alla certificazione dei dispositivi per la creazione di una firma o un sigillo elettronici qualificati.

Tali norme corrispondono ai cd. *common criteria*: criteri comuni alla base del sistema europeo di certificazione della cybersicurezza (EUCC), adottato con regolamento europeo di esecuzione n. 482/2024 della Commissione del 31 gennaio 2024.

Un secondo, correlato novero di modifiche incide sul **comma 5** del citato articolo 35 del CAD, onde espungere ancora una volta il richiamo dello schema nazionale per la valutazione e la certificazione di sicurezza nel settore della tecnologia dell'informazione.

Il comma 5 riformulato mantiene la previsione del testo previgente che la conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma elettronica qualificata o di un sigillo elettronico (quali prescritti dall'Allegato II del regolamento eIDAS) sia accertata dall'**Organismo di Certificazione della Sicurezza Informatica (OCSI)**.

L'OCSI è stato istituito dal decreto del Presidente del Consiglio dei ministri del 30 ottobre 2003 (il quale al contempo definiva lo schema nazionale di certificazione). Opera presso l'Agenzia Nazionale per la Cybersicurezza, in

seguito al trasferimento di competenze in materia di certificazione della cybersicurezza dal Ministero dello sviluppo economico all'Agenzia, previsto dall'articolo 7, lettera *e)* del decreto-legge n. 82 del 2021.

Articolo 3
(Modifiche all'articolo 7 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)

L'**articolo 3** novella il testo dell'articolo 7, comma 1, lettera *e)* del decreto legislativo n. 82/2021 (articolo recante la disciplina delle funzioni dell'Agenzia per la cybersicurezza nazionale).

L'**articolo 3** apporta due distinte modifiche all'articolo 7, comma 1, lettera *e)* del **decreto-legge n. 82/2021**.
È l'articolo che disciplina le funzioni dell'Agenzia per la cybersicurezza nazionale (istituita da quel medesimo decreto-legge).
Al comma 1, lettera *e)* stabilisce, in particolare, che l'Agenzia sia l'autorità nazionale di certificazione della cybersicurezza (*National Cybersecurity Certification Authority - NCCA*), ai sensi dell'articolo 58 del regolamento europeo n. 881/2019.

La prima modifica prevede che l'Agenzia per la cybersicurezza nazionale **autorizzi** le strutture specializzate del Ministero della difesa e del Ministero dell'interno, quali organismi di valutazione della conformità per i sistemi europei di certificazione della cybersicurezza.
Siffatta riformulazione esplicita (rispetto al testo fin qui vigente) come l'Agenzia per la cybersicurezza nazionale *non* espleti funzioni di accreditamento, non rientrando tra gli organismi nazionali di accreditamento previsti dal regolamento europeo n. 765/2008.
Altresì prevede che le **strutture specializzate del Ministero della difesa e del Ministero dell'interno stabiliscano requisiti specifici o supplementari**. Questo, a norma dell'articolo 54, paragrafo 1, lettera *f)*, del regolamento n. 881 del 2019.

L'articolo 60, paragrafo 3, del regolamento europeo n. 881/2019 prevede che, qualora i sistemi europei di certificazione della cybersicurezza stabiliscano requisiti specifici o supplementari, solo gli organismi di valutazione della conformità che soddisfino tali requisiti siano autorizzati dall'autorità nazionale di certificazione a svolgere i compiti previsti.
L'articolo 54 del medesimo regolamento individua gli elementi minimi propri dei sistemi europei di certificazione della cybersicurezza.
Tra questi, il paragrafo 1, lettera *f)*, prevede l'indicazione dei requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione

della conformità, al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cybersicurezza.
Si è nell'ambito delle disposizioni del regolamento UE n. 881/2019 noto come *Cybersecurity Act*, vale a dire la normativa europea che stabilisce un quadro comune per la sicurezza informatica.
Esso definisce il mandato permanente dell'ENISA (Agenzia dell'Unione europea per la cybersicurezza) che è stata dotata di maggiori poteri e risorse per prevenire e gestire le crisi informatiche a livello transfrontaliero, supportando operativamente gli Stati membri.
Inoltre, il regolamento istituisce il primo sistema europeo di certificazione per *hardware e software ICT* (*Information and Communication Technology*), al fine di creare un quadro normativo armonizzato, tale da certificare il livello di sicurezza di un qualsiasi prodotto, servizio o processo *ICT*.
L'articolo 56, paragrafo 6, del medesimo regolamento prevede che, ove un sistema europeo di certificazione della cybersicurezza, adottato a norma dell'articolo 49, richieda un livello di affidabilità 'elevato', il certificato europeo di cybersicurezza nell'ambito di tale sistema debba essere rilasciato solo da un'autorità nazionale di certificazione della cybersicurezza oppure, in casi specifici, da un organismo di valutazione della conformità.
L'articolo 60, invece, definisce il ruolo degli organismi di valutazione della conformità. I *Conformity Assessment Bodies* (*CABs*) sono enti terzi chiamati a verificare se prodotti, processi, servizi o sistemi rispettino i requisiti richiesti dalle normative tecniche, dagli *standard* internazionali e dalle direttive europee.
Essi sono organismi notificati cui i Paesi dell'Unione Europea affidano l'incarico di valutare la conformità di determinati prodotti prima che siano immessi sul mercato. Si precisa che solo gli organismi notificati ai sensi del diritto europeo possono rilasciare certificati di conformità per i prodotti armonizzati ed esclusivamente nel settore per il quale sono notificati.
L'articolo 58, inoltre, impone agli Stati membri di designare una o più autorità nazionali di certificazione della cybersicurezza.
La disposizione propone un lungo elenco di attività e poteri propri dell'Autorità. Tale organismo indipendente ha il compito di vigilare sul mercato, applicare le regole di conformità, supervisionare e far applicare le regole previste nei sistemi europei di certificazione della cybersicurezza, per il controllo della conformità dei prodotti, dei servizi e dei processi *ICT*, condurre indagini, adottare misure appropriate e chiedere informazioni agli organismi di valutazione della conformità e ai titolari di certificati europei della cybersicurezza.

La seconda, correlata modifica precisa che le strutture specializzate dei Ministeri richiamati siano **accreditate** ai sensi dell'articolo 60, paragrafo 1, del regolamento europeo n. 881/2019.
La disposizione incisa delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del *Cybersecurity Act*, il Ministero della difesa e il Ministero dell'interno al rilascio del certificato europeo di sicurezza cibernetica.
Ebbene, il rilascio avviene mediante le rispettive strutture accreditate, di cui all'articolo 60, paragrafo 1, del citato regolamento europeo n. 881/2019.

L'articolo 56, paragrafo 6, lettera *b)*, del regolamento europeo n 881/2019 stabilisce che, ove un sistema europeo di certificazione della cybersicurezza richieda un livello di affidabilità 'elevato', il certificato europeo di cybersicurezza debba essere rilasciato da un organismo di valutazione della conformità, sulla base di una delega rilasciata dall'autorità nazionale di certificazione della cybersicurezza.
L'articolo 60, paragrafo 1, attiene agli organismi di valutazione della conformità. Essi sono accreditati da organismi nazionali di accreditamento, designati ai sensi del regolamento europeo n. 765/2008. Il rilascio dell'accreditamento è subordinato al soddisfacimento dei requisiti, indicati nell'allegato del presente regolamento, da parte degli stessi organismi di valutazione della conformità.

Decreto-legge n. 82/2021, convertito, con modificazioni, dalla legge n. 109/2021	
Testo previgente	**Modificazioni apportate dall'art. 3 dell'AG 422**
Art. 7, comma 1, lettera *e)* *(Funzioni dell'Agenzia per la cybersicurezza nazionale)*	Art. 7, comma 1, lettera *e)* *(Funzioni dell'Agenzia per la cybersicurezza nazionale)*
L'Agenzia […] *e)* è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:	L'Agenzia […] *e)* è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

Decreto-legge n. 82/2021, convertito, con modificazioni, dalla legge n. 109/2021	
Testo previgente	**Modificazioni apportate dall'art. 3 dell'AG 422**
1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;	1) **autorizza**, ai sensi dell'articolo 60, paragrafo **3**, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi **europei di certificazione della cybersicurezza che stabiliscono requisiti specifici o supplementari a norma dell'articolo 54, paragrafo 1, lettera *f)*, del citato regolamento (UE) 2019/881;**
2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente legge, al rilascio del certificato europeo di sicurezza cibernetica;	2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate **ai sensi dell'articolo 60, paragrafo 1, del citato regolamento (UE) 2019/881**, al rilascio del certificato europeo di sicurezza cibernetica; […]

Articolo 4
(Clausola di invarianza finanziaria)

L’**articolo 4** reca una clausola di invarianza finanziaria.

L’articolo 4 stabilisce che le amministrazioni interessate provvedano all’attuazione delle disposizioni contenute nel presente provvedimento con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, **senza nuovi o maggiori oneri a carico della finanza pubblica**.

LE RECENTI INIZIATIVE LEGISLATIVE DELL'UNIONE EUROPEA IN MATERIA DI CYBERSICUREZZA

(a cura del Servizio per i Rapporti con l'Unione europea della Camera dei deputati)

Lo schema di decreto legislativo in esame interviene per adeguare l'ordinamento nazionale alle disposizioni del regolamento (UE) 2025/37 che modifica il regolamento (UE) 2019/881 (*c.d.* ***Cybersecurity Act***) al fine di estendere il sistema europeo di certificazione della cibersicurezza ai servizi di sicurezza gestiti.

Il **quadro normativo dell'Unione** in materia di cibersicurezza è tuttavia **oggetto di revisione** in quanto, nel più ampio processo di rafforzamento della resilienza digitale, la Commissione europea ha presentato un pacchetto di misure finalizzate a rendere la cibersicurezza una **leva** per la **protezione** delle **catene di approvvigionamento** e il **consolidamento** dell'**autonomia** strategica dell'Unione. Il pacchetto comprende:

- una proposta di regolamento volta all'abrogazione del regolamento (UE) 2019/881 e all'adozione di un ***Cybersecurity Act* 2.0**;
- una proposta di direttiva che **modifica** la **direttiva NIS 2** per quanto riguarda le misure di semplificazione e l'allineamento al ***Cybersecurity Act* 2.0**.

Presso la **Camera**, le proposte sono state esaminate, ai fini della verifica di conformità al principio di sussidiarietà, dalla **Commissione Politiche dell'UE** che ha adottato, il 6 maggio 2026, un documento recante una **valutazione conforme**, pur rilevando che la proposta di regolamento è solo parzialmente conforme al principio di proporzionalità.

Il nuovo ***Cybersecurity Act 2.0*** si articola intorno a **tre assi portanti**:

1) il **rafforzamento** dell'efficacia e la **semplificazione** della **certificazione** europea di **cibersicurezza**;
2) una **definizione** più **netta** della **relazione** tra i processi di **certificazione** e i **rischi di natura non tecnica**, con particolare riferimento alla sicurezza delle catene di approvvigionamento;
3) la **riorganizzazione** del **mandato** dell'Agenzia dell'UE per la cibersicurezza (**ENISA**) per incrementarne le funzioni di supporto operativo e di fornitura di servizi, eliminando ogni possibile incertezza interpretativa sulle sue mansioni.

Tra le modifiche che coinvolgono i servizi di sicurezza gestiti si segnala, in particolare, il nuovo articolo 85 che, al paragrafo 9, **stabilisce** il **divieto**, per i **servizi di sicurezza gestiti** in possesso di certificati europei di cibersicurezza **identificati**, interamente o in parte, come **risorsa chiave**, ai sensi del nuovo articolo 102, di **utilizzare**, **installare** o **integrare** in altro modo **componenti TIC** (tecnologie dell'informazione e della comunicazione) o componenti che comprendono componenti TIC **di fornitori** considerati **ad alto rischio**.
Per ulteriori approfondimenti sulle misure previste dal pacchetto si veda il dossier predisposto dal Servizio RUE.