dossier

XIX Legislatura

Luglio 2024

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

Atto del Governo n. 164

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO DEL BILANCIO
Tel. 06 6706 5790 – ✉ SBilancioCU@senato.it – 𝕏 @SR_Bilancio
Nota di lettura n. 163

Camera dei deputati

SERVIZIO BILANCIO DELLO STATO
Tel. 06 6760 2174 / 9455 – ✉ bs_segreteria@camera.it
Verifica delle quantificazioni n. 226

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

INDICE

INFORMAZIONI SUL PROVVEDIMENTO

Natura dell'atto:	Schema di decreto legislativo	
Atto del Governo n.	164	
Titolo breve:	Misure per un livello comune elevato di cibersicurezza nell'Unione	
Riferimento normativo:	Articoli 1 e 3 della legge 21 febbraio 2024, n. 15	
Relazione tecnica (RT):	Presente	
	Senato	**Camera**
Commissione competente:	5ª (Bilancio) *in sede consultiva* 1ª (Affari Costituzionali), 8ª (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) *in sede consultiva* 4ª (Politiche dell'Unione europea) *in sede osservazioni*	I (Affari costituzionali) e IX (Trasporti) riunite V Bilancio e Tesoro XIV Politiche dell'Unione Europea

PREMESSA

Lo schema di decreto legislativo A.G. 164 è diretto al recepimento della direttiva dell'Unione europea n. 2555 del 2022 (c.d. direttiva NIS 2) relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea.

Lo schema, che si compone di 6 Capi e 44 articoli, dispone l'abrogazione del D.Lgs. n. 65 del 2018 di recepimento della prima direttiva NIS *Network and Information Security*, di cui la direttiva NIS 2 dispone l'abrogazione a decorrere dal 18 ottobre 2024 e di alcune disposizioni (articoli 40 e 41) del D.Lgs. n. 259 del 2003 recante "Codice delle comunicazioni elettroniche", prevedendo una fase transitoria fino all'emanazione dei provvedimenti attuativi del decreto.

La direttiva (UE) 2022/2555 pone come termine per il suo recepimento il 17 ottobre 2024. A tal fine, la legge 21 febbraio 2024, n. 15 (legge di delegazione europea 2022-2023), oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, stabilisce, all'articolo 3, gli ulteriori princìpi e criteri direttivi specifici di delega assegnati al Governo per il suo recepimento.

Il comma 4 dell'articolo 31 della legge n. 234 del 2012 (Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea) prevede che gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della relazione tecnica di cui all'articolo 17, comma 3, della legge 31 dicembre 2009, n. 196. Su di essi è richiesto anche il parere delle Commissioni parlamentari competenti per i profili finanziari. Il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, ritrasmette alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

CAPO I
DISPOSIZIONI GENERALI

Articoli 1-8

L'articolo 1 afferma al comma 1 che il presente decreto stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno.

Il comma 2 si sofferma sui contenuti dello schema in cui si prevede:

a) la Strategia nazionale di cybersicurezza, recante previsioni volte a garantire un livello elevato di sicurezza informatica;
b) l'integrazione del quadro di gestione delle crisi informatiche, nel contesto dell'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza, di cui all'articolo 10 del decreto-legge 4 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;
c) la conferma dell'Agenzia per la cybersicurezza nazionale quale: 1) Autorità nazionale competente NIS, disciplinandone i poteri inerenti all'implementazione e all'attuazione del presente decreto; 2) Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero; 3) Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia);
d) la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, ciascuno per gli ambiti di competenza indicati all'articolo 2, comma 1, lettera g), quali Autorità nazionali di gestione delle crisi informatiche su vasta scala, assicurando la coerenza con il quadro nazionale esistente in materia di gestione generale delle crisi informatiche, ferme restando le competenze del Nucleo per la cybersicurezza di cui all'articolo 9 del decreto-legge 14 giugno 2021, n. 82;
e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS;
f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;
g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del presente decreto, in particolare, attraverso la partecipazione nazionale a livello dell'Unione europea: 1) al Gruppo di cooperazione NIS tra autorità competenti NIS e tra punti di contatto unici degli Stati membri dell'Unione europea, nell'ottica di incrementare la fiducia e la collaborazione a livello unionale; 2) alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi cibernetiche su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione europea; 3) alla Rete di CSIRT nazionali nell'ottica di assicurare una cooperazione, sul piano tecnico, rapida ed efficace.

L'articolo 2 reca l'elencazione delle definizioni che si applicano ai fini del decreto in esame.

L'articolo 3, definisce l'ambito di applicazione del provvedimento, distinguendo i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sotto settori e tipi di soggetti di cui agli allegati I e II, le categorie delle pubbliche amministrazioni sottoposte alla nuova disciplina, di cui all'allegato III, e le ulteriori tipologie di soggetti a cui si applica il presente decreto, di cui all'allegato IV. Al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri, la disposizione introduce (ai commi 2, 3 e 4) il criterio di individuazione dei soggetti su

base dimensionale, estendendo, rispetto al sistema delineato dalla direttiva NIS, l'applicazione della direttiva NIS2 a tutte le medie e grandi imprese che operano nei settori di cui agli allegati I e II. Alcuni soggetti sono inclusi nell'ambito applicativo del presente schema di decreto indipendentemente dalla loro dimensione, come nel caso di quelli di cui ai commi 5, 9 e 10, delle pubbliche amministrazioni di cui all'allegato III e dei soggetti elencati nell'allegato IV[1].

L'articolo 4, chiarisce essenzialmente a quali ambiti lo schema di decreto legislativo non si applica.

In tal senso, il comma 1 prevede che il presente decreto lascia impregiudicata la responsabilità dello Stato italiano di tutelare la sicurezza nazionale e il suo potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

Il comma 2 stabilisce che i soggetti di cui all'articolo 3, commi 6 e 7, non ricomprendono il Parlamento italiano, l'Autorità giudiziaria, la Banca d'Italia e l'Unità di informazione finanziaria per l'Italia di cui all'articolo 6 del decreto legislativo 21 novembre 2007, n. 231. Agli Organi costituzionali e di rilievo costituzionale non si applicano le previsioni di cui al capo V.

Il comma 3 prevede che il presente decreto non si applica anche agli enti, gli organi e le articolazioni della pubblica amministrazione che operano nei settori: della pubblica sicurezza; della difesa nazionale; dell'attività di contrasto, compresa l'indagine, l'accertamento e il perseguimento, di reati; né ancora agli organismi d'informazione di sicurezza dello Stato e all'Agenzia per la cybersicurezza nazionale (ACN).

L'articolo 5 individua, sostanzialmente riproducendo il contenuto dell'articolo 26 della direttiva, i criteri per definire a quale giurisdizione siano assoggettati i soggetti, individuati dall'articolo 3, che rientrano nell'ambito di applicazione del presente provvedimento.

L'articolo 6 individua i soggetti "essenziali" e "importanti", in base ai requisiti dimensionali e alla tipologia di prodotti o servizi forniti.

Il comma 1 provvede alla individuazione dei soggetti che, ai fini del presente decreto, sono considerati soggetti "essenziali":

a) i soggetti di cui all'allegato I (ossia i soggetti presenti nei settori ad alta criticità: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC e spazio) che superano

[1] Quelli individuati all'allegato I come settori ad alta criticità sono i seguenti: Energia (comprensivo dei sotto settori dell'energia elettrica, del teleriscaldamento e tele raffrescamento, del petrolio, del gas e dell'idrogeno);Trasporti (comprensivo dei sotto settori del trasporto aereo, del trasporto ferroviario, del trasporto per vie d'acqua e del trasporto su strada);Settore bancario; Infrastrutture dei mercati finanziari; Settore sanitario; Acqua potabile; Acque reflue; Infrastrutture digitali; Gestione dei servizi TIC (business-to-business);Spazio. L'allegato II individua i seguenti quali altri settori critici: Servizi postali e di corriere; Gestione dei rifiuti; Fabbricazione, produzione e distribuzione di sostanze chimiche; Produzione, trasformazione e distribuzione di alimenti; Fabbricazione (comprensivo dei sotto settori della fabbricazione di dispositivi medici e di dispositivi medico diagnostici in vitro, della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche, della fabbricazione di macchinari e apparecchiature n.c.a., della fabbricazione di autoveicoli, rimorchi e semirimorchi e della fabbricazione di altri mezzi di trasporto):Fornitori di servizi digitali; Ricerca. Gli allegati III e IV descrivono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetti a cui si applica il decreto in esame. Secondo l'allegato III, rientrano nell'ambito di applicazione del decreto: le amministrazioni centrali, vale a dire: gli Organi costituzionali e di rilievo costituzionale; la Presidenza del Consiglio dei ministri e i Ministeri; le Agenzie fiscali; le Autorità amministrative indipendenti; le amministrazioni regionali, vale a dire le Regioni e le Province autonome; le amministrazioni locali, vale a dire: le Città metropolitane; i Comuni con popolazione superiore a 100.000 abitanti; i Comuni capoluoghi di regione; le Aziende sanitarie locali; altri soggetti pubblici, tra cui: gli Enti di regolazione dell'attività economica; gli Enti produttori di servizi economici; gli Enti a struttura associativa; gli Enti produttori di servizi assistenziali, ricreativi e culturali; gli Enti e le Istituzioni di ricerca;. gli Istituti zooprofilattici sperimentali. Gli ulteriori soggetti individuati all'allegato IV sono: i soggetti che forniscono servizi di trasporto pubblico locale; gli istituti di istruzione che svolgono attività di ricerca; i soggetti che svolgono attività di interesse culturale; le società in *house*, le società partecipate e le società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175.

i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) i soggetti identificati come soggetti critici ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni, che è attualmente all'esame delle Camere (A.G. 165).;
c) i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui all'articolo 3, comma 5, lettera b), che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato alla citata raccomandazione 2003/361/CE;
d) i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'articolo 3, comma 5, lettere c) e d), indipendentemente dalle loro dimensioni;
e) le pubbliche amministrazioni centrali di cui all'allegato III, lettera a), ossia gli Organi costituzionali e di rilievo costituzionale; la Presidenza del Consiglio dei ministri e i Ministeri; le Agenzie fiscali e le Autorità amministrative indipendenti, tutte indipendentemente dalle loro dimensioni.

Il comma 2 prevede che rientrano ancora nella categoria dei soggetti essenziali, indipendentemente dalle loro dimensioni, come individuati dall'Autorità nazionale competente NIS: le pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; i soggetti delle tipologie di cui all'allegato IV, ossia: soggetti che forniscono servizi di trasporto pubblico locale; istituti di istruzione che svolgono attività di ricerca; soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico; i soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; le imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti.

Il comma 3 individua, in via residuale, la categoria dei soggetti importanti, facendovi rientrare tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto che non sono considerati essenziali ai sensi dei commi 1 e 2 dell'articolo in esame.

L'articolo 7 prevede il procedimento con cui sono identificati i soggetti importanti ed essenziali.

In particolare, il comma 1 prevede che dal 1° gennaio al 28 febbraio di ogni anno successivo alla data di entrata in vigore del presente decreto, i soggetti di cui all'articolo 3, si registrano o aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni e attribuite all'Agenzia per la cybersicurezza nazionale anche ai sensi del presente decreto.

Il comma 2 stabilisce che entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, l'Autorità nazionale competente NIS, redige, secondo le modalità di cui all'articolo 40, comma 5, l'elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni di cui al comma 1 e delle decisioni adottate ai sensi degli articoli 3, 4, e 6.

Ai sensi del comma 3, tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS comunica ai soggetti registrati: l'inserimento nell'elenco dei soggetti essenziali o importanti; la permanenza nell'elenco dei soggetti essenziali o importanti; l'espunzione dall'elenco dei soggetti.

Il comma 4 stabilisce che dal 15 aprile al 31 maggio di ogni anno successivo alla data di entrata in vigore del presente decreto, tramite la piattaforma digitale di cui al comma 1, i soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere a) e b), forniscono o aggiornano alcune informazioni.

Il comma 5 prevede alcuni obblighi informativi nei confronti dell'ACN ai fornitori di servizi di sistema dei nomi di dominio; ai gestori di registri di nomi di dominio di primo livello; ai fornitori di servizi di registrazione dei nomi di dominio; a i fornitori di servizi di *cloud computing*; ai fornitori di servizi di *data center*; ai fornitori di reti di distribuzione dei contenuti; ai fornitori di servizi gestiti; ai

fornitori di servizi di sicurezza gestiti; ai fornitori di mercati *on line*; ai fornitori di motori di ricerca *on line*; ai fornitori di piattaforme di *social network*.

L'articolo 8 riguarda il trattamento dei dati personali e rinvia al riguardo al codice della *privacy* e alla legislazione dell'Unione europea in materia di trattamento dei dati personali e tutela della vita privata e comunicazioni elettroniche.

La RT dopo una premessa generale, evidenzia che lo schema di decreto legislativo, nel recepire e razionalizzare le disposizioni della direttiva, determina un complessivo ampliamento di compiti e attività, sia per l'Agenzia per la cybersicurezza nazionale (nel seguito ACN) che per le altre Amministrazioni coinvolte, rendendo necessario un corrispondente incremento del fabbisogno annuo di spesa, del quale viene fornita una puntuale quantificazione, avuto riguardo alle varie disposizioni contenute nello schema di decreto.

Evidenzia che il Capo I (articoli 1-8) reca disposizioni generali che non hanno diretti riflessi di natura finanziaria. In tal senso, segnala quanto segue.

L'articolo 1 definisce l'oggetto del presente decreto legislativo, confermando, al comma 2, lettera c), l'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, Punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente (CSIRT Italia) in ambito nazionale. Tali funzioni sono assolte mediante la dotazione annua assegnata all'ACN dall'articolo 18, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

L'articolo 2 contiene le definizioni più ricorrenti nel testo del presente decreto legislativo.

Sugli articoli 3-6, la RT rileva che le disposizioni definiscono l'ambito di applicazione, norme di principio in materia di protezione degli interessi nazionali e commerciali**,** regole in materia di giurisdizione e territorialità per l'applicazione del presente decreto legislativo di carattere ordinamentale e norme volte all' individuazione dei "soggetti essenziali ed importanti" in base ai requisiti dimensionali e alla tipologia di prodotti/servizi forniti, norme che non hanno riflessi finanziari.

Sull'articolo 7 ribadisce che l'articolo disciplina le modalità di identificazione dei soggetti di cui all'articolo 6. Ai sensi del comma 3, l'ACN sta ultimando lo sviluppo di una piattaforma digitale, che sarà operativa all'entrata in vigore del presente decreto, interamente finanziata dai fondi PNRR, nell'ambito della misura 1.5 "*Cybersecurity*".

Sull'articolo 8 segnala che la norma detta apposite misure di protezione dei dati personali e non ha riflessi di natura finanziaria.

Al riguardo, rinviando agli articoli successivi per quanto concerne l'incremento delle risorse per le autorità pubbliche interessate, con particolare riferimento all'articolo 7 si osserva che le disposizioni sembrerebbero richiedere un aggiornamento e un potenziamento delle dotazioni s*oftware* e *hardware* delle Amministrazioni pubbliche coinvolte negli adempimenti previsti, per cui andrebbero fornite rassicurazioni circa la

piena sostenibilità di tali compiti avvalendosi delle sole risorse previste dalla legislazione vigente nei propri bilanci.

In relazione al finanziamento da fondi PNRR[2] della piattaforma digitale sviluppata dall'Agenzia per la cybersicurezza nazionale, andrebbero approfonditi gli oneri di gestione e manutenzione che ne deriveranno indicando le risorse che potranno essere utilizzate per farvi fronte.

CAPO II
QUADRO NAZIONALE DI SICUREZZA INFORMATICA

Articoli 9-11

L'articolo 9 stabilisce che spetta alla Strategia nazionale di cybersicurezza individuare obiettivi, risorse, elementi e misure strategiche per raggiungere e mantenere un alto grado di tutela della sicurezza delle reti e dei sistemi di interesse nazionale; la norma dispone, altresì, le modalità di valutazione e aggiornamento della Strategia nazionale della cybersicurezza.

In particolare, il comma 1 stabilisce che la Strategia nazionale di cybersicurezza individua obiettivi, risorse e misure per raggiungere e mantenere un alto grado di tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

In base al comma 4, l'Agenzia per la cybersicurezza nazionale provvede ai sensi dell'articolo 7 del citato decreto-legge n. 82 del 2021, sentite le amministrazioni componenti il Nucleo per la cybersicurezza, alla periodica valutazione della Strategia nazionale di cybersicurezza, nonché al suo aggiornamento ove necessario e comunque almeno ogni cinque anni sulla base di indicatori chiave di prestazione, proponendone l'adozione al Presidente del Consiglio dei ministri.

L'articolo 10 stabilisce che l'Agenzia per la cybersicurezza nazionale è l'Autorità nazionale competente NIS di cui all'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555 e pertanto:

a) sovrintende all'implementazione e all'attuazione del presente decreto;

b) predispone i provvedimenti necessari a dare attuazione al presente decreto;

c) svolge le funzioni e le attività di regolamentazione di cui al presente decreto, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti;

d) individua i soggetti essenziali e i soggetti importanti ai sensi degli articoli 3 e 6, nonché redige l'elenco di cui all'articolo 7, comma 2;

e) partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555;

f) definisce gli obblighi di cui all'articolo 7, comma 6, e al capo IV;

---

[2] Nell'ultima relazione sull'attuazione del PNRR aggiornata alle risultanze al 31 dicembre 2023, in relazione alla misura M1C1 - Investimento 1.5: Cybersecurity si legge che "per l'investimento volto a rafforzare le difese dell'Italia in tema di cybersecurity, l'evoluzione dello scenario geopolitico e l'aumentato rischio *cyber* hanno suggerito di non limitare gli interventi di potenziamento della *cybersecurity* a specifici settori e di riformulare quindi gli ambiti di intervento (M1C1-19, T4-2024), facendo riferimento ai settori previsti dalla normativa nazionale e comunitaria, ivi inclusi quelli dell'assistenza sanitaria, dell'energia e dell'ambiente. Inoltre, data l'incertezza dei tempi relativi all'adozione degli schemi di certificazione europei (quali ad esempio, gli EUCS e EU5G, rispettivamente, per il *Cloud Computing* e per il 5G) attualmente in fase di negoziazione nel contesto delle disposizioni del regolamento 2019/881 (c.d. *Cyber Security Act*), è stato eliminato dal target M1C1-21 (T4-2024) il riferimento all'attivazione di un laboratorio di certificazione europeo.". Nell'ambito della Misura citata risultavano assegnati al Dipartimento per la trasformazione digitale della presidenza del Consiglio dei ministri 623 milioni di euro, di cui 52 milioni di euro di spesa effettivamente sostenuta al 31 dicembre 2023. Cfr. Ministero degli affari europei, il Sud, le politiche di coesione ed il PNRR, Quarta relazione sullo stato di attuazione del Piano Nazionale di Ripresa e Resilienza, 22 febbraio 2024, pagine 103 e 118.

g) svolge le attività ed esercita i poteri di vigilanza ed esecuzione di cui al capo V.

L'Agenzia per la cybersicurezza nazionale è il Punto di contatto unico NIS di cui all'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555, svolgendo una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità nazionali con le autorità pertinenti degli altri Stati membri, la Commissione e l'Agenzia dell'Unione europea per la cybersicurezza (ENISA).

Ai fini dell'attuazione del presente articolo è autorizzata la spesa pari a euro 2.000.000 annui a decorrere dall'anno 2025 a cui si provvede ai sensi dell'articolo 44.

L'articolo 11, al fine di assicurare l'efficace attuazione del presente decreto a livello settoriale, individua le Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa, secondo le modalità di cui all'articolo 40, comma 2, lettera c) del decreto medesimo.

Il comma 2 designa quali Autorità di settore NIS:

- a) la Presidenza del Consiglio dei ministri per:
    - il settore gestione dei servizi TIC, di cui al numero 9 dell'allegato I, in collaborazione con l'Agenzia per la cybersicurezza nazionale;
    - il settore dello spazio, di cui al numero 10 dell'allegato I;
    - il settore delle pubbliche amministrazioni, di cui all'articolo 3, commi 6 e 7;
    - le società *in house* e le società partecipate o a controllo pubblico, di cui al numero 4 dell'allegato IV;
- b) il Ministero dell'economia e delle finanze, per i settori bancario e delle infrastrutture dei mercati finanziari, di cui ai numeri 3 e 4 dell'allegato I, sentite le autorità di vigilanza di settore, Banca d'Italia e Consob;
- c) il Ministero delle imprese e del *made in Italy* per: 1) il settore delle infrastrutture digitali, di cui al numero 8 dell'allegato I; 2) il settore dei servizi postali e di corriere, di cui al numero 1 dell'allegato II; 3) il settore della fabbricazione, produzione e distribuzione di sostanze chimiche, di cui al numero 3 dell'allegato II, sentito il Ministero della salute; 4) i sottosettori della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche e della fabbricazione di macchinari e apparecchiature n.c.a., di cui alle lettere b), c) e d) del settore fabbricazione, di cui al numero 5 dell'allegato II; 5) i sottosettori della fabbricazione di autoveicoli, rimorchi e semirimorchi, e della fabbricazione di altri mezzi di trasporto, di cui alle lettere e) e f) del settore fabbricazione, di cui al numero 5 dell'allegato II, sentito il Ministero delle infrastrutture e dei trasporti; 6) i fornitori di servizi digitali, di cui al numero 6 dell'allegato II;
- d) il Ministero dell'agricoltura, della sovranità alimentare e delle foreste per il settore produzione, trasformazione e distribuzione di alimenti, di cui al numero 4 dell'allegato II;
- e) il Ministero dell'ambiente e della sicurezza energetica per: 1) il settore energia, di cui al numero 1 dell'allegato I; 2) i settori: 2.1) fornitura e distribuzione di acqua potabile, di cui al numero 6 dell'allegato I; 2.2) acque reflue, di cui al numero 7 dell'allegato I; 2.3) gestione rifiuti, di cui al numero 2 dell'allegato II;
- f) il Ministero delle infrastrutture e dei trasporti per: 1) il settore trasporti, di cui al numero 2 dell'allegato I; 2) i soggetti che forniscono servizi di trasporto pubblico locale di cui al numero 1 dell'allegato IV;
- g) il Ministero dell'università e della ricerca per il settore ricerca di cui al numero 7 dell'allegato II e per gli istituti di istruzione che svolgono attività di ricerca di cui al numero 2 dell'allegato IV, anche in accordo con le altre amministrazioni vigilanti;
- h) il Ministero della cultura per i soggetti che svolgono attività di interesse culturale di cui al numero 3 dell'allegato IV;
- i) il Ministero della salute per:1) il settore sanitario, di cui al numero 5 dell'allegato I; 2) il sotto settore fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, di cui alla lettera a) del settore fabbricazione, di cui al numero 5 dell'allegato II.

Il comma 3 stabilisce che le Amministrazioni di cui al comma 2, per i rispettivi settori di competenza, sono altresì designate Autorità di settore per i soggetti di cui all'articolo 3, commi 9 e 10.

Il comma 4 prevede che le Autorità di settore NIS, per i rispettivi settori di competenza ai fini di cui al comma 1, procedono, in particolare:

- a) alla verifica dell'elenco dei soggetti di cui all'articolo 7, comma 2;
- b) al supporto nell'individuazione dei soggetti essenziali e dei soggetti importanti ai sensi degli articoli 3 e 6, in particolare identificando i soggetti essenziali e i soggetti importanti di cui ai commi 8, 9 e 10 dell'articolo 3;
- c) all'individuazione dei soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;
- d) al supporto per le funzioni e le attività di regolamentazione di cui al presente decreto secondo le modalità di cui all'articolo 40;
- e) all'elaborazione dei contributi per la relazione annuale di cui all'articolo 12, comma 5;
- f) all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione settoriale del presente decreto nonché al relativo monitoraggio. Per la partecipazione ai tavoli settoriali non sono previsti gettoni di presenza, compensi, emolumenti o rimborsi comunque denominati;
- g) alla partecipazione alle attività settoriali del Gruppo di Cooperazione NIS nonché dei consessi e delle iniziative a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555.

Il comma 5 prevede che con accordo definito entro il 30 settembre 2024 in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono definite modalità di collaborazione tra le Autorità di settore e le regioni interessate, quando il soggetto critico ha carattere regionale ovvero opera esclusivamente sul territorio di una regione nei settori di cui al comma 2, lettere a), numeri 3 e 4, d), e), f), h) e i), numero 1.

Il comma 6 stabilisce che per l'esercizio delle competenze attribuite dal presente decreto, ciascuna autorità di settore, ad eccezione del Ministero dell'economia, è autorizzata a reclutare, con contratto di lavoro subordinato a tempo indeterminato, n. 2 unità di personale non dirigenziale, appartenente all'area funzionari del vigente contratto collettivo nazionale - Comparto funzioni centrali, o categorie equivalenti, mediante procedure di passaggio diretto di personale tra amministrazioni pubbliche ai sensi dell'articolo 30 del decreto legislativo 30 marzo 2001, n. 165, scorrimento di vigenti graduatorie di concorsi pubblici o avvio di nuove procedure concorsuali pubbliche, nonché ad avvalersi di personale non dirigenziale posto in posizione di comando, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche. All'atto del collocamento fuori ruolo è reso indisponibile, nella dotazione organica dell'amministrazione di provenienza, per tutta la durata del collocamento fuori ruolo, un numero di posti equivalente dal punto di vista finanziario.

Il comma 7 dispone che per l'attuazione del comma 6 del presente articolo sia autorizzata la spesa di 409.424 euro per l'anno 2024 e di euro 925.695 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell'articolo 44.

La RT rileva che il Capo II (articoli 9-17) è volto a definire il quadro nazionale di sicurezza informatica.

Sull'articolo 9 evidenzia che definisce la strategia nazionale di cybersicurezza aggiornando, sulla base delle disposizioni della Direttiva NIS2, quanto già previsto nell'abrogando D. Lgs. n. 65/2018.

Rileva che gli oneri derivanti dall'attuazione delle misure strategiche, elencate al comma 3, sono sostenuti entro le disponibilità annuali, rispettivamente, del Fondo per l'attuazione della Strategia nazionale di cybersicurezza e del Fondo per la gestione della cybersicurezza, previsti all'articolo 1, comma 899, lettere a) e b) della legge n. 197 del

2022 (bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023- 2025)[3].

Ribadisce che l'articolo 10 definisce la funzione, attribuita all'ACN, di Autorità nazionale competente NIS e di punto di contatto unico NIS. Dette funzioni, a cui assolvere mediante l'impiego di idonee risorse professionali, determinano per l'ACN maggiori oneri annui, rispetto a quelli ordinariamente previsti, quantificati all'articolo 44, comma 1, in euro 2.000.000 annui, a decorrere dall'anno 2025.

Detti oneri sono così distinti:

- euro 1.750.000 annui per l'incremento delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1, del decreto-legge n. 82 del 2021, utili ai fini della rideterminazione della dotazione organica dello stesso da effettuare con le modalità previste dall'articolo 12, comma 5, del richiamato decreto-legge, che prevede la predetta rideterminazione con apposito DPCM di concerto con il Ministro dell'economia e delle finanze.
- euro 250.000 annui per le attività di formazione specialistica del personale ACN.

Sull'articolo 11 individua le autorità di settore NIS disciplinandone le funzioni ed i settori di competenza.

Ricorda che già con il decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva NIS1, erano state identificate quali autorità di settore:

- il Ministero dello sviluppo economico, per il settore infrastrutture digitali (sottosettori IXP, DNS, TLD, nonché per i servizi digitali);

- il Ministero delle infrastrutture e della mobilità sostenibili, per il settore trasporti (sottosettori aereo, ferroviario, per vie d'acqua e su strada);

- il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;

- il Ministero della salute, per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso, e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza

[3] La norma ivi richiamata prevede che al fine di dare attuazione alla Strategia nazionale di cybersicurezza, adottata con decreto del Presidente del Consiglio dei ministri 17 maggio 2022, e di rendere effettivo il relativo piano di implementazione, sono istituiti nello stato di previsione del Ministero dell'economia e finanze i seguenti Fondi da ripartire: a) Fondo per l'attuazione della Strategia nazionale di cybersicurezza, destinato a finanziare, anche ad integrazione delle risorse già assegnate a tale fine, gli investimenti volti al conseguimento dell'autonomia tecnologica in ambito digitale, nonché l'innalzamento dei livelli di cybersicurezza dei sistemi informativi nazionali, con una dotazione di 70 milioni di euro per l'anno 2023, di 90 milioni di euro per l'anno 2024, di 110 milioni di euro per l'anno 2025 e di 150 milioni di euro annui dal 2026 al 2037; b) Fondo per la gestione della cybersicurezza, destinato a finanziare le attività di gestione operativa dei progetti di cui alla lettera a), con una dotazione finanziaria pari a 10 milioni di euro per l'anno 2023, 50 milioni di euro per l'anno 2024 e 70 milioni di euro annui a decorrere dall'anno 2025.

sanitaria prestata dagli operatori autorizzati e accreditati dalle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

-il Ministero della transizione ecologica, per il settore energia (sottosettori energia elettrica, gas e petrolio);

-il Ministero della transizione ecologica e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

Rispetto al decreto n. 65 del 2018, il presente schema di decreto amplia i compiti ed i settori in cui le predette autorità sono chiamate ad intervenire:

a) il Ministero delle imprese e del *made in Italy*, oltre al settore delle infrastrutture digitali (numero 8 dell'allegato I), anche i seguenti:

il settore dei servizi postali e di corriere (numero 1 dell'allegato II);

il settore della fabbricazione, produzione e distribuzione di sostanze chimiche (numero 3 dell'allegato II) sentito il Ministero dell'ambiente e della sicurezza energetica e il Ministero della salute;

i sottosettori della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche e della fabbricazione di macchinari e apparecchiature n.c.a., di cui alle lettere b), c) e d) del settore fabbricazione (numero 5 dell'allegato II);

i sottosettori della fabbricazione di autoveicoli, rimorchi e semirimorchi, e della fabbricazione di altri mezzi di trasporto, di cui alle lettere e) e f) del settore fabbricazione (numero 5 dell'allegato II) sentito il Ministero delle infrastrutture e dei trasporti;

i fornitori di servizi digitali (numero 6 dell'allegato II);

b) il Ministero delle infrastrutture e dei trasporti, oltre al settore trasporti (numero 2 dell'allegato I), anche per i soggetti che forniscono servizi di trasporto pubblico locale (numero 1 dell'allegato IV);

c) il Ministero della salute per:

il settore sanitario (numero 5 dell'allegato I);

il sottosettore fabbricazione di dispositivi medici e di dispositivi medico-diagnostici *in vitro*, di cui alla lettera a) del settore fabbricazione (numero 5 dell'allegato II);

d) il Ministero dell'ambiente e della sicurezza energetica, oltre al settore energia (numero 1 dell'allegato I) anche per i seguenti settori:

fornitura e distribuzione di acqua potabile (numero 6 dell'allegato I);

acque reflue (numero 7 dell'allegato I);

gestione rifiuti (numero 2 dell'allegato II).

Rispetto a tale elenco, lo schema di decreto in esame identifica ulteriori amministrazioni con funzioni di autorità di settore NIS e, in particolare:

la Presidenza del Consiglio dei ministri, per il settore gestione dei servizi TIC (numero 9 dell'allegato I) in collaborazione con l'Agenzia per la cybersicurezza nazionale; il settore dello spazio (numero 10 dell'allegato I); il settore delle pubbliche amministrazioni, di cui all'articolo 3, commi 6 e 7, e all'allegato III; le società *in house* e le società partecipate o a controllo pubblico, di cui al numero 4 dell'allegato IV;

il Ministero dell'agricoltura, della sovranità alimentare e delle foreste, per il settore produzione, trasformazione e distribuzione di alimenti (numero 4 dell'allegato II);

il Ministero dell'università e della ricerca, per il settore ricerca (numero 7 dell'allegato II) e per gli istituti di istruzione che svolgono attività di ricerca (numero 2 dell'allegato IV);

il Ministero della cultura, per i soggetti che svolgono attività di interesse culturale (numero 3 dell'allegato IV).

Al fine di garantire l'efficiente ed efficace svolgimento dei compiti assegnati dal presente decreto alle Autorità di settore NIS, l'articolo 44, comma 2, prevede oneri, derivanti dall'articolo 11, pari a euro 409.424 per l'anno 2024 e ad euro 925.695 annui a decorrere dall'anno 2025.

Prevede che a tali oneri si provvede ai sensi dell'articolo 44.

Tali risorse potranno essere utilizzate da ciascuna Autorità di settore NIS, ad eccezione del MEF che ha mantenuto inalterati i propri settori di intervento e le relative funzioni rispetto al decreto n. 65 del 2018 (NIS1), al fine di reclutare, con contratto di lavoro subordinato a tempo indeterminato, n. 2 unità di personale non dirigenziale, appartenente all'area funzionari del vigente contratto collettivo nazionale - Comparto funzioni centrali, o categorie equivalenti, mediante procedure di passaggio diretto di personale tra amministrazioni pubbliche ai sensi dell'articolo 30 del decreto legislativo 30 marzo 2001, n. 165, scorrimento di vigenti graduatorie di concorsi pubblici o avvio di nuove procedure concorsuali pubbliche, nonché ad avvalersi di personale non dirigenziale posto in posizione di comando, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche. All'atto del collocamento fuori ruolo è reso indisponibile, nella dotazione organica dell'amministrazione di provenienza, per tutta la durata del collocamento fuori ruolo, un numero di posti equivalente dal punto di vista finanziario.

Rappresenta, altresì, che le Autorità di settore NIS, per i rispettivi settori di competenza procedono all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione del presente decreto nonché al relativo monitoraggio. Ai soggetti partecipanti ai tavoli non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati a carico della finanza pubblica.

La quantificazione degli oneri assunzionali è stata effettuata sulla base delle seguenti retribuzioni *pro capite*:

PCM	Stipendio 12 mensilità CCNL 2016-2018	13^ mens.	Indennità di Presidenza 12 mens.	Totale	Oneri riflessi	Totale retribuzione fondamentale lordo Stato unitario annuo	Retribuzioni accessorie FUP (Flessibilità - art. 15 CCNI) a.l. +Ind. Spec. Org. (art. 18 CCNI) a.l. comprensivo degli oneri	Retribuzione procapite totale lordo stato (A)	incremento contrattuale CCNL 2019-2021 (B)= (A*3,78%)	incremento contrattuale CCNL 2022-2024 C=(A+B)*5,78 %	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 3,78% CCNL 2019-2021 e 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo 3 mesi)	Onere complessivo (a regime dal 2025)
A1	29.538,98	2.462	7.682,04	39.683	15.230	54.913	25.515	80.428	3.040,18	4.824,47	88.293	2	**44.146,41**	**176.585,64**

MINISTERO DELLE IMPRESE E MADE IN ITALY	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	Incremento contrattuale CCNL 2022-2024 (5,78%)	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.528,68	4.213,13	12.887,51	47.089,74	2.721,79	49.811,53	**2**	**24.905,76**	**99.623,05**

MINISTERO DELL'AGRICOLTURA, SOVRANITA' ALIMENTARE E FORESTE	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	**Incremento contrattuale CCNL 2022-2024 (5,78%)**	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.529,48	2.825,53	12.434,07	45.249,50	2.615,42	**47.864,92**	**2**	**23.932,46**	**95.729,84**

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	Incremento contrattuale CCNL 2022-2024 (5,78%)	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.528,68	4.637,54	13.026,29	47.652,93	2.754,34	**50.407,27**	**2**	**25.203,64**	**100.814,54**

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	**Incremento contrattuale CCNL 2022-2024 (5,78%)**	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.683,88	1.080,56	11.922,73	43.147,59	2.493,93	**45.641,52**	**2**	**22.820,76**	**91.283,04**

MINISTERO DELL'UNIVERSITA' E DELLA RICERCA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	**Incremento contrattuale CCNL 2022-2024 (5,78%)**	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.529,48	1.878,27	12.124,32	43.992,49	2.542,77	46.535,25	**2**	**23.267,63**	**93.070,51**

MINISTERO DELLA CULTURA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	**Incremento contrattuale CCNL 2022-2024 (5,78%)**	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.529,32	5.553,68	13.326,12	48.869,54	2.824,66	51.694,19	**2**	**25.847,10**	**103.388,39**

MINISTERO DELLA SALUTE	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	**Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)**	**Incremento contrattuale CCNL 2022-2024 (5,78%)**	**RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024**	**UNITA' AUTORIZZATE**	**Onere 2024 (rateo)**	**Onere complessivo (a regime dal 2025)**
Funzionari	23.501,93	1.958,49	4.529,48	1.412,38	11.971,97	43.374,25	2.507,03	**45.881,28**	**2**	**22.940,64**	**91.762,56**

art. 11, c. 2	Oneri assunzionali		Spese funzionamento		Spese Concorsuali	Buoni pasto		Straordinari		TOTALE	
	2024 (rateo)	2025	2024	2025	2024	2024	2025	2024	2025	2024	2025
a) PCM n. 2 unità	44.146,41	176.585,64	10.000,00	1.000,00	100.000,00	770,00	3.080,00	1.482,53	5.930,10		
c) MIMIT n. 2 unità	24.905,76	99.623,05	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
d) MASAF n. 2 unità	23.932,46	95.729,84	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
e) MASE n. 2 unità	25.203,64	100.814,54	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
f) MIT n. 2 unità	22.820,76	91.283,04	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
g) MUR n. 2 unità	23.267,63	93.070,51	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
h) MIC n. 2 unità	25.847,10	103.388,39	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
i) M. Salute n. 2 unità	22.940,64	91.762,56	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
tot	*213.064,39*	*852.257,57*	*80.000,00*	*8.000,00*	*100.000,00*	*6.160,00*	*24.640,00*	*10.199,31*	*40.797,24*	*409.423,70*	*925.694,81*

Di seguito, i criteri di quantificazione dei seguenti costi correlati all'assunzione dei suddetti contingenti di personale:

BUONI PASTO	Buoni pasto mese n. 20 * 7 euro	Costo annuo calcolato su 11 mesi	Unità	Totale anno 2025	Anno 2024 (rateo)
	140	1540	2	3080	513,33

Straordinario PCM	Aliquota oraria lorda standard	Ore di straordinario annue: 120 (10 ore mensili)	Costo straordinari annuo lordo dipendente compeso	totale
2 unità cat. A1	18,62	120	2965,05	5930,10

CALCOLO STRAORDINARIO MINISTERI	
15,64	orario
5,11	oneri riflessi
20,75	totale orario
2.490,51	per 120 ore
34.867,19	14 unità

La RT rappresenta, altresì, che le Autorità di settore NIS, per i rispettivi settori di competenza procedono all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione del presente decreto nonché al relativo monitoraggio. Ai soggetti partecipanti ai tavoli non spettano gettoni di presenza, compensi, rimborsi di spese o altri emolumenti comunque denominati

Il prospetto riepilogativo ascrive alle norme i seguenti effetti sui saldi di finanza pubblica.

(milioni di euro)

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
10,3	Rafforzamento dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS - personale	S	C		1,75	1,75	1,75		1,75	1,75	1,75		1,75	1,75	1,75
10,3	Rafforzamento dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS - effetti riflessi	E	TC						0,85	0,85	0,85		0,85	0,85	0,85
10,3	Rafforzamento dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS - formazione specialistica	S	C		0,25	0,25	0,25		0,25	0,25	0,25		0,25	0,25	0,25
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,04	0,18	0,18	0,18	0,04	0,18	0,18	0,18	0,04	0,18	0,18	0,18
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte della PCM di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,02	0,10	0,10	0,10	0,02	0,10	0,10	0,10	0,02	0,10	0,10	0,10
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,05	0,05	0,05	0,01	0,05	0,05	0,05
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIMIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,02	0,10	0,10	0,10	0,02	0,10	0,10	0,10	0,02	0,10	0,10	0,10
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,05	0,05	0,05	0,01	0,05	0,05	0,05
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASAF di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,03	0,10	0,10	0,10	0,03	0,10	0,10	0,10	0,03	0,10	0,10	0,10

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,05	0,05	0,05	0,01	0,05	0,05	0,05
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MASE di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,04	0,04	0,04	0,01	0,04	0,04	0,04

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIT di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09
11,7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,05	0,05	0,05	0,01	0,05	0,05	0,05
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MUR di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,03	0,10	0,10	0,10	0,03	0,10	0,10	0,10	0,03	0,10	0,10	0,10
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,05	0,05	0,05	0,01	0,05	0,05	0,05
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,7-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,7-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del MIC di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - personale	S	C	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09	0,02	0,09	0,09	0,09
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,01	0,04	0,04	0,04	0,01	0,04	0,04	0,04
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - straordinari	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - effetti riflessi	E	TC					0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese di funzionamento	S	C	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,00
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte del Ministero della SALUTE di 2 unità di personale non dirigenziale appartenente all'area funzionari - buoni pasto	S	C	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Art/co.	Descrizione norma	e/s		Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
11,6-7	Reclutamento (con contratto di lavoro subordinato a tempo indeterminato), da parte di ciascuna Autorità di settore NIS, di 2 unità di personale non dirigenziale appartenente all'area funzionari - spese concorsuali	S	C	0,10				0,10				0,10			

Al riguardo, sull'articolo 9 andrebbe verificata l'adeguatezza delle risorse previste dalla legislazione vigente dalla legge di bilancio 2023, cosi come integrate dagli articoli 11, 13 e 15 dello schema in esame, che saranno assegnate all'Agenzia per la cybersicurezza nazionale (ACN), organismo centrale nell'elaborazione e nella gestione della Strategia di cybersicurezza nazionale[4], fornendo elementi di riscontro sul fabbisogno di risorse umane e strumentali necessarie a tal fine.

Sull'articolo 10, che prevede, in relazione alle maggiori funzioni da assolvere da parte dell'ACN, un'autorizzazione di spesa di 2.000.000 di euro annui a decorrere dall'anno 2025, pur trattandosi di un limite massimo di spesa, andrebbe fornito un quadro di sintesi dei fabbisogni di professionalità necessari all'Agenzia per l'assolvimento dei nuovi compiti, con informazioni sui profili di inquadramento previsti e sui trattamenti economici annui lordi corrispondenti, nonché sui tempi di reclutamento delle nuove risorse umane e relativi oneri di funzionamento nel limite massimo delle risorse stanziate[5].

Con riferimento alla seconda quota di risorse destinata alla formazione, pur considerando che si tratta di autorizzazione predisposta come limite massimo di spesa, andrebbero comunque forniti gli elementi e i dati utilizzati per la quantificazione della relativa spesa.

Quanto alla autorizzazione di spesa di cui all'articolo 11, nulla da osservare, dal momento che la RT evidenzia una particolareggiata quantificazione dei nuovi e maggiori oneri di personale, per ogni Autorità di settore NIS, pari complessivamente a 409.424 per l'anno 2024 e ad euro 925.695 annui a decorrere dall'anno 2025, comprensivi di oneri per lavoro straordinario, per spese concorsuali (solo per il 2024) e di funzionamento e per i buoni pasto, nonché degli incrementi contrattuali stabiliti all'esito della conclusa tornata contrattuale 2019-2021 (+ 3,78%) e accordati per il triennio 2022-2024 (+ 5,78%).

---

[4] L'articolo 7 della direttiva UE 2022/2555 stabilisce che ogni Stato membro adotta una strategia nazionale per la cibersicurezza che prevede gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza.

[5] Sul punto, si segnala quanto recentemente previsto dagli articoli 12 e 13 della legge n. 90 del 28 giugno 2024 (Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici). Cfr. Nota di lettura n. 149, pagine 14-15.

Preso atto dei dati riportati nella RT, di cui si attesta la congruità e prudenzialità quanto ai criteri e parametri utilizzati[6], andrebbero comunque forniti elementi di dettaglio in merito agli oneri previsti relativamente agli istituti del trattamento accessorio annuo lordo, per ciascuna delle Amministrazioni interessate, nonché rassicurazioni in merito alla prudenzialità dell'ipotesi considerata per il calcolo delle mensilità previste per il 2024, con un rateo di spesa mensile di soli 3 mesi.

Quanto allo scrutinio degli effetti attesi sui saldi di finanza pubblica, andrebbero forniti i quadri di calcolo degli effetti indotti per l'erario con l'indicazione delle aliquote applicate, come previsto dalla circolare n. 32/2010 del Dipartimento della R.G.S.

Secondo la RT le risorse potranno essere utilizzate da ciascuna delle Autorità di settore NIS, ad eccezione del MEF (che mantiene inalterati i propri settori di intervento e le relative funzioni), mediante procedure di passaggio diretto di personale tra amministrazioni pubbliche, scorrimento di vigenti graduatorie di concorsi pubblici o avvio di nuove procedure concorsuali pubbliche, nonché avvalendosi di personale non dirigenziale posto in posizione di comando, di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche. Sul punto, essendo previsto dalla norma che all'atto del collocamento fuori ruolo sia reso indisponibile, nella dotazione organica dell'amministrazione di provenienza, per tutta la durata del collocamento fuori ruolo, un numero di posti equivalente dal punto di vista finanziario, nulla da osservare, atteso che l'apposizione di tale clausola è pienamente coerente con l'obiettivo di assicurare l'invarianza degli effetti d'impatto sui saldi di finanza pubblica. Si rileva comunque che gli istituti normativi richiamati presentano sensibili differenze quanto ai loro riflessi sugli organici e retributivi sia per l'Amministrazione di appartenenza che per quella di effettivo impiego[7].

---

[6] Relativamente all'autorizzazione al reclutamento di n. 2 unità di Categoria A inquadrate presso la Presidenza del Consiglio dei ministri, si osserva che il Conto Annuale della R.G.S al 2022, indica una retribuzione media annua unitaria (lordo Stato) di 64.745 euro, di cui 31.951 di voci stipendiali (Tabellare, I.I.S., RIA, 13a mensilità) e 32.794 euro di voci accessorie; per il MIMIT la retribuzione media annua di un funzionario è indicata in 41.684 euro annui lordi (lordo Stato), di cui 28.895 euro di componenti stipendiali e 12.789 di componenti accessorie; per il MASAF la retribuzione media annua di un funzionario indicata dal Conto Annuale è di 44.439 euro lordi annui, di cui 30.161 euro di componenti retributive fondamentali e 14.278 euro di componenti accessorie; quanto al MASE la retribuzione media annua di un Funzionario indicata dal Conto Annuale è di 37.487 euro, di cui 27.652 di componenti del trattamento economico fondamentale e 9.834 euro riconducibili al trattamento accessorio; quanto al MIT la retribuzione media annua di un Funzionario indicata dal Conto Annuale è di 36.167 euro, di cui 28.282 di componenti fondamentali e 7.885 di componenti retributive accessorie; per il MUR la retribuzione media annua di un funzionario indicata dal Conto Annuale è di 38.651 euro, di cui 27.715 euro di componenti fondamentali e di 10.936 di componenti accessorie; per il MIC il trattamento economico annuo previsto per un Funzionario dal Conto Annuale è di 38.463 euro, di cui 27.095 euro di componenti stipendiali e 11.367 euro di componenti accessorie; per il Ministero della salute, la retribuzione media annua per un Funzionario indicata da Conto Annuale è di 38.791 euro, di cui 27.051 di componenti fondamentali e 11.741 di componenti accessorie. I valori indicati andrebbero poi integrati dell'8,5% relativo alla contribuzione a carico del datore dei lavoratori.

[7] A tale riguardo, si rinvia agli articoli 57 e 59 del D.P.R. n. 3/1957, nonché, per gli enti dotati di autonomia di bilancio, al comma 12 dell'articolo 70 del T.U.P.I. Quanto alla durata massima del comando o fuori ruolo si rinvia al comma 2-*sexies* dell'articolo 30 del T.U.P.I.

Sull'istituzione di tavoli settoriali, relativamente ai quali la RT afferma che ai partecipanti non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati a carico della finanza pubblica, nulla da osservare. Ciò premesso, andrebbero comunque fornite conferme in merito alla possibilità che l'istituzione e il funzionamento di tali tavoli possa essere effettuato da parte delle Autorità di settore avvalendosi delle sole risorse previste in bilancio ai sensi della legislazione vigente.

Articolo 12

Il comma 1 istituisce il Tavolo permanente per l'attuazione della disciplina NIS2 presso l'Agenzia per la cybersicurezza nazionale (ACN).

Il comma 2 ne stabilisce la composizione.

Il comma 3 prevede che possono essere chiamati a partecipare alle riunioni: altri rappresentanti delle amministrazioni di riferimento delle autorità NIS in relazione alle materie oggetto di trattazione; rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca; operatori privati interessati dalle previsioni di cui al presente provvedimento.

Il comma 4 stabilisce che il Tavolo è convocato dal presidente o su richiesta di almeno tre componenti e si riunisce almeno una volta per trimestre.

Il comma 5 individua i compiti del Tavolo:

- a) supportare l'Agenzia per la cybersicurezza - Autorità nazionale competente NIS nello svolgimento delle funzioni relative all'implementazione e all'attuazione del presente provvedimento, con particolare riferimento ai compiti ad essa conferiti dall'articolo 10, comma 1, (ad eccezione dei poteri di vigilanza);
- b), formulare proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo;
- c) predisporre una relazione annuale sull'attuazione del presente provvedimento.

Il comma 6 stabilisce che con determinazione dell'ACN, sentito il Tavolo, possono essere dettate ulteriori disposizioni per l'organizzazione e per il funzionamento del Tavolo, per la cui partecipazione non sono previsti gettoni di presenza, compensi, rimborsi di spese o altri emolumenti, comunque denominati.

La RT evidenzia che l'articolo reca l'istituzione, in via permanente, del Tavolo per l'attuazione della disciplina NIS2 di cui alla direttiva 2555/2022, al fine di assicurare l'implementazione e attuazione del presente decreto legislativo.

In particolare, il comma 6 stabilisce che la partecipazione al Tavolo in parola non dà luogo alla corresponsione di gettoni di presenza, compensi o rimborsi di spese o altri emolumenti, comunque denominati.

Assicura che la disposizione, pertanto, non reca nuovi o maggiori oneri.

Al riguardo, tenuto conto di quanto previsto dal comma 6 in merito all'assenza di compensi o rimborsi per i component del Tavolo, nulla di particolare da osservare.

Ad ogni modo, andrebbe confermato che l'Agenzia per la cybersicurezza nazionale (ACN) possa assicurare, in via permanente, il supporto al Tavolo per l'attuazione della disciplina NIS, al fine di consentire l'implementazione e la corretta attuazione del

presente decreto, avvalendosi delle sole risorse umane e strumentali già previste ai sensi della legislazione vigente.

Articolo 13

L'articolo 13 individua quali Autorità nazionali di gestione delle crisi informatiche l'Agenzia per la cybersicurezza nazionale (ACN), con funzioni di coordinatore, e il Ministero della difesa, ciascuno per gli ambiti di competenza.

Tali enti individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi. Si demanda a uno o più D.P.C.M. – da adottarsi entro 12 mesi dalla data di entrata in vigore del provvedimento – la definizione del Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Il piano è aggiornato periodicamente e, comunque, ogni tre anni.

Tale piano stabilisce:

- obiettivi e misure delle attività nazionali di preparazione;
- compiti e responsabilità delle due Autorità nazionali;
- procedure di gestione delle crisi;
- pertinenti portatori di interessi pubblici e privati;
- le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'UE.

Il comma 6 stabilisce che ai fini dell'attuazione del comma 1 del presente articolo è autorizzata la spesa pari a euro 1.000.000 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell'articolo 44.

La RT rileva che l'articolo delinea la composizione ed il funzionamento del quadro nazionale di gestione delle crisi informatiche individuando, quali autorità competenti alla gestione degli incidenti e delle crisi informatiche su vasta scala (Autorità di gestione delle crisi informatiche), di cui all'articolo 9 della direttiva, l'ACN, anche con funzioni di coordinatore ai sensi del paragrafo 2, del medesimo articolo 9, insieme al Ministero della difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g), del presente decreto.

In relazione ai predetti compiti, l'articolo 44, comma 3, quantifica oneri a decorrere dall'anno 2025, per l'importo pari a euro 1.000.000 annui, così distinti:

- euro 500.000 da assegnare all'ACN per far fronte ai seguenti oneri di funzionamento:
  - euro 200.000, derivanti dalle specifiche funzioni, anche attraverso l'implementazione di strutture tecnologiche utili al coordinamento delle attività di gestione delle crisi cibernetiche su vasta scala e allo scambio informativo in condizioni di sicurezza;
  - euro 300.000, derivanti dalle attività necessarie e funzionali alla partecipazione alle esercitazioni a livello europeo e alle attività formative, esercitative e di preparazione a livello nazionale.
- euro 500.000 da assegnare al Ministero della difesa per i nuovi e maggiori oneri, ripartiti nel seguente modo:
  - 250.000 euro, nell'ambito del supporto alle attività di sicurezza della *supply chain* strategica della difesa, essenziale per il funzionamento delle capacità

operative dello strumento militare, nonché per lo sviluppo ed il potenziamento info-strutturale di canali sicuri di scambio di informazioni;

- 150.000 euro, nell'ambito delle attività di difesa dello Stato. In particolare, tali risorse risultano necessarie per il potenziamento info-strutturale e capacitivo nei settori della *Cyber Situational Awareness*, monitoraggio; protezione e risposta;
- 100.000 euro necessari per la formazione del personale.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica ascrive alle norme i seguenti effetti:

(milioni di euro)

Co.	Descrizione		e/s	nat.	Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
					2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
6	Oneri di funzionamento e formazione per l'attuazione del quadro nazionale di gestione delle crisi informatiche	Agenzia per la cybersicurezza nazionale	S	C		0,5	0,5	0,5		0,5	0,5	0,5		0,5	0,5	0,5
		Ministero della Difesa	S	C		0,5	0,5	0,5		0,5	0,5	0,5		0,5	0,5	0,5

Al riguardo, per i profili di quantificazione, pur considerando che il comma 6 predispone l'autorizzazione come tetto di spesa, a fronte di oneri che appaiono peraltro pienamente rimodulabili, andrebbe comunque fornita l'illustrazione dei criteri e parametri considerati nella quantificazione delle risorse, al fine di consentire una valutazione, almeno di massima, del grado di adeguatezza delle risorse rispetto alle finalità espressamente indicate dalla RT.

Articolo 14

L'articolo 14 reca disposizioni in tema di cooperazione tra le Autorità nazionali in tema di Cybersicurezza.

In particolare, il comma 1 dispone che siano assicurate la cooperazione e la collaborazione reciproca tra ACN e l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazioni (autorità di contrasto), il Garante per la protezione dei dati personali, l'Ente nazionale per l'aviazione civile, l'AgID, l'AGCOM, e il Ministero della difesa, nonché con altre autorità nazionali competenti, per lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

Il comma 2 dispone che l'ACN e Garante cooperino nei casi di incidenti che comportano violazioni dei dati personali. Inoltre, qualora il Garante o le autorità di controllo di altri Stati membri impongano una sanzione amministrativa pecuniaria, l'ACN non procede all'irrogazione delle sanzioni amministrative pecuniarie imputabile al medesimo comportamento. Infine si prevede l'adozione di un D.P.C.M. per definire l'elenco dei soggetti – all'interno di quelli individuati annualmente come "essenziali" o "importanti" ai sensi del comma 2 dell'art. 7 – che impattano sulla efficienza dello Strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'ACN comunica

tempestivamente al Ministero della difesa gli incidenti e le ulteriori informazioni di sicurezza cibernetica.

Il comma 3 specifica che la collaborazione tra l'ACN e le altre autorità nazionali è assicurata con gli strumenti previsti dal regolamento (UE) 2022/2554 e dal provvedimento di attuazione.

Il comma 4 specifica che l'ACN informa il forum di sorveglianza quando esercita i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dal provvedimento da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di ICT.

Il comma 5 specifica che l'ACN coopera con le autorità nazionali competenti anche con lo scambio periodico di informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti identificati come critici, e sulle misure adottate in risposta a tali rischi, minacce e incidenti.

Il comma 6 disciplina le modalità esecutive per la collaborazione di cui al comma precedente.

La RT evidenzia che l'articolo si limita a definire le modalità di cooperazione a livello nazionale, integrando le previsioni dell'abrogando D.lgs. n. 65 del 2018 con quanto previsto dalla direttiva.

Assicura che le disposizioni non determinano nuovi o maggiori oneri a carico del bilancio dello Stato, esplicandosi in attività già svolte nell'ambito delle funzioni istituzionali dell'ACN.

Al riguardo, per i profili di quantificazione, alla luce delle rassicurazioni fornite dalla RT secondo cui si tratta di attività già svolte nell'ambito delle funzioni istituzionali dell'ACN, non ci sono osservazioni.

Articoli 15-16

L'articolo 15 disciplina il Gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT), istituito presso l'Agenzia per la cybersicurezza nazionale (ACN), con i seguenti compiti:

a) è l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso;

b) dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale attraverso la quale scambiare informazioni con i soggetti essenziali o importanti e con gli altri portatori di interesse pertinenti;

c) coopera e, se opportuno, scambia informazioni pertinenti conformemente all'articolo 17 (v. *infra*) con comunità settoriali o intersettoriali di soggetti essenziali e di soggetti importanti;

d) partecipa alla revisione tra pari di cui all'articolo 21 (v. *infra*);

e) garantisce la collaborazione effettiva, efficiente e sicura, nella Rete di CSIRT nazionali di cui all'articolo 20 (v. *infra*);

f) può stabilire relazioni di cooperazione con gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi. Nell'ambito di tali relazioni di cooperazione, facilita uno scambio di informazioni efficace, efficiente e sicuro con tali CSIRT nazionali, o strutture nazionali equivalenti di Paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, ivi inclusi quelli adottati e sviluppati dalle principali comunità nazionali, europee e internazionali del settore. Il CSIRT Italia può scambiare informazioni pertinenti con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, compresi dati personali ai sensi della normativa nazionale vigente e del diritto dell'Unione europea in materia di protezione dei dati personali;

g) può cooperare con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, in particolare al fine di fornire loro assistenza in materia di sicurezza informatica.

Il comma 2 dell'articolo in esame prevede le seguenti dotazioni del CSIRT Italia:

- è dotato di un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di malfunzionamento e dispone di mezzi che gli permettono di essere contattato e di contattare i soggetti e altri CSIRT nazionali in qualsiasi momento. Il CSIRT Italia indica chiaramente i canali di comunicazione e li rende noti ai soggetti e agli altri CSIRT nazionali;
- dispone di locali e sistemi informativi di supporto ubicati in siti sicuri;
- utilizza un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;
- garantisce la riservatezza e l'affidabilità delle proprie attività;
- è dotato di sistemi ridondanti e spazi di lavoro di *backup* al fine di garantire la continuità dei propri servizi;
- partecipa, se del caso, a reti di cooperazione internazionale.

Il comma 3 individua i seguenti compiti del CSIRT Italia:

- monitora e analizza le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale e, su richiesta, fornisce assistenza ai soggetti essenziali e ai soggetti importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informativi e di rete, secondo un ordine di priorità delle attività definito dal CSIRT Italia, onde evitare oneri sproporzionati o eccessivi;
- emette preallarmi, allerte e bollettini e divulga informazioni ai soggetti essenziali e ai soggetti importanti interessati, nonché alle autorità nazionali competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;
- fornisce una risposta agli incidenti e assistenza ai soggetti essenziali e ai soggetti importanti interessati, ove possibile;
- raccoglie e analizza dati forensi e fornisce un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla sicurezza informatica;
- effettua, su richiesta di un soggetto essenziale o importante, secondo modalità e procedure definite, una scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;
- partecipa alla Rete di CSIRT nazionali di cui all'articolo 20 (v. *infra*) e fornisce assistenza reciproca secondo le proprie capacità e competenze agli altri membri della Rete di CSIRT nazionali su loro richiesta;
- agisce in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 16 (v. *infra*);
- contribuisce allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui al comma 1, lettera b);
- può effettuare, secondo modalità e procedure definite, una scansione proattiva e non intrusiva dei sistemi informativi e di rete accessibili al pubblico di soggetti essenziali e di soggetti importanti. Tale scansione è effettuata per individuare sistemi informativi e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.

Il comma 4 dispone che il CSIRT Italia applichi un approccio basato sul rischio per stabilire l'ordine di priorità nello svolgimento dei suddetti compiti di cui al comma 3.

Il comma 5 prevede che in caso di eventi malevoli per la sicurezza informatica, le strutture pubbliche con funzione di *computer emergency response team* (CERT) collaborano con il CSIRT Italia, anche ai fini di un più efficace coordinamento della risposta agli incidenti.

Il comma 6 prevede che il CSIRT Italia instaura rapporti di cooperazione con i pertinenti portatori di interesse nazionali del settore privato al fine di perseguire gli obiettivi del presente decreto in relazione alle proprie competenze.

Il comma 7 stabilisce che al fine di agevolare la cooperazione di cui al comma 5, il CSIRT Italia promuove l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda: a) le procedure di gestione degli incidenti; b) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 16.

Il comma 8 dispone che ai fini dell'attuazione del presente articolo sia autorizzata la spesa pari a euro 2.000.000 annui a decorrere dall'anno 2025, cui si provvede ai sensi dell'articolo 44.

L'articolo 16 attribuisce al gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia) il ruolo di coordinatore dei soggetti interessati ai fini della divulgazione coordinata delle vulnerabilità e di intermediario tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti, prevedendo che sia adottata da parte dell'Autorità nazionale competente NIS una politica nazionale di divulgazione coordinata delle vulnerabilità, tenuto conto degli orientamenti del gruppo di cooperazione NIS, nonché di implementare mezzi tecnici per agevolare l'attuazione di tale politica.

La RT evidenzia che l'articolo disciplina il Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT Italia) già incardinato all'interno di ACN. L'ottimale funzionamento di detta struttura, che ha natura e compiti prettamente operativi, richiede la presenza continua di personale altamente qualificato, nonché di strumenti *hardware* e *software* estremamente performanti. A tal fine è autorizzata una spesa pari a euro 2.000.000 annui, a decorrere dall'anno 2025, così ripartiti:

- euro 1.750.000 annui per l'incremento delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1, del decreto-legge n. 82 del 2021, utili ai fini della rideterminazione della dotazione organica dello stesso da effettuare con le modalità previste dall'articolo 12, comma 5, del richiamato decreto-legge, che prevede la predetta rideterminazione con apposito DPCM di concerto con il Ministro dell'economia e delle finanze.
- euro 250.000 annui per l'acquisizione di strumenti *hardware* e *software*.

Sottolinea che l'articolo 16 reca disposizioni in tema di divulgazione coordinata delle vulnerabilità e attribuisce allo CSIRT Italia il ruolo di coordinatore dei soggetti interessati e di intermediario tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi.

Evidenzia che la disposizione non ha riflessi finanziari diretti poiché dette attività rientrano nell'ambito complessivo dei compiti svolti da CSIRT Italia, delineati all'articolo 15 che reca, altresì l'indicazione per la copertura dei relativi oneri finanziari.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica ascrive alle norme i seguenti effetti:

(milioni di euro)

Co.	Descrizione		e/s	nat.	Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
					2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
8	Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)	personale	S	C		1,75	1,75	1,75		1,75	1,75	1,75		1,75	1,75	1,75
		effetti riflessi	E	TC						0,85	0,85	0,85		0,85	0,85	0,85
		acquisto *software e hardware*	S	K		0,25	0,25	0,25		0,25	0,25	0,25		0,25	0,25	0,25

Al riguardo, l'autorizzazione indicata al comma 8 è chiaramente predisposta nella forma di tetto massimo di spesa a fronte di un onere che appare pienamente rimodulabile e pertanto compatibile con un meccanismo di limite massimo.

Ad ogni modo, dal momento che - stando alla RT - la somma di 1.750.000 euro annui è destinata all'incremento delle risorse finanziarie per il personale dell'Autorità e la somma di 250.000 euro annui all'acquisizione di strumenti *hardware* e *software*, andrebbero in ogni caso forniti i criteri e parametri utilizzati per le ipotesi sui fabbisogni di spesa considerati nella quantificazione, come previsto dalla Circolare n. 32/2010 del Dipartimento della R.G.S.[8].

Sull'articolo 16, tenuto conto che le disposizioni in esame trovano copertura a valere sulle risorse previste dall'articolo 15, non ci sono osservazioni.

Articolo 17

L'articolo 17 disciplina lo scambio volontario di informazioni sulla sicurezza informatica tra i soggetti coinvolti. Questi scambi possono riguardare minacce informatiche, vulnerabilità e raccomandazioni, e sono finalizzati a prevenire incidenti e migliorare la sicurezza informatica. Lo scambio di informazioni avviene tra soggetti essenziali, soggetti importanti e, se opportuno, relativi fornitori, tramite accordi specifici che rispettano la natura sensibile delle informazioni. L'Agenzia per la cybersicurezza nazionale facilita questi accordi, definendo anche gli elementi operativi e supportando i soggetti coinvolti. I soggetti essenziali e i soggetti importanti devono notificare la loro partecipazione o ritiro dagli accordi.

Gli Organismi di informazione per la sicurezza hanno accesso alle informazioni rilevanti.

La RT conferma che l'articolo 17 disciplina gli accordi di condivisione delle informazioni sulla sicurezza informatica tra i soggetti che rientrano nell'ambito di applicazione del presente decreto, che si sostanziano nello scambio di informazioni sulla sicurezza informatica.

La disposizione, che riveste carattere ordinamentale, non reca nuovi o maggiori oneri per la finanza pubblica.

---

[8] Il Paragrafo 4.1, alla lettera h) della Circolare citata indica l'essenzialità dei dati, parametri e metodologie utilizzati per valutare gli effetti di ciascuna disposizione sugli andamenti tendenziali del saldo di cassa e dell'indebitamento netto ed indicazione dei criteri per la quantificazione e la compensazione di tali effetti, rilevando come "necessario" della RT, "qualsiasi dato o informazione che si dimostri utile alla quantificazione degli effetti finanziari, anche se non espressamente indicato dalla legge n. 196 del 2009". Cfr. Ministero dell'economia e delle finanze, Dipartimento della R.G.S., I.G.B., Circolare n. 32/2010, pagina 4.

Al riguardo, convenendo in linea di principio con la RT in merito al carattere essenzialmente ordinamentale delle disposizioni, non ci sono particolari osservazioni.

Ad ogni modo, andrebbe confermato che l'Agenzia per la cybersicurezza possa svolgere i compiti di supporto allo scambio di informazioni avvalendosi delle risorse disponibili a legislazione vigente.

Articoli 18-20

L'articolo 18 disciplina l'attività del Gruppo di cooperazione NIS, già operante ai sensi dell'abrogando decreto legislativo n. 65 del 2018, prevedendo che l'Autorità nazionale competente NIS (l'Agenzia per la cybersicurezza) partecipi alle attività del Gruppo avvalendosi, se lo richiede, del supporto delle Autorità di settore NIS sulla base delle loro specifiche competenze[9].

L'articolo 19 disciplina la partecipazione dell'Agenzia per la cybersicurezza nazionale quale autorità nazionale di gestione delle crisi informatiche alla Rete delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe.

Il comma 2 prevede che ai fini del comma 1, l'Autorità nazionale di gestione delle crisi informatiche contribuisca a:

- aumentare il livello di preparazione per la gestione di incidenti e crisi informatiche su vasta scala;
- sviluppare una conoscenza condivisa sui medesimi eventi;
- valutare le conseguenze dei medesimi eventi e proporre misure di attenuazione;
- coordinare la gestione dei medesimi eventi e sostenere il processo decisionale politico in materia;
- discutere, su richiesta di uno Stato membro, i piani nazionali di risposta agli incidenti e alle crisi informatiche su vasta scala previsti dall'articolo 9, paragrafo 4, della direttiva oggetto di recepimento (in base a tale norma della direttiva il piano deve, tra le altre cose, comprendere, le attività nazionali di preparazione, i compiti e le responsabilità delle autorità di gestione delle crisi informatiche e la gestione delle crisi informatiche); in relazione a tale previsione il comma 3 specifica poi che anche l'Agenzia può richiedere di discutere il piano nazionale;
- supportare la collaborazione con il gruppo di cooperazione NIS;
- cooperare con la rete di CSIRT nazionali;
- predisporre la relazione al Parlamento europeo e al Consiglio sui lavori della Rete, relazione prevista dall'articolo 16, paragrafo 7, della direttiva oggetto di recepimento (tale disposizione della direttiva prevede che la prima relazione sia preparata entro il 17 luglio 2024 e successivamente ogni 18 mesi).

L'articolo 20 regola la partecipazione del CSIRT Italia alla rete di CSIRT nazionali.

A tale fine, al comma 2 si dispone che il CSIRT Italia contribuisce a:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;

b) agevolare, ove possibile, la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT nazionali;

---

[9] La direttiva (UE) 2022/2555 ha istituito all'articolo 14 il Gruppo di cooperazione, costituito dai rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA), con il compito di implementare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri rafforzandone la fiducia reciproca.

c) scambiare, su richiesta di un CSIRT nazionale di un altro Stato membro potenzialmente interessato da un incidente, informazioni relative a tale incidente, alle minacce informatiche, ai rischi e alle vulnerabilità associate;

d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di sicurezza informatica;

e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;

f) su richiesta di un membro della Rete di CSIRT nazionali potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente, ai rischi e alle vulnerabilità associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;

g) su richiesta di un membro della Rete di CSIRT nazionali, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

h) fornire assistenza ai CSIRT nazionali di altri Stati membri nel far fronte a incidenti che interessano due o più Stati membri;

i) cooperare e scambiare migliori pratiche con i CSIRT nazionali designati dagli altri Stati membri in qualità di coordinatori ai sensi dell'articolo 12 della direttiva (UE) 2022/2555, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

l) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a: 1) categorie di minacce informatiche e incidenti; preallarmi; 2) assistenza reciproca; 3) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri; 4) contributi al piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3, su richiesta di uno Stato membro;

m) su richiesta di un membro della Rete di CSIRT nazionali, discutere le capacità e lo stato di preparazione del CSIRT nazionale richiedente;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza informatica regionali e a livello dell'Unione europea, al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche a livello dell'Unione europea;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;

p) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi-incidenti, le minacce informatiche, i rischi e le vulnerabilità;

q) informare il Gruppo di cooperazione NIS sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera i) e, se necessario, chiedere orientamenti non vincolanti in merito;

r) fare il punto sui risultati delle esercitazioni di sicurezza informatica, comprese quelle organizzate dall'ENISA;

s) fornire orientamenti non vincolanti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

La RT evidenzia che l'articolo 18 disciplina l'attività del Gruppo di cooperazione NIS, già operante ai sensi dell'abrogando D.lgs. n. 65 del 2018. La disposizione non prevede nuovi o maggiori oneri rispetto a quelli già sostenuti nell'ambito delle attività istituzionali di ACN.

Sugli articoli 19 e 20 si limita a confermare che gli articoli in esame regolano, rispettivamente, la partecipazione dell'Autorità nazionale di gestione delle crisi cibernetiche alla Rete delle organizzazioni di collegamento per le crisi cibernetiche (EU-CyCLONe) e la partecipazione del CSIRT Italia alla rete di CSIRT nazionali.

Assicura che anche dalle disposizioni citate non scaturiscono nuovi o maggiori oneri.

Al riguardo, premesso che gli articoli 19 e 20 provvedono al recepimento degli articoli 15 e 16 della direttiva UE 2022/2555, andrebbe confermato che le attività potranno essere svolte da parte dell'Autorità nazionale di gestione delle crisi informatiche avvalendosi delle sole risorse umane e strumentali già previste dalla legislazione vigente.

Articolo 21

L'articolo disciplina una procedura di revisione delle modalità attuative della direttiva NIS 2 - in particolare per questioni specifiche di natura transfrontaliera o intersettoriale denominata "procedura di revisione tra pari" ai sensi dell'articolo 19 della direttiva NIS2.

Ai sensi del comma 1 l'Autorità nazionale competente NIS contribuisce alla definizione della metodologia e degli aspetti organizzativi delle revisioni tra pari (nel quadro della metodologia di cui all'articolo 18, comma 4, lettera m), del presente provvedimento) e può partecipare alla procedura di revisione tra pari, attraverso le seguenti due modalità distinte:

- richiedendo l'esecuzione di una revisione tra pari in relazione all'attuazione della direttiva a livello nazionale (lett.a);
- indicando uno o più rappresentanti dell'ACN o delle Autorità di settore NIS quali esperti di sicurezza informatica per eseguire revisioni tra pari presso altri Stati membri, su richiesta di questi ultimi, nel rispetto dei codici di condotta. Eventuali rischi di conflitto di interessi riguardanti gli esperti di sicurezza informatica designati sono condivisi con gli altri Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA prima dell'inizio della revisione tra pari (lett. b).

Quando la revisione è richiesta dall'ACN – Autorità nazionale NIS, questa, con propria determinazione (comma 2):

- individua almeno uno dei seguenti aspetti da sottoporre alla revisione tra pari:
- il livello di attuazione degli obblighi in materia di misure di gestione del rischio (art. 24) e di notifica degli incidenti informatici (art. 25);
- il livello delle capacità e l'efficacia dello svolgimento dei compiti dell'Autorità medesima;
- le capacità operative del CSIRT Italia;
- lo stato di attuazione dell'assistenza reciproca tra l'ACN – Autorità nazionale NIS e le autorità competenti degli altri Paesi membri;
- lo stato di attuazione degli accordi per la condivisione delle informazioni in materia di sicurezza informatica da parte die soggetti che rientrano nell'ambito di applicazione del presente provvedimenti;
- eventuali altre questioni specifiche di natura transfrontaliera o intersettoriale;
- notifica, prima dell'inizio della revisione tra pari, agli Stati membri partecipanti, l'ambito di applicazione della medesima, comprese le questioni specifiche individuate;
- effettua un'autovalutazione degli aspetti oggetto della revisione;
- seleziona, tra gli esperti di sicurezza informatica indicati dagli altri Stati membri partecipanti, gli esperti idonei da designare. Qualora l'ACN - Autorità nazionale competente NIS si opponga alla designazione di uno o più esperti indicati, comunica allo Stato membro indicante i motivi debitamente giustificati;
- fornisce l'autovalutazione di cui sopra agli esperti designati;
- fornisce agli esperti designati le informazioni necessarie per la valutazione;
- formula osservazioni sulla relazione elaborata dagli esperti designati; può pubblicare la relazione elaborata dagli esperti designati.

Quando la revisione è promossa da altri Stati membri, il comma 3 individua alcuni compiti e obblighi in capo agli esperti di sicurezza informatica partecipanti alla revisione indicati dall'Autorità nazionale competente NIS, i quali:

- non devono divulgare a terzi le eventuali informazioni sensibili o riservate ottenute nel corso delle revisioni;
- partecipano alle attività necessarie allo svolgimento delle revisioni tra pari tramite visite in loco fisiche o virtuali e scambi di informazioni a distanza;
- contribuiscono all'elaborazione delle relazioni sui risultati e sulle conclusioni delle revisioni tra pari.

La RT afferma che l'articolo introduce la procedura di revisione tra pari ai sensi dell'articolo 19 della direttiva NIS2 e che non comporta oneri a carico della finanza pubblica, in quanto le attività previste verranno svolte dall'ACN con le autorità di settore con le risorse umane, strumentali, finanziarie disponibili a legislazione vigente.

Al riguardo, andrebbero fornite maggiori informazioni sulle risorse disponibili presso l'Agenzia per la cybersicurezza nazionale da destinare alla procedura in esame, che comporta l'impiego di esperti, l'eventuale svolgimento di missioni (previste in via facoltativa dal comma 3, lettera b)), nonché l'elaborazione di relazioni sui risultati e sulle conclusioni delle revisioni tra pari.

Articolo 22

L'articolo 22 individua gli obblighi di comunicazione nei confronti dell'Unione europea da parte rispettivamente della Presidenza del Consiglio dei ministri, dell'Agenzia per la cybersicurezza nazionale in qualità di Autorità nazionale competente e Punto di contatto unico NIS, nonché di Autorità nazionale di gestione delle crisi cibernetiche

La RT evidenzia che l'articolo 22 individua gli obblighi di comunicazione verso entità dell'Unione europea da parte rispettivamente della Presidenza del Consiglio dei ministri, dell'Agenzia per la cybersicurezza nazionale in qualità di Autorità nazionale competente e Punto di contatto unico NIS, nonché di Autorità nazionale di gestione delle crisi cibernetiche, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva.

Assicura che tali attività sono svolte con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

Al riguardo, per i profili di quantificazione, si conviene con la RT in merito al tenore ordinamentale delle norme. Pertanto, nulla da osservare.

CAPO IV
OBBLIGHI IN MATERIA DI GESTIONE DEL RISCHIO PER LA SICUREZZA INFORMATICA E DI NOTIFICA DI INCIDENTE

Articolo 23

L'articolo disciplina gli obblighi e le responsabilità degli organi di amministrazione e direttivi dei soggetti essenziali e importanti.

Il comma 1 prevede che gli organi di amministrazione e gli organi direttivi dei soggetti "essenziali" e dei soggetti "importanti"**:**

- a) approvano le modalità di messa a punto delle misure di gestione dei rischi per la sicurezza informatica adottate, dagli stessi soggetti essenziali e importanti, ai sensi dell'articolo 24;

- b) sovrintendono all'attivazione degli obblighi del capo IV e di cui all'articolo 7 del decreto;

-c) sono responsabili delle violazioni del decreto in commento compiute dagli stessi soggetti.

Il comma 2 impone agli organi di amministrazione e agli organi direttivi dei soggetti essenziali e dei soggetti importanti di:

a) seguire una formazione in materia di sicurezza informatica.

b) promuovere l'offerta periodica di una formazione, coerente con quella in materia di sicurezza informatica seguita dagli organi citati, in favore dei loro dipendenti. Tale formazione è finalizzata a favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica, nonché il loro impatto sulle attività del soggetto (essenziale o importante) e sui servizi offerti.

Il comma 3 prevede che gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti siano informati periodicamente o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

La RT conferma che il Capo IV (articoli da 23 a 33) è dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente.

Rileva poi che l'articolo in esame indica gli obblighi e le responsabilità degli organi di amministrazione e direttivi dei soggetti essenziali.

La disposizione non comporta nuovi o maggiori oneri a carico della finanza pubblica poiché dette attività rientrano nell'ambito delle attività istituzionali svolte dai soggetti pubblici interessati dall'attuazione della disposizione.

Al riguardo, pur se la RT afferma che le attività previste rientrano tra quelle istituzionali svolte dai soggetti pubblici interessati, andrebbero fornite maggiori informazioni circa le risorse destinate dai soggetti pubblici all'offerta periodica di formazione per i dipendenti e gli organi direttivi.

Articoli 24-38

L'articolo 24 prevede una serie di obblighi per i soggetti essenziali e i soggetti importanti al fine di gestire i rischi per la sicurezza informatica. In particolare, ivi si prevede l'obbligo di adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi, specificandone le caratteristiche e gli elementi essenziali. Stabilisce altresìche, per valutare l'adeguatezza delle misure di sicurezza nella catena di approvvigionamento, i citati soggetti considerino le vulnerabilità specifiche di ogni fornitore e la qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei fornitori,

incluse le loro procedure di sviluppo sicuro. Devono altresì tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

L'articolo 25 introduce una serie di obblighi in materia di notifica degli incidenti. In particolare, come prescritto anche dalla direttiva NIS2, sono previste le seguenti tempistiche: una prenotifica, entro 24 ore da quando i soggetti sono venuti a conoscenza dell'incidente significativo; successivamente, una notifica entro 72 ore; una eventuale relazione intermedia, su richiesta del CSIRT Italia; infine, una relazione finale, entro un mese dalla trasmissione della notifica.

L'articolo 26 disciplina la possibilità, per alcuni soggetti, di trasmettere al CSIRT, su base volontaria, informazioni su incidenti, minacce o quasi-incidenti relativi alla fornitura dei loro servizi. La disposizione si aggiunge a quanto disposto dall'articolo 25 dedicato ai casi per i quali ricade l'obbligo di notifica.

L'articolo 27 conferisce all'Agenzia per la cybersicurezza nazionale in quanto Autorità nazionale competente NIS la possibilità di imporre ai soggetti essenziali e ai soggetti importanti l'utilizzo di determinati prodotti, servizi e processi TIC (tecnologie dell'informazione e della sicurezza).

L'articolo 28 attribuisce all'Autorità nazionale competente NIS la facoltà di promuovere l'uso di specifiche tecniche, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, nonché di predisporre e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica, tenendo conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA.

In particolare, il comma 1 stabilisce che al fine di favorire l'attuazione efficace e armonizzata dell'articolo 24, commi 1 e 2, l'Autorità nazionale competente NIS promuova l'uso di specifiche tecniche europee e internazionali, anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relative alla sicurezza dei sistemi informativi e di rete, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia.

Il comma 2 dispone che l'Autorità nazionale competente NIS tenga conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA ai sensi dell'articolo 25, paragrafo 2, della direttiva (UE) 2022/2555. La medesima Autorità può, inoltre, redigere e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica

Il comma 3 precisa che tale elenco – il quale non ha carattere vincolante o esaustivo – è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale al fine di fornire un orientamento sulle specifiche tecniche, di cui al comma 1, e sulle norme di settore nazionali ed europee applicabili alle tipologie di soggetti di cui agli allegati I, II, III e IV al presente decreto.

L'articolo 29 stabilisce al comma 1 che per contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.

Il comma 2 prevede che ai fini del comma 1, la banca dei dati di registrazione dei nomi di dominio contiene le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio sotto i TLD (*top level domain*). Tali informazioni includono, almeno: a) il nome di dominio; b) la data di registrazione; c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione; d) l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.

Il comma 3 dispone che i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio predispongono e rendono pubbliche politiche e procedure, incluse

le procedure di verifica, al fine di garantire che le banche dati di cui al comma 1 contengano informazioni accurate e complete.

Il comma 4 stabilisce che i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio per i domini di primo livello rendano pubblicamente disponibili, senza ingiustificato ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.

Il comma 5 prevede che i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio, su richiesta motivata dei soggetti legittimati, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione europea in materia di protezione dei dati. I soggetti che gestiscono i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondono senza ingiustificato ritardo e, comunque, entro 72 ore dalla ricezione della richiesta di accesso. Tale risposta reca gli specifici dati di registrazione dei nomi di dominio richiesti, ovvero, le motivazioni per cui la richiesta non è stata ritenuta legittima o debitamente motivata. E' stabilito che le politiche e le procedure relative alla divulgazione di tali dati hanno evidenza pubblica.

Il comma 6 afferma che ai fini del comma 5 l'Agenzia per la cybersicurezza nazionale può richiedere l'accesso ai dati di registrazione dei nomi di dominio e può stipulare appositi protocolli con i gestori di registri dei nomi di dominio di primo livello e i fornitori di registrazione dei nomi di dominio.

Il comma 7 dispone che al fine di evitare una duplicazione della raccolta di dati di registrazione dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio individuano modalità e procedure di collaborazione per la raccolta e il mantenimento dei dati di cui al comma 1.

L'articolo 30 dispone che i soggetti importanti e i soggetti essenziali dal 1° maggio al 30 giugno di ogni anno comunicano e aggiornano un elenco delle proprie attività e dei propri servizi.

In particolare, il comma 1 prevede che ai fini di cui all'articolo 24, comma 1, dal 1° maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione di cui all'articolo 7, comma 3, lettera a), tramite piattaforma digitale di cui all'articolo 7, comma 1, i soggetti essenziali e i soggetti importanti comunichino e aggiornino un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza.

Il comma 2 prevede che l'Autorità nazionale competente NIS stabilisca, secondo le modalità di cui all'articolo 40, comma 5, anche tenuto conto di quanto previsto dall'articolo 25, comma 1, le categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi di cui al presente articolo.

Il comma 3 dispone che entro novanta giorni dalla comunicazione tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS fornisca riscontro ai soggetti essenziali e ai soggetti importanti circa la conformità di quanto comunicato rispetto alle modalità e ai criteri di cui al comma 2. Il predetto termine può essere prorogato dall'Autorità nazionale competente NIS, per una sola volta e fino ad un massimo di ulteriori sessanta giorni, qualora sia necessario svolgere approfondimenti. Ove si renda necessario richiedere integrazioni e informazioni aggiuntive ai soggetti essenziali o importanti, i termini di cui al presente comma sono interrotti sino alla data di ricevimento delle predette integrazioni e informazioni, che sono rese entro il termine di trenta giorni dalla richiesta.

Il comma 4 prevede che in assenza del riscontro di cui al comma 3 da parte dall'Autorità nazionale competente NIS entro i termini di cui al medesimo comma, la conformità di cui al comma 3 si intende convalidata.

Il comma 5 stabilisce che per l'espletamento di tali attività, l'ACN - l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali istituiti per i rispettivi settori di competenza dalla medesima ACN di cui all'articolo 11, comma 4, lettera f) del provvedimento in esame.

L'articolo 31 stabilisce che l'Agenzia, in qualità di Autorità nazionale competente NIS, adotti criteri di proporzionalità e gradualità nella definizione degli obblighi in materia di gestione del rischio di

sicurezza cibernetica e di notifica di incidenti. La norma attribuisce poi alla medesima Autorità il potere di stabilire termini, modalità, specifiche e tempi graduali di implementazione dei suddetti obblighi.

L'articolo 32 prevede che l'Autorità nazionale competente NIS possa imporre obblighi specifici a soggetti essenziali e importanti che forniscono servizi alla pubblica amministrazione. È previsto, inoltre, che alcuni enti possano essere esentati da specifici obblighi. Particolari esenzioni sono, poi, previste per i fornitori di servizi di registrazione dei nomi di dominio. Si prevede infine che, indipendentemente dalla designazione di un rappresentante nell'Unione europea, ai soggetti che offrono servizi nell'Unione, ma sono stabiliti fuori dalla stessa, si applichino gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente.

In particolare, il comma 2 prevede che l'Autorità nazionale competente NIS, con propria determinazione e sentito il Tavolo per l'attuazione della disciplina NIS, possa individuare, tra gli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente (capo IV), quelli che non si applicano:

- alle Città metropolitane, ai Comuni con popolazione superiore a 100.000 abitanti, ai Comuni capoluoghi di regione, alle Aziende sanitarie locali;
- agli enti di regolazione dell'attività economica, agli enti produttori di servizi economici, agli enti a struttura associativa, agli enti produttori di servizi assistenziali, ricreativi e culturali, agli enti e le istituzioni di ricerca, agli Istituti zooprofilattici sperimentali;
- ai soggetti delle tipologie di cui all'allegato IV del decreto, individuati secondo le procedure di cui al comma 13 dell'articolo 3 del provvedimento in commento. Si tratta, in particolare, dei soggetti che forniscono servizi di trasporto pubblico locale, degli istituti di istruzione che svolgono attività di ricerca, dei soggetti che svolgono attività di interesse culturale, delle società *in house*, società partecipate e società a controllo pubblico;
- al soggetto considerato critico, quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti;
- indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri: a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale; b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale; c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale; d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

L'articolo 33 contiene disposizioni di coordinamento con la normativa nazionale relativa al Perimetro di sicurezza nazionale cibernetica in particolare per quel che concerne la disciplina sugli obblighi dei soggetti e dei loro rispettivi sistemi informativi, reti e servizi informatici.

L'articolo 34 attribuisce all'Agenzia per la cybersicurezza nazionale, in quanto Autorità nazionale competente NIS, i compiti di monitoraggio del rispetto degli obblighi previsti dal provvedimento per i soggetti essenziali e per i soggetti importanti. Il comma 1 afferma che le attività di vigilanza saranno svolte attraverso: il monitoraggio, l'analisi e il supporto; la verifica e le ispezioni; l'adozione di misure di esecuzione; l'irrogazione di sanzioni amministrative pecuniarie e accessorie

L'articolo 35 prevede una serie di obblighi di monitoraggio, analisi e supporto in capo all'Agenzia per la cybersicurezza nazionale in quanto Autorità nazionale competente NIS. Al comma 1 si stabilisce che l'Agenzia verifica e fornisce riscontro circa le informazioni trasmesse e la relativa corrispondenza ai requisiti prescritti per i soggetti registrati, ai fini dell'inserimento nell'elenco dei soggetti essenziali e dei soggetti importanti assicurando altresì adeguata pubblicità ai criteri concernenti l'ambito di applicazione del presente decreto e dei relativi obblighi.

Secondo il comma 2, l'Agenzia monitora l'attuazione degli obblighi previsti dal decreto in esame da parte dei soggetti che rientrano nel suo ambito di applicazione, implementando, altresì, interventi di supporto per i soggetti medesimi.

Al comma 3 si prevede che, ai fini dell'attività di monitoraggio di cui al comma 2, la medesima Agenzia può:

a) richiedere ai soggetti una rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi di cui al provvedimento in esame, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali, dichiarando la finalità della richiesta;

b) richiedere ai soggetti l'esecuzione, periodica o mirata, di *audit* sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto;

c) richiedere ai soggetti l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

d) emanare raccomandazioni e avvertimenti relativi a presunte violazioni del presente decreto da parte dei soggetti interessati.

Ai fini del comma 2, l'Agenzia indica modalità e termini ragionevoli e proporzionati per adempiere, nonché per riferire circa lo stato di attuazione degli adempimenti (comma 4). Le risultanze delle attività di cui al presente capo sono analizzate dall'Agenzia stessa al fine di stabilire l'ordine di priorità degli interventi di supporto di cui al comma 2 nonché di individuare gli indirizzi di sviluppo della regolamentazione di cui all'articolo 31 (comma 5). Qualora ciò non costituisca un onere sproporzionato o eccessivo, è la medesima Autorità nazionale competente NIS a implementare gli interventi di supporto di cui al comma 2 (comma 6).

Nello svolgimento delle attività di cui al capo in esame, l'Autorità si può avvalere dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f) (comma 7).

L'articolo 36 prevede che l'Autorità nazionale competente NIS possa effettuare verifiche documentali, ispezioni *in loco* e a distanza, e richiedere dati e informazioni ai soggetti rientranti nell'ambito di applicazione del decreto. Tali poteri possono essere esercitati nei confronti dei soggetti importanti solo qualora ci siano prove o indicazioni di possibili violazioni del decreto.

L'articolo 37 individua le misure di esecuzione attribuite all'Autorità nazionale competente NIS. In particolare, l'Autorità può intimare di eseguire alcuni adempimenti ai soggetti interessati. L'articolo dispone in merito al procedimento per lo svolgimento delle misure di esecuzione: vi è una prima fase dedicata alla notifica delle conclusioni preliminari; vi è quindi la possibilità di controdedurre da parte dei soggetti interessati; l'Autorità procede poi all'intimazione dei comportamenti da tenere; si prevede infine, in caso di mancata ottemperanza, la diffida ad adempiere. Misure specifiche sono previste per i provvedimenti urgenti.

L'articolo 38 prevede che l'Agenzia per la cybersicurezza nazionale è l'autorità competente alla irrogazione delle sanzioni amministrative; disciplina le fattispecie oggetto di sospensione dell'attività e di sanzione amministrativa, il regime della reiterazione delle violazioni, gli strumenti deflattivi del contenzioso e la destinazione dei proventi delle sanzioni amministrative all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale.

La RT rileva sugli articoli 24-26 che questi individuano, nel dettaglio, rispettivamente gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e quelli in materia di "notifica", anche volontaria, di incidente.

Assicura che tali attività sono svolte esclusivamente nell'ambito delle funzioni istituzionali dei soggetti pubblici coinvolti, con le risorse umane, strumentali e

finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

Rileva che l'articolo 27 consente all'Autorità nazionale competente NIS di imporre, ai sensi della direttiva, ai soggetti essenziali e importanti l'utilizzo di determinati prodotti TIC, servizi TIC e processi TIC; sull'articolo 28 evidenzia che attribuisce alla medesima Autorità la facoltà di promuove l'uso di specifiche tecniche per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica; in merito all'articolo 29 rileva che disciplina la banca dei dati di registrazione dei nomi di dominio. Assicura che tali articoli rivestono carattere ordinamentale e, pertanto, non comportano nuovi o maggiori oneri per la finanza pubblica.

Conferma che l'articolo 30 regola la modalità circa l'iscrizione nell'elenco dei soggetti importanti ed essenziali, tramite la piattaforma digitale prevista dall'articolo 7. Assicura che la disposizione riveste carattere ordinamentale e, pertanto, non comporta nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 31 stabilisce che l'Autorità nazionale competente NIS (la ACN) deve prevedere criteri di proporzionalità e gradualità obblighi in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidente; in merito all'articolo 32, afferma che detta regole specifiche per le pubbliche amministrazioni centrali, regionali e locali e per i soggetti essenziali e importanti che forniscono servizi, anche digitali, alle medesime; sull'articolo 33 assicura che le norme recano disposizioni di coordinamento della normativa NIS2 con la disciplina del Perimetro di sicurezza nazionale cibernetica. Nel complesso, assicura che le disposizioni riportate agli articoli 31-33, riguardando attività a prevalente carattere di indirizzo e coordinamento, sono svolte sono svolte nell'ambito delle funzioni istituzionali di ACN con le sole risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

Rileva preliminarmente che il Capo V (articoli dal 34 al 39) disciplina le attività di monitoraggio, vigilanza ed esecuzione a carico dell'Autorità nazionale competente NIS (ACN), con riferimento ai compiti di monitoraggio, di verifica ed ispezioni, all'adozione di misure di esecuzione e all'eventuale irrogazione delle sanzioni.

L'articolo 34 reca principi generali per lo svolgimento delle attività di supervisione e non ha riflessi finanziari.

Quanto all'articolo 35 conferma che la disposizione reca la disciplina delle modalità di effettuazione della attività di monitoraggio, analisi e supporto. Assicura che tali attività saranno svolte nell'ambito delle funzioni istituzionali di ACN con le sole risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica.

Sugli articoli 36-37 evidenzia che le norme disciplinano le attività di verifica e ispezione e la relativa esecuzione dell'esercizio dei poteri da parte dell'Autorità NIS.

Tali compiti - già attualmente svolti da ACN nell'ambito della propria attività istituzionale - non determinano nuovi o maggiori oneri.

Rileva che l'articolo 38 reca disposizioni in materia di sanzioni amministrative. In particolare, sul comma 16, afferma che prevede che i proventi delle sanzioni amministrative pecuniarie irrogate dall'Autorità nazionale competente NIS versati all'entrata del bilancio dello Stato siano oggetto di riassegnazione all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze (cap. 1672) recante la dotazione finanziaria da assegnare annualmente all'ACN. La disposizione, peraltro, è pienamente coerente con l'articolo 11, comma 2, del decreto-legge n. 82 del 2021 che, alla lettera f), indica i predetti proventi delle sanzioni tra le entrate dell'Agenzia.

Sul punto specifica, altresì, che l'acquisizione in bilancio di risorse aggiuntive derivanti dalle predette sanzioni rappresenta per l'ACN una mera eventualità; le stesse, infatti, hanno il fine esclusivo di rappresentare un efficace strumento di deterrenza volto a garantire l'attuazione delle misure previste dal provvedimento.

Assicura, infine, che i proventi in discorso rappresentano una nuova voce di entrata del bilancio dello Stato, non essendovi fino ad oggi somme versate per la medesima causale. Pertanto, la previsione di riassegnazione all'ACN degli eventuali introiti ha carattere di neutralità finanziaria e non determina riflessi negativi sui saldi di bilancio.

Al riguardo, vanno segnalate le prescrizioni dell'articolo 24, laddove è previsto l'obbligo per i "soggetti essenziali" e i "soggetti importanti" di porre in essere le misure tecniche, operative e organizzative "adeguate e proporzionate alla gestione dei rischi per la sicurezza informatica" e ciò "senza indebito ritardo", nonché "tutte le misure appropriate e proporzionate correttive necessarie". Andrebbe pertanto approfondita l'affermazione della RT secondo cui si tratterebbe di attività già svolte dai soggetti pubblici interessati.

In merito a quanto previsto dagli articoli da 34 a 38, si prende atto delle rassicurazioni fornite dalla RT che le attività di monitoraggio, analisi e supporto, verifica, ispezione e irrogazione di sanzioni saranno svolte nell'ambito delle funzioni istituzionali di ACN, con le sole risorse umane, strumentali e finanziarie disponibili a legislazione vigente, anche se andrebbero fornite informazioni specifiche circa le risorse di cui l'Agenzia dispone per lo svolgimento di tali attività.

Per quanto riguarda i proventi delle sanzioni, trattandosi di effetti in conto di maggiori entrate non stimabili preventivamente, non ci sono osservazioni.

Articolo 39

L'articolo disciplina le modalità di cooperazione e assistenza reciproca tra l'Autorità nazionale competente NIS e le Autorità competenti degli altri Stati membri.

Il comma 1 conferma che l'Autorità nazionale competente NIS, che come detto corrisponde all'Agenzia per la cybersicurezza nazionale, aderisce al circuito di cooperazione e assistenza con le Autorità competenti degli altri Stati membri, e ne regola le modalità di partecipazione.

Il comma 2 precisa che la cooperazione comprende, in particolare, la notifica e la consultazione tramite il Punto di contatto unico NIS circa le attività ispettive e le misure di esecuzione (lettera a)) che possono essere oggetto di una richiesta giustificata (lettera b)) e prevedere interventi di assistenza

proporzionata alle risorse per garantire un'attuazione efficace, efficiente e coerente (lettera c)). Tali interventi, ai sensi del comma 3, possono riguardare richieste di informazioni e attività ispettive anche *in loco* o *audit* sulla sicurezza mirati.

Il comma 4 contiene disposizioni in merito ai casi in cui l'Autorità nazionale competente NIS possa respingere una richiesta di assistenza. Si tratta, in particolare, dei casi in cui l'Autorità richiedente non è competente (lettera a)), oppure se l'attività richiesta non è proporzionata ai compiti previsti dallo schema di decreto (lettera b)) o se riguarda attività il cui svolgimento contrasta con gli interessi essenziali di sicurezza nazionale, di pubblica sicurezza o di difesa dello Stato (lettera c)).

A tali fini, il comma 5 stabilisce che prima di respingere una richiesta l'Autorità nazionale competente consulta le autorità degli Stati membri interessati e su richiesta anche solo di uno di essi può interpellare la Commissione europea e l'ENISA.

Ai sensi del comma 6, poi, sono previste attività ispettive o di esecuzioni comuni tra le Autorità competenti nazionali.

Il comma 7 attribuisce, inoltre, alla lettera a), all'Autorità nazionale competente NIS, in caso di richiesta di assistenza da parte di Autorità competenti di altri Stati membri, la possibilità di esercitare i poteri di monitoraggio, vigilanza ed esecuzione di cui al Capo V del presente schema di decreto nei confronti di un soggetto che risponde ai requisiti espressi al comma 1, lettera a) dell'articolo in commento.

Infine, secondo la lettera b) del comma 7, l'Autorità nazionale competente NIS può anche inoltrare una richiesta di assistenza reciproca alle autorità degli altri Stati membri per l'esercizio dei poteri relativi alle misure di gestione del rischio di cybersicurezza, di cui al Capo IV della direttiva (UE) 2022/2555, nei confronti dei soggetti individuati al comma 1, lettera b), dell'articolo in commento.

La RT non si sofferma sulla disposizione.

Al riguardo, per i profili di quantificazione, ritenuto il mero rilievo ordinamentale delle norme, non ci sono particolari osservazioni.

CAPO VI
DISPOSIZIONI FINALI E TRANSITORIE

Articolo 40

L'articolo 40 disciplina l'adozione dei provvedimenti attuativi previsti dal provvedimento. Si tratta di decreti del Presidente del Consiglio dei ministri (DPCM) e di determinazioni dell'Agenzia per la cybersicurezza nazionale.

Per i DPCM, i commi 1, 2 e 3 affermano che gli stessi saranno adottati "anche in deroga all'articolo 17" della legge n. 400 del 1988

I commi 4 e 5 ricapitolano quelle che sono le determinazioni che l'Agenzia per la cybersicurezza nazionale dovrà adottare per l'attuazione del provvedimento.

Il comma 10 dispone che i decreti del Presidente del Consiglio dei ministri di cui al presente articolo sono aggiornati periodicamente e, comunque, ogni tre anni.

Il comma 11 prevede che le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al presente articolo sono aggiornate periodicamente e, comunque, ogni due anni.

La RT non si sofferma sulle norme.

Al riguardo, nulla da osservare.

Articolo 41

L'articolo dispone l'abrogazione del D.Lgs. n. 65 del 2018 di recepimento della prima direttiva NIS e degli articoli 40 ("*Sicurezza delle reti e dei servizi*") e 41 ("*Attuazione e controllo*") del D.Lgs. n. 259 del 2003 recante "Codice delle comunicazioni elettroniche", prevedendo una fase transitoria fino all'emanazione dei provvedimenti attuativi del decreto. Si prevede, inoltre, al D.Lgs. n. 259 del 2003, l'abrogazione della lettera h) dell'articolo 2, comma 1, e l'abrogazione dell'articolo 30, comma 26. In particolare l'articolo 7, comma 8 (recante un'autorizzazione di spesa di 1,3 milioni di euro annui in favore dell'Agenzia per la cybersicurezza nazionale) e l'articolo 8, comma 10 (recante un'autorizzazione di spesa di 2 milioni di euro annui per le spese relative al funzionamento del CSIRT) sono abrogati a partire dall'anno 2025.

La RT conferma che l'articolo reca disposizioni abrogative e che fa salva la vigenza delle autorizzazioni di spesa di cui agli articoli 7, comma 8, e 8, comma 10, del d.lgs. n. 65/2018 fino al 1° gennaio 2025.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica ascrive alle norme i seguenti effetti, in conto minori spese correnti:

(milioni di euro)

Art.	Descrizione	e/s	nat	Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
				2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
41	Abrogazione del D.Lgs. 65/2018, di attuazione della direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione	S	C		-3,30	-3,22	-2,83		-3,30	-3,22	-2,83		-3,30	-3,22	-2,83

Al riguardo, nulla da osservare, in relazione ai risparmi che conseguono dall'abrogazione dall'anno 2025 degli articoli 7, comma 8, e 8, comma 10, del d.lgs. n. 65/2018. Tuttavia, poiché secondo il prospetto riepilogativo tali risparmi ammontano ai 3,3 milioni di euro previsti complessivamente dalle norme citate soltanto nell'anno 2025, per poi diminuire progressivamente negli anni successivi, andrebbe data conferma di tale dinamica discendente illustrandone le ragioni.

Articolo 42

Il comma 1, lett. a), dell'articolo 42 dispone che, in fase di prima applicazione, alcuni dei soggetti essenziali e importanti tenuti alla registrazione alla piattaforma digitale ai sensi dell'articolo 7 del presente decreto sono tenuti a registrarsi entro il 17 gennaio 2025. Si tratta in particolare dei seguenti soggetti:

- i fornitori di servizi di sistema dei nomi di dominio;
- i gestori di registri dei nomi di dominio di primo livello;
- i fornitori di servizi di registrazione dei nomi di dominio;

- i fornitori di servizi di *cloud computing*;
- i fornitori di servizi di *data center*;
- i fornitori di reti di distribuzione dei contenuti;
- i fornitori di servizi gestiti;
- i fornitori di servizi di sicurezza gestiti;
- i fornitori di mercati *online*, di motori di ricerca *online* e di piattaforme di servizi di *social network*.

Il comma 1, lett. b), prevede che, fino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS si riunisce almeno una volta ogni 60 giorni (ai sensi dell'art. 12, comma 4, il Tavolo NIS è tenuto, a regime, a riunirsi almeno una volta ogni tre mesi).

Il comma 1, lett. c), stabilisce che, fino al 31 dicembre 2025, il termine per l'adempimento degli obblighi in materia di notifica di incidenti (di cui all'articolo 25) è fissato in 9 mesi dalla ricezione della comunicazione, da parte dell'autorità NIS, con la quale viene notificato agli enti interessati l'inserimento nell'elenco dei soggetti essenziali e importanti. Parimenti, il termine per l'adempimento degli obblighi di cui agli articoli 23 e 24 (approvazione delle modalità di implementazione delle misure di gestione dei rischi) e 29 (realizzazione della banca dati di registrazione dei nomi di dominio) è fissato in 18 mesi dalla comunicazione di cui sopra.

Ai sensi del comma 2 i soggetti essenziali ed importanti comunicano l'elenco delle proprie attività a partire dal 1° gennaio 2026 (a regime si prevede che la comunicazione avvenga ogni anno dal 1° maggio al 30 giugno, v. art. 31, comma1).

Infine, i soggetti essenziali e i soggetti importanti possono registrarsi alla piattaforma digitale a partire dalla data di pubblicazione della medesima piattaforma di cui all'articolo 7, comma 1, cui sono tenuti a registrarsi e ad aggiornare la propria registrazione, a regime. dal 1° gennaio al 28 febbraio di ogni anno (comma 3).

La RT non si sofferma sulle norme.

Al riguardo, non ci sono osservazioni.

Articolo 43

L'articolo 43 reca alcune modifiche normative ai decreti-legge n. 82/2021 e n. 105/2019, volte ad assicurare la coerenza delle disposizioni introdotte con l'architettura nazionale di cybersicurezza, con i compiti dell'ACN nonché con il perimetro di sicurezza nazionale cibernetica.

La RT non si sofferma sulle disposizioni.

Al riguardo, nulla da osservare.

Articolo 44

Il comma 1 assicura la coerenza delle spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 10, 11, 13 e 15 del presente decreto e, più in generale, le spese ICT sostenute per l'adeguamento dei sistemi informativi al presente decreto con il Piano triennale per l'informatica nella pubblica amministrazione

Il comma 2 stabilisce che agli oneri derivanti dagli articoli 10, 11, 13, comma 1, e 15, pari a 409.424 euro per l'anno 2024 e a 5.925.695 euro annui a decorrere dall'anno 2025, si provvede:

a) quanto a 409.424 euro per l'anno 2024, 2.625.695 euro per l'anno 2025, 2.707.695 euro per l'anno 2026 e 3.100.695 euro annui a decorrere dall'anno 2027, mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234;

b) quanto a 3.300.000 euro per l'anno 2025, 3.218.000 euro per l'anno 2026 e 2.825.000 euro annui a decorrere dall'anno 2027, mediante utilizzo delle risorse rivenienti dall'abrogazione di cui al comma 1 dell'articolo 41.

Il comma 3 prevede che dall'attuazione del presente decreto, ad esclusione dell'articolo 11 per l'anno 2024 e degli articoli 10, 11, 13, comma 1, e 15 a decorrere dall'anno 2025, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e le amministrazioni pubbliche provvedono con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

La RT si limita a ribadire il contenuto della norma.

Il prospetto riepilogativo degli effetti d'impatto attesi sui saldi di finanza pubblica ascrive alle norme i seguenti effetti:

(milioni di euro)

Co.	Lett.	Descrizione	e/s	nat	Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
					2024	2025	2026	2027	2024	2025	2026	2027	2024	2025	2026	2027
2	a)	Riduzione del Fondo per il recepimento della normativa europea di cui all'art. 41-*bis* della L. 234/2012	S	C	-0,41	-2,63	-2,71	-3,10	-0,41	-2,63	-2,71	-3,10	-0,41	-2,63	-2,71	-3,10

Al riguardo, per i profili di copertura, in relazione alla riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234, verificata l'esistenza delle occorrenti disponibilità[10], andrebbero fornite rassicurazioni circa l'adeguatezza delle rimanenti risorse a fronte del recepimento di direttive europee già programmate con oneri previsti per le stesse annualità e a decorrere.

Quanto alle risorse derivanti dall'abrogazione disposta dall'articolo 41 si rinvia alla relativa scheda.

[10] Si tratta del capitolo 2815 iscritto nello stato di previsione del Ministero dell'economia e delle finanze che reca uno stanziamento di 124 milioni di euro per il 2024 e una disponibilità di competenza (al 26 giugno 2024) di 56,6 milioni di euro, con risorse già accantonate per un importo pari a 4,7 milioni di euro. Per il 2025 e 2026 lo stanziamento è, rispettivamente, di 105,3 milioni e 102,9 milioni (di cui disponibili 88,1 milioni per il 2025 e 85,6 milioni per il 2026). Cfr. Ministero dell'economia e delle finanze, Dipartimento della R.G.S., I.G.B., Sistema *Datamart/RGS*, interrogazione al 26 giugno 2024 sulla dotazione del capitolo 2815 dello Stato di previsione del MEF.