PROVVEDIMENTO URGENTE IN DIRAMAZIONE

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

Presidenza del Consiglio dei Ministri
DAGL 0007197 P-
del 12/07/2019

24256773

Roma 12 LUG. 2019

A TUTTI I CAPI
UFFICIO LEGISLATIVO
LORO SEDI

Al Ragioniere Generale dello Stato
R O M A

52606/10.3.1

OGGETTO: schema di disegno di legge in materia di perimetro di sicurezza nazionale cibernetica

(PRESIDENZA)

Ai fini di cui all'art. 2, comma 3, della legge 23 agosto 1988, n. 400, e dell'art. 3, comma 4, del D.P.C.M. 10 novembre 1993, si trasmette lo schema del provvedimento in oggetto, da sottoporre al Consiglio dei Ministri, previo esame del Preconsiglio.

d'ordine del
PRESIDENTE DEL CONSIGLIO DEI MINISTRI

SCHEMA DI DISEGNO DI LEGGE IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Art. 1

(Perimetro di sicurezza nazionale cibernetica)

1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica.
2. Entro sei mesi dalla data di entrata in vigore della presente legge, con decreto del Presidente del Consiglio dei ministri, che ne disciplina altresì i relativi termini e modalità attuative, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):
   a) fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, sono individuati le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati di cui al comma 1, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; all'identificazione si procede sulla base dei seguenti criteri:
      1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
      2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;
   b) sono definiti i criteri in base ai quali i soggetti di cui alla precedente lettera a) predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante dell'Agenzia per l'Italia digitale (AgID); entro sei mesi dalla data di entrata in vigore della presente legge, i soggetti pubblici e quelli di cui all'articolo 29, del decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi della lettera a), trasmettono tali elenchi ad AgID; i soggetti privati di cui alla medesima lettera a), trasmettono tali elenchi al Ministero dello sviluppo economico; l'AgID e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.
3. Entro dodici mesi dalla data di entrata in vigore della presente legge, con decreto del Presidente del Consiglio dei ministri, che ne disciplina altresì i relativi termini e modalità attuative, adottato su proposta del CISR:
   a) sono definite le procedure secondo cui i soggetti individuati ai sensi del comma 2, lettera a), notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera b), al Gruppo di intervento per la sicurezza informatica in caso di incidente

(CSIRT) italiano, che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche così ricevute all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché ad AgID, se provenienti da un soggetto pubblico o di cui all'articolo 29, del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b), relative a: politiche di sicurezza; gestione del rischio; prevenzione, mitigazione e gestione di incidenti; struttura organizzativa in materia di sicurezza; protezione fisica e logica; protezione dei dati; integrità delle reti e dei sistemi informativi; continuità operativa; gestione operativa; monitoraggio, test e controllo; formazione e consapevolezza; affidamento di forniture di beni, sistemi e servizi ICT, anche mediante definizione di caratteristiche e requisiti di carattere generale; all'elaborazione di tali misure provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante dell'Agenzia per l'Italia digitale (AgID).

4. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalità di cui ai predetti commi con cadenza almeno biennale.

5. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dodici mesi dalla data di entrata in vigore della presente legge, sono disciplinati le procedure, le modalità e i termini con cui:

   a) fatto salvo quanto previsto dall'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni e di servizi ICT cui sia indispensabile procedere in sede estera, i soggetti di cui al comma 2, lettera a), che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), diversi da quelli necessari per lo svolgimento delle attività di prevenzione e di repressione dei reati, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, che, sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, può, entro 30 giorni, imporre condizioni e test di hardware e software; in tale ipotesi, i relativi bandi di gara o contratti vengono integrati di clausole che subordinano l'affidamento della fornitura o del servizio al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN; per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, individuati ai sensi del comma 2, lettera b), il predetto Ministero procede, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dalla presente legge, attraverso un proprio Centro di valutazione in raccordo con AgID e Ministero dello sviluppo economico per i profili di rispettiva competenza; resta fermo che per lo svolgimento delle attività di prevenzione e di repressione dei reati e nei casi in cui si deroga all'obbligo di cui alla presente lettera, sono utilizzati reti, sistemi informativi e servizi informatici conformi ai livelli di sicurezza di cui al comma 3, lettera b), qualora non incompatibili con gli specifici impieghi cui essi sono destinati;

   b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera b), assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, al Centro di valutazione operante presso il Ministero della difesa, la propria collaborazione per l'effettuazione delle attività di test di cui al

comma 5, lettera a), sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o ad AgID, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì ad AgID le analoghe segnalazioni del Centro di valutazione del Ministero della difesa;

c) AgID, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera a), e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera b), dal comma 3 e dalla lettera a) del presente comma e senza che ciò comporti accesso a dati o metadati personali e amministrativi, impartendo, se necessario, specifiche prescrizioni; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera b), connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché in tema di prevenzione e di contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti all'AgID per i profili di competenza.

6. Nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), il CVCN assume i seguenti compiti:
   a) contribuisce all'elaborazione delle misure di sicurezza di cui al comma 3, lettera b), per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;
   b) ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, svolge le attività di cui al comma 5, lettera a), dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dodici mesi dalla data di entrata in vigore della presente legge, su proposta del CISR, impiegando, per le esigenze delle Amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni;
   c) elabora e adotta, previo conforme avviso dell'organismo tecnico di supporto al CISR, schemi di certificazione cibernetica, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.
7. I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-ter, comma 2, del decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:
   a) osservano le misure di sicurezza previste, rispettivamente, dai predetti decreti legislativi, ove di livello almeno equivalente a quelle adottate ai sensi del comma 3, lettera b); le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dalla presente legge sono definite da AgID, per i soggetti pubblici e per quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera a), e dal Ministero dello sviluppo economico per i soggetti privati di cui al medesimo comma, avvalendosi anche del CVCN; il Ministero dello sviluppo economico e l'AgID si raccordano, ove necessario, con le autorità competenti di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65;
   b) assolvono l'obbligo di notifica di cui al comma 3, lettera a), che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-ter del decreto

legislativo 1° agosto 2003, n. 259, e delle correlate disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera a), anche in relazione alle disposizioni di cui all'articolo 16-ter del decreto legislativo 1° agosto 2003, n. 259, il CSIRT italiano inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera a), all'autorità competente di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.

8. Salvo che il fatto costituisca reato, in caso di violazione delle disposizioni di cui al presente articolo si applicano le sanzioni amministrative pecuniarie di seguito indicate:
   a) per il mancato adempimento dell'obbligo di cui al comma 2, lettera b), si applica una sanzione da euro 200.000 a euro 1.200.000;
   b) per la mancata o tardiva notifica di cui al comma 3, lettera a), si applica una sanzione da euro 250.000 a euro 1.500.000;
   c) per l'inosservanza delle misure di sicurezza di cui al comma 3, lettera b), si applica una sanzione da euro 250.000 a euro 1.500.000;
   d) per la mancata comunicazione di cui al comma 5, lettera a), si applica una sanzione da euro 300.000 a euro 1.800.000;
   e) per l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), non ottemperando alle condizioni ovvero in assenza del superamento dei test di cui al comma 5, lettera a), si applica una sanzione da euro 300.000 a euro 1.800.000;
   f) per la mancata collaborazione nei confronti del CVCN ovvero del Centro di valutazione del Ministero della difesa da parte dei soggetti di cui al comma 5, lettera b), ai fini delle attività di test di cui al comma 5, lettera a), si applica una sanzione da euro 250.000 a euro 1.500.000;
   g) per il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o da AgID in esito alle attività di ispezione e verifica ai sensi del comma 5, lettera c), si applica una sanzione da euro 250.000 a euro 1.500.000;
   h) per il mancato rispetto delle prescrizioni di cui al comma 6, lettera b), si applica una sanzione da euro 250.000 a euro 1.500.000.
9. In caso di inottemperanza alle condizioni o in assenza dell'esito favorevole dei test di cui al comma 5, lettera a), la stipula del contratto non produce effetto ed è fatto divieto alle parti di darvi, anche provvisoriamente, esecuzione. La violazione di tale divieto comporta, per coloro che abbiano disposto l'affidamento del contratto, l'incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle società aventi ad oggetto, anche se non principale, attività afferenti alle tecnologie dell'informazione e della comunicazione, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.
10. Chiunque, tenuto ad effettuare le comunicazioni richieste nell'espletamento dei procedimenti di cui al comma 2, lettera b), al comma 5, lettera a), ovvero delle attività ispettive e di vigilanza previste dal comma 5, lettera c), fornisce informazioni e dati non rispondenti al vero ovvero espone fatti parimenti non rispondenti al vero, allo scopo di ostacolare o condizionare l'espletamento dei medesimi procedimenti o attività, ovvero allo stesso scopo omette di comunicare informazioni, dati o fatti necessari per tali procedimenti o attività, è punito con la pena della reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a 400 quote.
11. Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni sono l'AgiD, per i soggetti pubblici e per i soggetti di cui all'articolo 29, del decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera a), e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma.
12. Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 8, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689. La reiterazione della violazione determina l'aumento fino al triplo della sanzione prevista.

13. Per i dipendenti dei soggetti pubblici individuati ai sensi del comma 2, lettera a), la violazione delle disposizioni di cui al presente articolo costituisce elemento di responsabilità disciplinare e amministrativo-contabile.
14. Le autorità titolari delle attribuzioni di cui alla presente legge assicurano gli opportuni raccordi con il Dipartimento delle informazioni per la sicurezza e con l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.
15. All'articolo 4, comma 5, del decreto legislativo 18 maggio 2018, n. 65, dopo le parole "un elenco nazionale degli operatori di servizi essenziali." sono aggiunte le seguenti: "Il Ministero dello sviluppo economico inoltra tale elenco al punto di contatto unico e all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.".
16. All'articolo 8, comma 9, del decreto legislativo 18 maggio 2018, n. 65, le parole "a far data dalla entrata in vigore del" sono sostituite dalle seguenti: "a decorrere dalla data indicata dal".
17. All'articolo 9, comma 3, del decreto legislativo 18 maggio 2018, n. 65, le parole "e il punto di contatto unico" sono sostituite dalle seguenti: ", il punto di contatto unico e l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155".
18. Gli eventuali adeguamenti alle prescrizioni di sicurezza definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2, lettera a), sono effettuati con le risorse finanziarie disponibili a legislazione vigente.
19. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione e certificazione nazionale (CVCN) di cui al comma 5 è autorizzata la spesa di 3,2 milioni di euro per l'anno 2019 e di 2,850 milioni di euro per ciascuno degli anni dal 2020 al 2023 e di 0,750 milioni di euro annui a decorrere dall'anno 2024.

Art. 2

(Personale per esigenze di funzionamento del CVCN e di AgID)

1. Tenuto conto dell'esigenza di disporre di personale in possesso della professionalità necessaria per lo svolgimento delle funzioni del CVCN, di cui all'articolo 1, comma 6, il Ministero dello sviluppo economico è autorizzato ad assumere a tempo indeterminato, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facoltà assunzionali, un contingente massimo di 57 unità reclutate dal Dipartimento della funzione pubblica utilizzando le modalità semplificate previste dall'articolo 3 della legge 19 giugno 2019, n. 56, nel limite di spesa annua di euro 1.002.000 per l'anno 2019 ed euro 3.005.000 annui a decorrere dall'anno 2020.
2. Fino al completamento delle procedure di cui al comma 1, il Ministero dello sviluppo economico, fatte salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, può avvalersi, per le esigenze del CVCN di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo o di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, per un massimo del 40% delle unità di personale di cui

al comma 1. Nei limiti complessivi della stessa quota il Ministero dello sviluppo economico può avvalersi in posizione di comando di personale con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa fino a un massimo di 20 unità, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico dell'amministrazione di appartenenza e successivo rimborso da parte del Ministero dello sviluppo economico dei soli oneri relativi al trattamento accessorio di cui al fondo efficienza servizi istituzionali.

3. Per lo svolgimento delle nuove funzioni come previste all'articolo 1, l'AgID è autorizzata ad assumere con contratti di lavoro a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di 10 unità di personale da inquadrare nella III area del personale non dirigenziale, posizione economica F1, nel limite di spesa di euro 171.000 per l'anno 2019 ed euro 512.000 annui a decorrere dall'anno 2020.
4. Fino al completamento delle procedure di cui al comma 3, l'AgID, fatte salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, può avvalersi, entro il limite del 40% delle unità previste dal medesimo comma, di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1 comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo, di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127 e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, nonché di esperti o consulenti, nominati ai sensi dell'articolo 7, comma 6, del decreto legislativo 30 marzo 2001, n. 165, in possesso di particolare e comprovata specializzazione in materia informatica.
5. Il reclutamento del personale di cui ai commi 1 e 3 avviene mediante uno o più concorsi pubblici espletati secondo le modalità previste dall'articolo 4, commi 3 e 3-bis, del decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla legge 30 ottobre 2013, n. 125, dall'articolo 35, comma 5, del decreto legislativo 30 marzo 2001, n. 165, e dall'articolo 3, comma 6, della legge 19 giugno 2019, n. 56.

Art. 3
(Copertura finanziaria)

1. Agli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi 4,373 milioni di euro per l'anno 2019, 6,367 per ciascuno degli anni dal 2020 al 2023, e 4,267 euro annui a decorrere dall'anno 2024, si provvede:

a) quanto a 1,173 milioni di euro per l'anno 2019 e a 4,267 milioni di euro annui a decorrere dal 2020, mediante corrispondente riduzione dello stanziamento del Fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del Programma Fondi di riserva e speciali della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2019, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero dello sviluppo economico per 0,474 milioni di euro per l'anno 2019 e per 0,350 milioni di euro annui a decorrere dall'anno 2020 e l'accantonamento relativo al Ministero dell'economia e delle finanze per 0,699 milioni di euro per l'anno 2019 e per 3,917 milioni di euro annui a decorrere dall'anno 2020;

b) quanto a 3,2 milioni di euro per l'anno 2019 e a 2,1 milioni di euro per ciascuno degli anni dal 2020 al 2023, mediante corrispondente utilizzo dell'autorizzazione di spesa recata dall'articolo 1, comma 95, della legge 30 dicembre 2018, n. 145, da imputare sulla quota parte del fondo attribuita al Ministero dello sviluppo economico.

2. Il Ministro dell'Economia e delle Finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

RELAZIONE ILLUSTRATIVA

La pervasività assunta dalle reti e dai sistemi informativi e dai servizi informatici per l'espletamento di funzioni essenziali dello Stato, ovvero per la prestazione di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali, rende immediata e sempre più grave e concreta l'evenienza di situazioni di possibile malfunzionamento, interruzione, anche parziale, ovvero utilizzo improprio di tali reti, sistemi informativi e servizi informatici, con serio pregiudizio per la sicurezza nazionale: è quindi urgente la necessità di apprestare misure e procedure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi consentendo, al contempo, la estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Il disegno di legge reca disposizioni volte ad assicurare, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica (di seguito "perimetro"), un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, e dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

La formulazione delle norme è improntata ai seguenti criteri:

- definizione delle finalità del perimetro e delle modalità di individuazione tanto dei soggetti pubblici e privati che ne fanno parte quanto delle rispettive reti, sistemi informativi e servizi informatici rilevanti per le finalità di sicurezza nazionale cibernetica (di seguito "reti, sistemi e servizi rilevanti"), per i quali si applicano le misure di sicurezza e le procedure che vengono introdotte con l'intervento normativo. Al fine di circoscrivere il novero dei soggetti da includere nel perimetro sono stati introdotti – così come già praticato dal legislatore nel decreto di recepimento della Direttiva UE NIS per la designazione degli operatori di servizi essenziali – criteri di carattere generale in base ai quali il Comitato interministeriale per la sicurezza della Repubblica (CISR) procederà alla loro individuazione;
- previsione di un'architettura normativa snella. In particolare, l'attuazione è demandata, con scadenze temporali diversificate, a tre decreti del Presidente del Consiglio dei ministri (DPCM) adottati su proposta del CISR, e a un regolamento da emanare ai sensi dell'articolo 17, comma 1 della legge 23 agosto 1988, n. 400;
- possibilità di agevole aggiornamento dei citati DPCM, per rispondere a una duplice finalità: mantenere la normativa al passo con l'evoluzione tecnologica e consentire un graduale ampliamento del novero dei soggetti da includere nel perimetro;
- coinvolgimento del CISR quale proponente dei DPCM applicativi. Ciò, in quanto si tratta di provvedimenti che dettano misure rivolte alla tutela della sicurezza nazionale in campo cibernetico. In questo ambito, il CISR si avvale, quale supporto a fini istruttori, del c.d. CISR-tecnico di cui all'articolo 5 del decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, presieduto dal Direttore generale del Dipartimento delle

informazioni per la sicurezza (DIS), con la partecipazione dei Vertici amministrativi dei Dicasteri interessati. In tal modo è pertanto assicurata la collegialità dei processi attuativi del perimetro;

- previsione di misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi e dei servizi rilevanti;
- istituzione di un meccanismo teso ad assicurare un *procurement* più sicuro per i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti. Il processo di verifica viene effettuato dal Centro di valutazione e certificazione nazionale (CVCN) sulla base di una valutazione del rischio anche in relazione all'ambito di impiego e in un'ottica di gradualità, limitando le procedure più onerose in termini di tempi e costi solamente alla componentistica più critica. In proposito, sono stati esclusi gli approvvigionamenti necessari per le attività di prevenzione e repressione dei reati ed è stato previsto di demandare al DPR attuativo la disciplina dei casi di deroga per le forniture in sede estera;
- individuazione delle competenze del Ministero dello sviluppo economico (MiSE) – per i soggetti privati inclusi nel perimetro – e dell'Agenzia per l'Italia Digitale (AgID) – per le amministrazioni pubbliche e i soggetti di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (CAD) inclusi nel perimetro – in coerenza con le funzioni già esercitate da tali soggetti istituzionali alla luce delle norme vigenti. In particolare, il MiSE quale: autorità competente con poteri ispettivi e sanzionatori (per i settori energia, infrastrutture digitali e per i servizi digitali) e depositario dell'elenco degli operatori di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva europea NIS; autorità di riferimento con poteri ispettivi e sanzionatori verso i fornitori di servizi di comunicazione elettronica ai sensi del decreto legislativo 1° agosto 2003, n. 259, e correlate disposizioni attuative (quali il c.d. 'decreto Telco'); organismo di certificazione e sicurezza informatica presso cui è stato istituito il Centro di Valutazione e Certificazione Nazionale (CVCN) ai sensi dell'articolo 11 del DPCM 17 febbraio 2017;
- disciplina dei compiti del CVCN nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti;
- semplificazione della procedura di notifica di incidente per i soggetti (OSE, FSD e operatori 'Telco') che siano ad un tempo inclusi nel perimetro e sottoposti agli obblighi stabiliti dal decreto legislativo 18 maggio 2018, n. 65, o dal decreto legislativo 1° agosto 2003, n. 259, prevedendo che le segnalazioni effettuate secondo la presente disciplina valgano anche quale adempimento degli analoghi obblighi previsti dai suddetti ambiti normativi;
- istituzione di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti – prevedendo che AgID e MiSE svolgano attività di ispezione e verifica e impartiscano, ove necessario, le opportune prescrizioni – nonché di un articolato sistema sanzionatorio per i casi di violazione, nella forma della sanzione penale e amministrativa pecuniaria nonché della misura interdittiva a ricoprire incarichi societari nel settore ICT, prevedendone altresì, per i dipendenti pubblici, la valutazione sotto i profili della responsabilità disciplinare e amministrativo-contabile. Una specifica disciplina in tema di ispezioni e verifiche è stata prevista per le reti, i sistemi e i servizi rilevanti connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica nonché per quelli connessi alla difesa e sicurezza militare dello Stato;

- in tale contesto è stato disposto che le attività di ispezione e verifica siano svolte, senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi nonché per quanto riguarda la prevenzione e il contrasto del crimine informatico delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti all'AgID per i profili di competenza;
- previsione di un raccordo tra le autorità titolari delle attribuzioni di cui alla presente legge e Dipartimento delle informazioni per l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'art. 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

L'articolo 1 definisce finalità e ambito di applicazione del perimetro.

Il comma 2 dell'articolo 1 demanda a un DPCM, da adottare su proposta del CISR entro sei mesi dalla data di entrata in vigore della presente legge, l'individuazione dei soggetti rientranti nel perimetro – ferma restando, per gli organismi di informazione e sicurezza, la specifica disciplina di cui alla legge 3 agosto 2007, n. 124 e successive modificazioni – e dei criteri per la formazione degli elenchi delle reti, dei sistemi e dei servizi rilevanti. L'elaborazione di tali criteri è affidata al CISR-tecnico, organismo già esistente (art. 5 del DPCM 17 febbraio 2017), di supporto del Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della medesima legge n. 124 del 2007, che, allo scopo, adotterà i più idonei moduli organizzativi – integrato con la partecipazione di un rappresentante dell'AgID. Sul punto è stato, inoltre, stabilito che, all'interno del perimetro, le amministrazioni pubbliche e i soggetti di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (CAD) trasmettono tali elenchi ad AgID e che i soggetti privati li inviino al MiSE. AgID e MiSE, a loro volta, li inoltrano, in relazione alle attività di rispettiva competenza, al DIS e all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

Il comma 3 demanda a un DPCM – da adottare su proposta del CISR entro dodici mesi dalla data di entrata in vigore della presente legge – la definizione, con la previsione di termini e modalità attuative:

a) delle procedure per la notifica di incidenti, aventi impatto sulle reti, i sistemi e i servizi rilevanti, al CSIRT italiano, che le inoltra al DIS. Il Dipartimento ne assicura la successiva trasmissione all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 nonché ad AgID, se provenienti da un soggetto pubblico o di cui all'articolo 29, del decreto legislativo 7 marzo 2005, n. 82, ovvero al MiSE, se effettuate da un soggetto privato;
b) delle misure volte a garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi rilevanti, che devono essere rispettate dai soggetti inclusi nel perimetro. Al riguardo, viene disposto che all'elaborazione di tali misure provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con rappresentante dell'Agenzia per l'Italia digitale (AgID).

Il comma 4 prevede che all'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si provveda secondo le modalità di cui ai medesimi commi con cadenza almeno biennale.

Il comma 5 demanda a un regolamento – da emanare ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dodici mesi dalla data di entrata in vigore della presente legge– la definizione di procedure, modalità e termini con cui:

a) i soggetti inclusi nel perimetro, per l'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per l'espletamento dei servizi rilevanti, sono tenuti a darne comunicazione al CVCN che – entro 30 giorni – può imporre condizioni, quali una certificazione di sicurezza informatica, e test di hardware e software sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità. In questo caso, i relativi bandi di gara o contratti devono essere integrati di clausole che subordinano l'affidamento della fornitura o del servizio al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. In proposito, sono state eccettuate le forniture necessarie per le attività di prevenzione e repressione dei reati ed è stato previsto di demandare al DPR attuativo la disciplina dei casi di deroga per le forniture cui sia indispensabile procedere in sede estera. Anche in tali casi, resta ferma la necessità di utilizzare reti, sistemi informativi e servizi informatici conformi ai livelli di sicurezza previsti dal perimetro, qualora non incompatibili con gli specifici impieghi cui essi sono destinati. Quanto alle forniture di beni e servizi ICT da impiegare su reti, sistemi e servizi rilevanti del Ministero della difesa, è stato stabilito che il Dicastero proceda, senza nuovi o maggiori oneri a carico della finanza pubblica, attraverso un proprio Centro di valutazione in raccordo con AgID e MiSE per i profili di rispettiva competenza;
b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti assicurano al CVCN ed al citato Centro del Ministero della Difesa, per quanto di rispettiva competenza, la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri. Il CVCN segnala la mancata collaborazione al MiSE, in caso di fornitura destinata a soggetti privati, o ad AgID, in caso di fornitura destinata a soggetti pubblici o a quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (CAD). Analogamente procede, informandone AgID, il Centro di valutazione del Ministero della difesa;
c) MiSE e AgID, negli ambiti rispettivamente assegnati loro nel perimetro, svolgono attività di ispezione e verifica in relazione a quanto previsto dalla presente legge, senza che ciò comporti accesso a dati o metadati personali e amministrativi, impartendo, se necessario, prescrizioni. In tale contesto, in considerazione delle specificità, è stato previsto che per le reti, i sistemi e i servizi rilevanti connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica siano svolte, senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonchè in tema di prevenzione e contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti all'AgID per i profili di competenza.

Il comma 6 stabilisce i compiti assunti dal CVCN nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti:

a) contributo all'elaborazione delle misure di sicurezza per ciò che concerne affidamenti di forniture di beni e servizi;

b) svolgimento delle attività di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, anche prescrizioni di utilizzo al committente. Al riguardo, è previsto che il CVCN si avvale anche di laboratori accreditati dal medesimo CVCN secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato su proposta del CISR entro dodici mesi dalla data di entrata in vigore della presente legge, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni;
c) elaborazione e adozione di schemi di certificazione cibernetica, laddove, per ragioni di sicurezza nazionale e su conforme avviso del CISR-tecnico, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

Il comma 7 stabilisce modalità di raccordo e semplificazione in materia di osservanza di misure di sicurezza e di assolvimento dell'obbligo di notifica di incidenti per i soggetti inclusi nel perimetro e, al contempo, tenuti al rispetto delle prescrizioni di cui al decreto legislativo 18 maggio 2018, n. 65, o al decreto legislativo 1 agosto 2003, n. 259 e correlate disposizioni attuative.
Viene, in particolare, stabilito che i soggetti inclusi nel perimetro osservino le misure di sicurezza stabilite dai citati decreti legislativi, ove di livello almeno equivalente a quelle adottate in applicazione della presente legge. Le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti sono definite, in relazione agli ambiti di competenza nel perimetro, da AgID e MiSE che si raccordano, ove necessario, con le autorità competenti di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65. L'assolvimento dell'obbligo di notifica al CSIRT italiano ai sensi della presente legge costituisce anche adempimento degli obblighi di notifica previsti dal decreto legislativo 1 agosto 2003, n. 259, e dal decreto legislativo 18 maggio 2018, n. 65. In relazione a quest'ultimo, il CSIRT italiano ha l'onere di informare l'autorità competente NIS.

I commi da 8 a 13 disciplinano un articolato sistema sanzionatorio per i casi di violazione degli obblighi previsti dalla presente legge. In particolare, è previsto che:
- siano puniti con la pena della reclusione da uno a cinque anni coloro che, tenuti ad effettuare le comunicazioni richieste nell'espletamento dei procedimenti di cui al comma 2, lettera b), al comma 5, lettera a), ovvero delle attività ispettive e di vigilanza previste dal comma 5, lettera c), forniscono informazioni e dati non rispondenti al vero ovvero espongono fatti parimenti non rispondenti al vero, allo scopo di ostacolare o condizionare l'espletamento dei medesimi procedimenti o attività, ovvero allo stesso scopo omettono di comunicare informazioni, dati o fatti necessari per tali procedimenti o attività; all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a 400 quote;
- il decreto legislativo 8 giugno 2001, n. 231 venga conseguentemente integrato con un apposito articolo relativo alla "Falsità ovvero omissione di comunicazioni in materia di perimetro di sicurezza nazionale cibernetica";
- salvo che il fatto costituisca reato, vengano irrogate sanzioni amministrative pecuniarie – scaglionate, in relazione alla gravità della condotta, su tre livelli (con minimi edittali che ammontano a 200.000, 250.000 e 300.000 euro) – per il cui accertamento e irrogazione sono competenti il MiSE e l'AgID;

- per i dipendenti pubblici gli stessi inadempimenti siano altresì oggetto di valutazione ai fini della responsabilità disciplinare e amministrativo-contabile;
- in caso di inottemperanza alle condizioni o in assenza dell'esito favorevole dei test disposti dal CVCN, la stipula del contratto non produca effetto e sia fatto divieto alle parti di darvi, anche provvisoriamente, esecuzione. La violazione di tale divieto comporta, per coloro che abbiano disposto l'affidamento del contratto, l'incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle società aventi ad oggetto, anche se non principale, attività afferenti al settore ICT, per un periodo di tre anni a decorrere dalla data di accertamento della violazione;

Il comma 14 stabilisce che le autorità titolari delle attribuzioni di cui alla presente legge assicurino gli opportuni raccordi con il DIS e con l'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attività di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

I commi 15, 16 e 17 introducono delle modifiche al decreto legislativo del 18 maggio 2018, n. 65 al fine di incrementarne l'efficacia. In particolare il:

- comma 15 modifica l'articolo 4, comma 5, del decreto legislativo prevedendo che il MiSE inoltri l'elenco degli operatori di servizi essenziali anche al punto di contatto unico e all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;
- comma 16 modifica l'articolo 8, comma 9, del decreto legislativo stabilendo che le funzioni svolte dal MiSE in qualità di CERT nazionale, nonché di quelle svolte da AgID in qualità di CERT-PA siano trasferite al CSIRT italiano a decorrere dalla data che verrà indicata nel decreto del Presidente del Consiglio dei ministri in tema di disciplina di organizzazione e funzionamento del CSIRT italiano – da adottarsi ai sensi del comma 2 del medesimo articolo 8 – in luogo che dalla data della entrata in vigore di tale provvedimento;
- comma 17 modifica l'articolo 9, comma 3, del decreto legislativo introducendo l'inoltro delle notifiche NIS all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

Gli eventuali adeguamenti alle prescrizioni di sicurezza, definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2, lettera a), sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione e certificazione nazionale (CVCN) è autorizzata la spesa di 3,2 milioni di euro per l'anno 2019 e di 2,850 milioni di euro per ciascuno degli anni dal 2020 al 2023 e di 0,750 milioni di euro annui a decorrere dall'anno 2024.

L'articolo 2 del disegno di legge prevede interventi per far fronte ad esigenze di personale specializzato per lo svolgimento delle funzioni del CVCN e dell'AgID, come prevista dall'articolo 1.

Il Ministero dello sviluppo economico è autorizzato ad assumere a tempo indeterminato, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facoltà assunzionali, un

contingente massimo di 57 unità reclutate dal Dipartimento della funzione pubblica utilizzando le modalità semplificate previste dall'articolo 3 della legge 19 giugno 2019, n. 56, nel limite di spesa annua di euro 1.002.000 per l'anno 2019 ed euro 3.005.000 annui a decorrere dall'anno 2020; fino al completamento di tali procedure, il Ministero dello sviluppo economico, fatte salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, può avvalersi, per le esigenze del CVCN di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo o di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, per un massimo del 40% delle unità di personale di cui al comma 1. Nei limiti complessivi della stessa quota il Ministero dello sviluppo economico può avvalersi in posizione di comando di personale con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa fino a un massimo di 20 unità, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico dell'amministrazione di appartenenza e successivo rimborso da parte del Ministero dello sviluppo economico dei soli oneri relativi al trattamento accessorio di cui al fondo efficienza servizi istituzionali.

Per lo svolgimento delle nuove funzioni come previste all'articolo 1, l'AgID è autorizzata ad assumere con contratti di lavoro a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di 10 unità di personale da inquadrare nella III area del personale non dirigenziale, posizione economica F1, nel limite di spesa di euro 171.000 per l'anno 2019 ed euro 512.000 annui a decorrere dall'anno 2020 fino al completamento di tali procedure e fatte comunque salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, l'AgID può avvalersi, entro il limite del 40% delle unità previste dal medesimo comma, di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1 comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo, di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127 e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, nonché di esperti o consulenti, nominati ai sensi dell'articolo 7, comma 6, del decreto legislativo 30 marzo 2001, n. 165, in possesso di particolare e comprovata specializzazione in materia informatica.

Il reclutamento del personale avviene mediante uno o più concorsi pubblici espletati secondo le modalità previste dall'articolo 4, commi 3 e 3-bis, del decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla legge 30 ottobre 2013, n. 125, dall'articolo 35, comma 5, del decreto legislativo 30 marzo 2001, n. 165, e dall'articolo 3, comma 6, della legge 19 giugno 2019, n. 56.

L'articolo 3 concerne la copertura finanziaria degli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi 4,373 milioni di euro per l'anno 2019, 6,367 per ciascuno degli anni dal 2020 al 2023, e 4,267 euro annui a decorrere dall'anno 2024.

Il disegno di legge non è corredato di relazione AIR in quanto rientrante nel caso di esclusione di cui al comma 1, lettera c), D.P.C.M. 15 settembre 2017, n. 169.

RELAZIONE TECNICA

Il disegno di legge reca disposizioni volte ad assicurare, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica, un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, e dal cui malfunzionamento o interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Per quanto riguarda i riflessi di carattere finanziario, gli articoli 1 e 2 prevedono:

- l'individuazione, con decreto del Presidente del Consiglio dei ministri, da adottarsi, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) - entro sei mesi dall'entrata in vigore della legge – delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, inclusi nel perimetro, tenuti al rispetto delle misure e degli obblighi conseguentemente previsti (art. 1, comma 2, lett. a));
- la definizione, con lo stesso DPCM suindicato, in base ai parametri di legge contenuti nel comma 1, dei criteri con cui i soggetti inclusi nel perimetro, compresi i soggetti pubblici, elaborano e aggiornano un elenco delle reti, dei sistemi e dei servizi rilevanti per le finalità indicate dalla normativa. Rispetto a tali *asset* (e non riguardo alla generalità delle proprie dotazioni informatiche) gli stessi soggetti sono tenuti all'osservanza delle misure e degli obblighi previsti dalla normativa. All'elaborazione dei criteri provvede il CISR-tecnico, organismo già esistente (art. 5 del DPCM 17 febbraio 2017), di supporto del Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della medesima legge n. 124 del 2007 (art. 1, comma 2, lett. b));
- la definizione, con altro decreto del Presidente del Consiglio dei ministri, adottato sempre su proposta del CISR, entro dodici mesi dalla data di entrata in vigore della legge, delle procedure con cui i soggetti inclusi nel perimetro notificano al CSIRT italiano gli incidenti aventi impatto sulle reti, i sistemi o i servizi individuati, che le inoltra tempestivamente al Dipartimento delle informazioni per la sicurezza (DIS), che provvede a sua volta ad inoltrarle al Ministero dello sviluppo economico (MiSE) - se effettuate da soggetti privati - all'Agenzia per l'Italia digitale (AgID) – se effettuate da soggetti pubblici - nonché all'Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (art. 1, comma 3, lett. a));
- la previsione, con lo stesso decreto del Presidente del Consiglio da ultimo indicato, di misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi e dei servizi informatici sulla base dei parametri previsti dalla norma stessa (art. 1, comma 3, lett. b)), alla cui elaborazione provvede il CISR-tecnico, adottando opportuni moduli organizzativi;

Con regolamento da adottarsi, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dodici mesi dall'entrata in vigore della legge, inoltre (art. 1, comma 5):

- vengono disciplinate le procedure, le modalità e i termini con cui i soggetti inclusi nel perimetro, che intendono procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, i sistemi informativi e riguardo ai servizi informatici d'interesse, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN) istituito presso il MISE, che, sulla base di una valutazione del rischio, può imporre condizioni e test hardware e software dei prodotti interessati. Per le forniture da impiegare su reti, sistemi e servizi del Ministero della Difesa, il predetto Ministero si avvale di un proprio Centro di valutazione, in raccordo con AgID e MiSE. Per l'attività di tale centro si provvede nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica (art. 1, comma 5, lett. a));
- vengono previste attività di ispezione e verifica, in capo ad AgID e al MiSE, rispettivamente, per i soggetti pubblici e per i soggetti privati, in relazione al rispetto degli obblighi previsti dalla normativa, che possono impartire, se necessario, specifiche prescrizioni. Tali attribuzioni di ispezione e verifica vengono riservate alle strutture specializzate dei rispettivi Dicasteri per quanto riguarda le reti, i sistemi e i servizi informatici delle Forze armate e delle Forze di polizia, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica (art. 1, comma 5, lett. c)).

Per quanto concerne l'osservanza, da parte dei soggetti pubblici inclusi nel perimetro, dell'obbligo di attuare le misure di sicurezza previste dalla norma con riferimento alle reti, ai sistemi e ai servizi rilevanti per le finalità indicate, la relativa disciplina verrà resa effettiva a seguito dell'adozione, entro dodici mesi dalla data di entrata in vigore della legge, del decreto del Presidente del Consiglio dei ministri (art. 1, comma 3, lettera b)). A tali oneri, a decorrere dagli esercizi finanziari 2020/2021, si provvederà con le risorse finanziarie, umane e strumentali già previste a legislazione vigente.

Vengono poi in rilievo i compiti del MiSE, dell'AgID, nonché del Ministero dell'interno e del Ministero della difesa, limitatamente alle reti, ai sistemi informativi e ai servizi informatici connessi, rispettivamente, alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, nonché alla difesa nazionale.

Per quanto concerne i compiti del MiSE connessi al funzionamento del perimetro, ciò determinerà l'espletamento delle seguenti attività:

- svolgimento dell'attività di ispezione e verifica (art. 1, comma 5, lettera c));
- svolgimento dell'attività di accertamento delle violazioni e di irrogazione delle sanzioni amministrative previste (art. 1, comma 11);
- l'esercizio di nuovi compiti assunti dal CVCN, in particolare, nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti (art. 1, comma 6):
    - per lo svolgimento, a favore dei soggetti pubblici inclusi nel perimetro, dei test di hardware e software sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego (art. 1, comma 5, lettera a). Gli oneri relativi ai soggetti privati sono a carico degli stessi.

Le richiamate attività di ispezione e verifica nonché di accertamento delle violazioni e di irrogazione delle sanzioni amministrative verranno svolte dal MiSE nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Per le attività di predisposizione delle misure di sicurezza di cui (art. 1, comma 3, lettera b)) provvede il CISR-tecnico, organismo già esistente (art. 5 del DPCM 17 febbraio 2017), di supporto del Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della medesima legge n. 124 del 2007 (art. 1, comma 2, lett. b)), come integrato con rappresentante di AgID.

Per le spese di personale necessarie per espletamento delle attività del CVCN, il Ministero dello sviluppo economico è autorizzato ad assumere a tempo indeterminato, nel limite della dotazione organica vigente, in aggiunta alle ordinarie facoltà assunzionali, un contingente massimo di 57 unità reclutate dal Dipartimento della funzione pubblica utilizzando le modalità semplificate previste dall'articolo 3 della legge 19 giugno 2019, n. 56, nel limite di spesa annua di euro 1.002.000 per l'anno 2019 ed euro 3.005.000 annui a decorrere dall'anno 2020; fino al completamento di tali procedure, il Ministero dello sviluppo economico, fatte salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, può avvalersi, per le esigenze del CVCN di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo o di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, per un massimo del 40% delle unità di personale di cui al comma 1. Nei limiti complessivi della stessa quota il Ministero dello sviluppo economico può avvalersi in posizione di comando di personale con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa fino a un massimo di 20 unità, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico dell'amministrazione di appartenenza e successivo rimborso da parte del Ministero dello sviluppo economico dei soli oneri relativi al trattamento accessorio di cui al fondo efficienza servizi istituzionali (art. 2, commi 1 e 2).

Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione e certificazione nazionale (CVCN) è autorizzata la spesa di 3,2 milioni di euro per l'anno 2019 e di 2,850 milioni di euro per ciascuno degli anni dal 2020 al 2023 e di 0,750 milioni di euro annui a decorrere dall'anno 2024 (art. 1, comma 19).

Per quanto concerne i nuovi compiti di AgID, connessi al funzionamento del perimetro, ciò determinerà l'espletamento delle seguenti attività nei confronti dei soggetti pubblici e di quelli di cui all'art 29 del decreto legislativo 7 marzo 2005, n. 82:

- svolgimento dell'attività di ispezione e verifica (art. 1, comma 5, lettera c));
- svolgimento dell'attività di accertamento delle violazioni e di irrogazione delle sanzioni amministrative previste (art. 1, comma 11)

Le richiamate attività di predisposizione delle misure di sicurezza, di ispezione e verifica nonché di accertamento delle violazioni e di irrogazione delle sanzioni amministrative verranno svolte da AgID nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Per le spese di personale necessarie all'espletamento di nuove e incrementali attività, l'AgID è autorizzata ad assumere con contratti di lavoro a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di 10 unità di personale da inquadrare nella III area del personale non dirigenziale, posizione economica F1, nel limite di spesa di euro 171.000 per l'anno 2019 ed euro 512.000 annui a decorrere dall'anno 2020; fino al completamento di tali procedure e fatte comunque salve le esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito dell'Alleanza atlantica, l'AgID può avvalersi, entro il limite del 40% delle unità previste dal medesimo comma, di personale non dirigenziale appartenente alle pubbliche amministrazioni di cui all'articolo 1 comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di fuori ruolo, di comando o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127 e dell'articolo 70, comma 12 del decreto legislativo 30 marzo 2001, n. 165, nonché di esperti o consulenti, nominati ai sensi dell'articolo 7, comma 6, del decreto legislativo 30 marzo 2001, n. 165, in possesso di particolare e comprovata specializzazione in materia informatica.

Per quanto concerne i compiti del Ministero dell'interno e del Ministero della difesa connessi al funzionamento del perimetro, si provvede mediante strutture specializzate già esistenti e nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente (art. 1, comma 5, lettera c).

Per le attività dei laboratori accreditati di cui potrà avvalersi il CVCN per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità, eventualmente istituiti presso le Amministrazioni centrali dello Stato, si provvede senza nuovi o maggiori oneri a carico della finanza pubblica (art. 1, comma 6, lettera b)).

Altre disposizioni non comportano nuovi o maggiori oneri a carico della finanza pubblica, trattandosi di disposizioni di carattere ordinamentale e/o procedurale.

L'articolo 3 prevede che agli oneri (di cui agli articoli 1, comma 19, e 2, commi 1 e 3, del presente disegno di legge) pari a complessivi 4,373 milioni di euro per l'anno 2019, 6,367 per ciascuno degli anni dal 2020 al 2023, e 4,267 euro annui a decorrere dall'anno 2024, si provvede:

a) quanto a 1,173 milioni di euro per l'anno 2019 e a 4,267 milioni di euro annui a decorrere dal 2020, mediante corrispondente riduzione dello stanziamento del Fondo speciale di parte

corrente iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del Programma Fondi di riserva e speciali della missione «Fondi da ripartire» dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2019, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero dello sviluppo economico per 0,474 milioni di euro per l'anno 2019 e per 0,350 milioni di euro annui a decorrere dall'anno 2020 e l'accantonamento relativo al Ministero dell'economia e delle finanze per 0,699 milioni di euro per l'anno 2019 e per 3,917 milioni di euro annui a decorrere dall'anno 2020;

b) quanto a 3,2 milioni di euro per l'anno 2019 e a 2,1 milioni di euro per ciascuno degli anni dal 2020 al 2023, mediante corrispondente utilizzo dell'autorizzazione di spesa recata dall'articolo 1, comma 95, della legge 30 dicembre 2018, n. 145, da imputare sulla quota parte del fondo attribuita al Ministero dello sviluppo economico.