COMMISSIONI RIUNITE

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

S O M M A R I O

ATTI DEL GOVERNO:

Schema di decreto legislativo recante 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 n. 422 *(Seguito dell'esame, ai sensi dell'articolo 143, comma 4, del regolamento, e conclusione – Parere favorevole)* 15

ALLEGATO 1 (Parere approvato) 17

ALLEGATO 2 (Proposta alternativa di parere del Gruppo MoVimento 5 Stelle) 18

ATTI DEL GOVERNO

Mercoledì 29 luglio 2026. — Presidenza del presidente della IX Commissione, Salvatore DEIDDA. – Interviene la sottosegretaria di Stato per i rapporti con il Parlamento, Giuseppina Castiello.

La seduta comincia alle 15.25.

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 n. 422.

(Seguito dell'esame, ai sensi dell'articolo 143, comma 4, del regolamento, e conclusione – Parere favorevole).

Le Commissioni proseguono l'esame dello schema di decreto, rinviato nella seduta del 22 luglio 2026.

Salvatore DEIDDA, *presidente*, avverte che il gruppo PD-IDP ha chiesto che la pubblicità dei lavori sia assicurata anche attraverso il sistema di ripresa audiovideo a circuito chiuso. Non essendovi obiezioni, ne dispone l'attivazione.

Ricorda che nella seduta del 22 luglio 2026 è stata svolta la relazione introduttiva.

Avverte, inoltre, che la Commissione Bilancio ha espresso, in data odierna, una valutazione favorevole sullo schema di decreto in esame.

Enzo AMICH (FDI), *relatore per la IX Commissione*, anche a nome del relatore per la I Commissione, onorevole De Corato, formula una proposta di parere favorevole *(vedi allegato 1)*.

Salvatore DEIDDA, *presidente*, avverte che il Gruppo MoVimento 5 Stelle ha presentato una proposta alternativa di parere *(vedi allegato 2)*.

La sottosegretaria Giuseppina CASTIELLO condivide la proposta di parere formulata dai relatori.

Antonino IARIA (M5S) illustra la proposta alternativa di parere presentata dal proprio gruppo, evidenziando le criticità dell'articolo 3 con particolare riguardo al ruolo dell'Agenzia per la cybersicurezza nazionale (ACN). Osserva, in particolare, che lo schema di decreto in esame sembra implementarne le funzioni, senza tuttavia attribuirle un effettivo rafforzamento dei poteri di vigilanza e sanzionatorio. Rileva, pertanto, una discrasia tra l'ampliamento formale delle competenze e l'effettiva capacità dell'Agenzia di esercitare le proprie funzioni.

Rileva, quindi, ulteriori profili di criticità nello schema di decreto all'esame delle Commissioni, soffermandosi anzitutto sul possibile conflitto di interessi derivante dal fatto che i soggetti istituzionali maggiormente coinvolti nell'acquisizione dei servizi, ossia il Ministero della difesa e il Ministero dell'interno, risultano anche competenti a valutarne e certificarne i fornitori.

Evidenzia, inoltre, i rischi per la competitività della filiera industriale nazionale, osservando che una disciplina difforme rispetto a quella adottata dagli altri Stati membri dell'Unione europea potrebbe indurre le imprese italiane a conseguire la certificazione presso autorità estere.

Illustra, infine, le principali modifiche proposte dal proprio gruppo nella proposta alternativa di parere, le quali prevedono che le attività di accreditamento e rilascio delle certificazioni restino attribuite all'ACN, che le strutture specializzate dei Ministeri della difesa e dell'interno limitino le valutazioni di conformità ai sistemi di rispettiva competenza, che non possano essere introdotti requisiti ulteriori rispetto a quelli previsti dalla normativa europea e che i requisiti e le procedure siano pubblici, fatti salvi i soli casi strettamente necessari alla tutela della sicurezza nazionale.

Nessun altro chiedendo di intervenire, le Commissioni approvano la proposta di parere favorevole dei relatori *(vedi allegato 1)*.

Salvatore DEIDDA, *presidente*, avverte che, essendo stata approvata la proposta di parere dei relatori, la proposta alternativa di parere del gruppo MoVimento 5 Stelle risulta preclusa e non sarà pertanto posta in votazione.

La seduta termina alle 15.30.

ALLEGATO 1

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 n. 422.

PARERE APPROVATO

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

esaminato lo 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 n. 422);

condivise le finalità del provvedimento, volto a dare attuazione alla delega conferita al Governo dall'articolo 16 della legge n. 36 del 2026, ai fini dell'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 (cosiddetto CSA-*cybersecurity act*) con riguardo ai servizi di sicurezza gestiti, ossia ai servizi prestati a terzi consistenti nello svolgimento di attività legate alla gestione dei rischi del cliente in materia di sicurezza informatica;

considerato che l'articolo 1, che reca modifiche al decreto legislativo n. 123 del 2022, introduce la definizione di servizio di sicurezza gestito, riproducendo quella prevista dal regolamento (UE) 2025/37, ed estende a tali servizi la normativa europea in materia di certificazioni di sicurezza, comprese le attività di controllo e vigilanza sull'emissione delle stesse;

considerato, altresì, che il medesimo articolo 1 modifica la disciplina dei poteri sanzionatori e inibitori dell'Agenzia per la cybersicurezza nazionale (ACN), nonché quella relativa alle attività di vigilanza del mercato, prevedendo che l'Agenzia, per il tramite dell'Organismo di certificazione della sicurezza informatica (OCSI), possa rilasciare anche certificati di livello sostanziale e base, oltre a revocarli qualora accerti l'emissione di certificati non conformi;

preso atto che l'articolo 2, novellando l'articolo 35 del codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005, elimina i riferimenti allo schema nazionale per la valutazione e la certificazione della sicurezza nel settore delle tecnologie dell'informazione, in considerazione del fatto che tale sistema ha cessato di produrre effetti dal 27 febbraio 2026, a seguito dell'adozione dello schema europeo di certificazione della cybersicurezza previsto dal regolamento di esecuzione UE n. 482 del 2024;

preso, altresì, atto che l'articolo 3 modifica l'articolo 7 del decreto-legge n. 82 del 2021, concernente le funzioni dell'Agenzia per la cybersicurezza nazionale (ACN), prevedendo che l'Agenzia 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, mentre l'articolo 4 reca la clausola di invarianza finanziaria riferita all'attuazione del provvedimento,

esprimono

PARERE FAVOREVOLE.

ALLEGATO 2

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 n. 422.

PROPOSTA ALTERNATIVA DI PARERE DEL GRUPPO MOVIMENTO 5 STELLE

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

esaminato lo 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 n. 422);

premesso che:

lo schema di decreto legislativo in esame attua la delega disposta dall'articolo 16 della legge n. 36 del 2026 (legge di delegazione europea per il 2025), il quale recava 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, concernente i servizi di sicurezza gestiti;

secondo la definizione data dalla richiamata normativa unionale (articolo 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 »;

l'obiettivo del Governo è quello di adeguare l'ordinamento italiano alla predetta disciplina europea, estendendo ai servizi di sicurezza gestiti il sistema europeo di certificazione della cybersicurezza;

attualmente, la normativa nazionale rilevante in materia è rappresentata dal decreto legislativo n. 123 del 2022, recante norme di adeguamento della normativa nazionale alle disposizioni in materia 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;

l'articolo 1 modifica il vigente decreto legislativo n. 123 del 2022, che disciplina i servizi di sicurezza gestiti, adottando per i servizi di sicurezza gestiti la stessa definizione data dalla normativa europea e inserisce i servizi di sicurezza gestiti tra quei servizi che devono essere conformi ai requisiti stabiliti dal quadro europeo di certificazione e non pregiudicare la salute, la sicurezza o qualsiasi altro aspetto volto a garantire la protezione del pubblico interesse;

l'articolo 2 apporta modifiche tecniche e procedurali al decreto legislativo n. 82 del 2005, cosiddetto codice dell'amministrazione digitale (CAD), in materia di dispositivi sicuri e procedure per la generazione della firma qualificata;

l'articolo 3 apporta modifiche determinanti per la *governance* dei sistemi di sicurezza gestiti, delle procedure di accre-

ditamento e sulla certificazione: attualmente, infatti, l'ACN è l'autorità nazionale di certificazione della cybersicurezza, ma con la modifica introdotta dallo schema di decreto in esame cessa di esserlo per trasformarsi nell'organismo che accredita le strutture specializzate dei Ministeri della difesa e dell'interno, i quali diventano *tout court* organismi di valutazione della conformità per i sistemi europei di certificazione della cybersicurezza – nel testo attualmente vigente i due dicasteri sono, sì, organismi di valutazione della conformità, ma solo per i sistemi di rispettiva competenza – in più, ACN delega le strutture specializzate del Ministero della difesa e del Ministero dell'interno al rilascio del certificato europeo di sicurezza cibernetica e anche a stabilire requisiti specifici o supplementari rispetto a quelli stabiliti dalla disciplina UE;

preme ribadire che le strutture specializzate dei due dicasteri non rappresentano una novità, ma nella disciplina attualmente vigente è (era) l'ACN ad accreditarle per svolgere funzioni di valutazione di conformità – per i soli settori di competenza – mentre ora l'ACN si spoglia delle funzioni di valutazione e conformità dei requisiti dei servizi in parola e l'ambito di competenza dei dicasteri viene ampliato fino a ricomprendere tutto il sistema di certificazione dei sistemi di sicurezza gestiti in generale, cui si aggiunge la possibilità di introdurre nuovi e supplementari requisiti, anche specifici;

preme rappresentare che i due dicasteri ai quali vengono attribuite le funzioni di valutazione della conformità sono, al tempo stesso, tra i principali committenti di servizi di sicurezza gestiti sul mercato nazionale: il medesimo soggetto acquista i servizi, ne valuta la conformità, ne rilascia la certificazione e può definirne requisiti supplementari, in contrasto con il principio di separazione tra controllore e controllato che informa l'intero quadro europeo di certificazione della cybersicurezza;

criticità in ordine al riassetto della *governance* e, in particolare, l'intreccio di competenze tra l'ACN, il Ministero della difesa e il Ministero dell'interno, erano già state sollevate in modo trasversale da esperti del settore tecnologico, associazioni di categoria, operatori economici di settore, esperti e giuristi in occasione della richiamata legge di delegazione europea;

forte preoccupazione è stata espressa da parte del mondo imprenditoriale:

il regolamento (UE) 2025/37 individua espressamente tra le proprie finalità quella di agevolare l'ingresso nel mercato e di semplificare, per quanto possibile, gli oneri normativi, amministrativi e finanziari a carico dei fornitori, in particolare delle piccole e medie imprese e delle microimprese, nonché di garantire l'accessibilità dei servizi di sicurezza gestiti agli attori di dimensioni ridotte e alle autorità locali e regionali dotate di capacità e risorse limitate; la scelta di articolare l'accreditamento e la certificazione su filiere amministrative distinte produce l'effetto opposto, moltiplicando gli oneri proprio per i soggetti che il regolamento intende tutelare, tra i quali rientrano i comuni, le aziende sanitarie e gli enti territoriali, oggi tra i più esposti agli attacchi informatici;

nonché a causa del rischio di:

doppie/plurime procedure: gli operatori temono che la suddivisione delle competenze per i requisiti di accreditamento e certificazione costringa i *provider* privati a doversi interfacciare con filiere amministrative diverse (quella civile/regolatoria di ACN e quelle dell'amministrazione dei Ministeri della difesa e dell'interno);

rallentamento del mercato: un impianto di certificazione eccessivamente burocratizzato, gestito da Ministeri con logiche di stampo militare o di ordine pubblico, rischia di penalizzare le PMI e rallentare l'adozione delle misure di sicurezza previste dal regolamento (UE) 2025/37;

i provvedimenti di diniego, sospensione o revoca del certificato incidono direttamente sulla possibilità di operare sul mercato: ove adottati sulla base di requisiti

coperti da vincoli di riservatezza, essi risultano difficilmente sindacabili in sede giurisdizionale, con conseguente compressione del diritto di difesa delle imprese interessate e rischio di contenzioso sistematico sugli atti di certificazione;

esperti di diritto e analisti di *governance* geopolitica, hanno evidenziato criticità di tipo strutturale:

la scelta unionale con il *Cybersecurity Act* punta alla standardizzazione del mercato unico digitale, che è per sua natura civile ed economico, spostare la gestione operativa e di valutazione verso la difesa e l'interno rischia di « militarizzare » l'ecosistema *cyber* nazionale;

le recenti evoluzioni normative che tendono a ridistribuire la gestione delle crisi informatiche gravi tra il Ministero della difesa e il Dipartimento delle Informazioni per la Sicurezza (DIS) creano una potenziale « zona grigia » di competenze – diventa complesso tracciare una linea netta tra ciò che inerisce la resilienza, anche economica, di competenza ACN, e ciò che è minaccia alla sicurezza nazionale (ambito della difesa e dell'interno);

la costruzione di una filiera nazionale di certificazione difforme da quella adottata negli altri Stati membri rischia di incidere sulla circolazione dei certificati rilasciati in Italia e di spingere i fornitori nazionali a certificarsi in altri Paesi dell'Unione europea, con un effetto di delocalizzazione della certificazione che contraddice l'obiettivo di rafforzamento dell'autonomia tecnologica nazionale;

infine, si rilevano:

l'allentamento del principio di « interfaccia unico » richiesto e raccomandato dall'Europa (*Single point of Contact*) per non frammentare il mercato interno della cybersicurezza, mentre ora, con lo schema di decreto in esame, *governance* e funzioni vengono « distribuite », in maniera neppure chiara, tra ACN, Ministero della difesa e Ministero dell'interno – ACN mantiene tutte le funzioni attinenti, per esempio, al settore della cosiddetta resilienza, acquisisce quelle sulla sicurezza informatica (articolo 1 dello schema di decreto) e sull'introduzione di sistemi di certificazione nazionali di cybersicurezza, per i servizi di sicurezza gestiti sia « di base » che di livello elevato (articolo 1) nonché l'attività di vigilanza, controllo e sanzionatoria, ma dismette l'attività di accreditamento e di certificazione di « certi » servizi;

l'indebolimento del ruolo di ACN: l'Agenzia, nata per essere l'autorità unica e indipendente sul modello dell'omologa Autorità francese, vede progressivamente svuotate o frammentate le proprie prerogative operative a favore delle amministrazioni di dicasteri (di dicasteri « pesanti »);

carenza di trasparenza: c'è il rischio che i requisiti di sicurezza e le procedure di conformità, se gestiti sotto l'egida della difesa o dell'interno, finiscano per essere coperti da clausole o vincoli di segretezza e riservatezza, riducendo la trasparenza delle attività nel mercato della cybersicurezza;

alla luce delle considerazioni suesposte e rilevato, altresì, che un corretto adeguamento alla disciplina europea avrebbe richiesto di mantenere in capo all'Agenzia per la cybersicurezza nazionale le funzioni di accreditamento e di rilascio dei certificati, di riservare alle strutture specializzate del Ministero della difesa e del Ministero dell'interno la valutazione della conformità per i soli sistemi di rispettiva competenza, di escludere la facoltà di stabilire requisiti supplementari rispetto a quelli europei e di garantire la pubblicità dei requisiti di sicurezza e delle procedure di conformità, salvo quanto strettamente necessario alla tutela della sicurezza nazionale,

esprimono

PARERE CONTRARIO.

Alfonso Colucci, Iaria, Auriemma, Baldino, Penza, Barzotti, Fede.