Senato della Repubblica

XVIII LEGISLATURA

N. 1448

DISEGNO DI LEGGE

presentato dal Presidente del Consiglio dei ministri (CONTE)

di concerto con il Ministro della pubblica amministrazione (BONGIORNO)

con il Ministro dello sviluppo economico (DI MAIO)

con il Ministro della difesa (TRENTA)

con il Ministro dell'interno (SALVINI)

e con il Ministro dell'economia e delle finanze (TRIA)

COMUNICATO ALLA PRESIDENZA IL 1° AGOSTO 2019

Disposizioni in materia di perimetro di sicurezza nazionale cibernetica

TIPOGRAFIA DEL SENATO

INDICE

ONOREVOLI SENATORI. – 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 – come già praticato dal legislatore nel decreto legislativo n. 65 del 2018 di recepimento della direttiva (UE) 2016/1148 (recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) 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 due decreti del Presidente del Consiglio dei ministri 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 decreti del Presidente del Consiglio dei ministri, 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 decreti del Presidente del Consiglio dei ministri 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 cosiddetto CISR-tecnico di cui all'articolo 5 del decreto del Presidente del Consiglio dei ministri 17 febbraio 2017,

pubblicato nella *Gazzetta Ufficiale* n. 87 del 13 aprile 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, accertamento e repressione dei reati ed è stato previsto di demandare al decreto del Presidente della Repubblica 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 codice dell'amministrazione digitale, di cui al 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 citato 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 codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, e correlate disposizioni attuative; 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 decreto del Presidente del Consiglio dei ministri del 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 codice di cui al 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;

svolgimento delle attività di ispezione e verifica, 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, il Dipartimento delle informazioni per la sicurezza (DIS) e 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.

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

Il comma 2 dell'articolo 1 demanda a un decreto del Presidente del Consiglio dei ministri, da adottare su proposta del CISR entro sei mesi dalla data di entrata in vigore della 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 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, di supporto del 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 CAD trasmettano tali elenchi all'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 decreto del Presidente del Consiglio dei ministri – da adottare su proposta del CISR entro dodici mesi dalla data di entrata in vigore della 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 all'AgID, se provenienti da un soggetto pubblico o di cui all'articolo 29 del CAD, 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 provvedano, secondo gli ambiti di competenza delineati dal presente disegno di legge, il Ministero dello sviluppo economico e l'AgID, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

Il comma 4 prevede che all'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si provveda secondo le mo-

dalità 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 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 trenta 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 con 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, accertamento e repressione dei reati ed è stato previsto di demandare al decreto del Presidente della Repubblica 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 all' AgID, in caso di fornitura destinata a soggetti pubblici o a quelli di cui all'articolo 29 del CAD. Analogamente procede, informandone l'AgID, il Centro di valutazione del Ministero della difesa;

c) il MiSE e l'AgID, negli ambiti rispettivamente assegnati loro nel perimetro, svolgono attività di ispezione e verifica in relazione a quanto previsto dal disegno di 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, nonché 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 avvalga 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 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 codice di cui 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 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, dall'AgID e dal 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 codice di cui al 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 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, dati o fatti non rispondenti al vero, allo scopo di ostacolare o condizionare l'espletamento dei medesimi procedimenti o attività, ovvero allo stesso scopo omettono di comunicare, nei termini prescritti, informazioni, dati o fatti necessari per tali procedimenti o attività; all'ente privato, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento quote;

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 possano costituire causa di 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 al presente disegno di 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.

Il comma 15 introduce delle modifiche al decreto legislativo del 18 maggio 2018, n. 65, al fine di incrementarne l'efficacia. In particolare:

la lettera *a)* 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;

la lettera *b)* 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 adottare ai sensi del comma 2 del medesimo articolo 8 – in luogo che dalla data della entrata in vigore di tale provvedimento;

la lettera *c)* 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 euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 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 unità dedicate all'assolvimento delle esigenze connesse alle operazioni con-

dotte 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 per cento 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 che non risulti impiegato in compiti operativi o specialistici, 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 del Ministero dello sviluppo economico, ai sensi dell'articolo 1777 del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e dell'articolo 2, comma 91, della legge 24 dicembre 2007, n. 244.

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 unità dedicate all'assolvimento delle 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 per cento 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 17, e 2, commi 1 e 3, per complessivi euro 4.373.000 per l'anno 2019, euro 6.367.000 per ciascuno degli anni dal 2020 al 2023 ed euro 4.267.000 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 all'articolo 6, comma 1, lettera *c)*, del decreto del Presidente del Consiglio dei ministri 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 provvedono, secondo gli ambiti di competenza delineati dal presente disegno di legge, il Ministero dello sviluppo economico e AgID, d'intesa con il Ministero della difesa, il Ministero dell'interno e il Dipartimento delle informazioni per la sicurezza, *sentito il Ministero dell'economia e delle finanze*;

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.

Alle attività di elaborazione delle misure di sicurezza (di cui all' art. 1, comma 3, lettera b)) provvedono nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente, secondo gli ambiti di competenza delineati dal presente disegno di legge, il Ministero dello sviluppo economico e AgID, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

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); Il CVCN, ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, può imporre prescrizioni di utilizzo (art. 1, comma 6, lettera b), nonché condizioni e test di hardware e software (art. 1, comma 5, lettera a). Gli oneri relativi allo svolgimento delle attività di test sono a carico dei soggetti individuati quali fornitori di beni, sistemi e servizi (art. 1, comma 5, lettera b).

Le richiamate attività di elaborazione delle misure di sicurezza, 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 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 (art. 2, comma 1).
L'onere totale a regime conseguente al reclutamento del predetto contingente di personale, che trova copertura all'articolo 3, è pari a euro 3.005.000 ed è, nel dettaglio, illustrato nella tabella seguente:

ONERI MISE					
Qualifica	Pro capite	Numero unità	Onere totale	Anno 2019	Anno 2020 - Regime
Area III-F4	€ 55.000	23	€ 1.265.000	€ 421.666,67	€ 1.265.000
Area III-F3	€ 50.000	21	€ 1.050.000	€ 350.000	€ 1.050.000
Area II-F5	€ 45.000	12	€ 540.000	€ 180.000	€ 540.000
Dirigente	€ 150.000	1	€ 150.000	€ 50.000	€ 150.000
Totale		57	€ 3.005.000	€ 1.001.667	€ 3.005.000

Gli importi sono comprensivi del trattamento accessorio e al lordo degli oneri riflessi.

L'onere per l'anno 2019, pari ad euro 1.002.000, è stato valutato tenendo conto dei tempi tecnici necessari per portare a compimento le procedure concorsuali pubbliche e che le relative assunzioni non potranno verosimilmente essere effettuate prima del mese di settembre 2019.
L'articolo 2, comma 2 dispone che fino al completamento di tali procedure, il Ministero dello sviluppo economico, fatte salve le unità dedicate all'assolvimento delle 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 che non risulti impiegato in compiti operativi o specialistici 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 del Ministero dello sviluppo economico, ai sensi dell'articolo 1777 del decreto legislativo 15 marzo 2010, n. 66, e dell'articolo 2, comma 91, della legge 24 dicembre 2007, n. 244. La disposizione recata all'articolo 2, comma 2 non determina nuovi o maggiori oneri per la finanza pubblica, tenuto conto che ad essa si dà attuazione nei limiti degli ordinari stanziamenti, previsti a legislazione vigente, dei pertinenti capitoli di bilancio.

Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione e certificazione nazionale (CVCN) è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024 (art. 1, comma 17).

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'articolo 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 (art. 2, comma 3).

L'onere totale a regime, conseguente al reclutamento del predetto contingente di personale, che trova copertura all'articolo 3, è pari a euro 512.000 ed è, nel dettaglio, illustrato nella tabella seguente:

ONERI AGID					
Qualifica	Pro capite	Numero unità	Onere totale	Anno 2019	Anno 2020 - Regime
Area III-F1	€ 51.134,06	10	€ 511.340,60	€ 170.446,87	€ 511.340,60
Totale		10	€ 511.340,60	€ 170.447	€ 511.340,60

Gli importi, comprensivi del trattamento accessorio e al lordo degli oneri riflessi, sono stati quantificati tenendo conto dei valori retributivi contenuti nel C.C.N.L. Funzioni Centrali 2016-2018.
L'onere per l'anno 2019, pari ad euro 171.000, è stato valutato tenendo conto dei tempi tecnici necessari per portare a compimento le procedure concorsuali pubbliche e che le relative assunzioni non potranno verosimilmente essere effettuate prima del mese di settembre 2019.

L'articolo 2, comma 4 dispone che fino al completamento di tali procedure e fatte comunque salve le unità dedicate all'assolvimento delle 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.
La disposizione recata all'articolo 2, comma 4 non determina nuovi o maggiori oneri per la finanza pubblica, tenuto conto che ad essa si dà attuazione nei limiti degli ordinari stanziamenti, previsti a legislazione vigente, dei pertinenti capitoli di bilancio.

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.

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 17, e 2, commi 1 e 3, del presente disegno di legge) pari a complessivi euro 4.373.000 per l'anno 2019, euro 6.367.000 per ciascuno degli anni dal 2020 al 2023, e euro 4.267.000 a decorrere dall'anno 2024, si provvede:

a) quanto a euro 1.173.000 per l'anno 2019 e a euro 4.267.000 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 euro 474.000 per l'anno 2019 e euro 350.000 annui a decorrere dall'anno 2020 e l'accantonamento relativo al Ministero dell'economia e delle finanze per euro 699.000 per l'anno 2019 e per euro 3.917.000 annui a decorrere dall'anno 2020;

b) quanto a euro 3.200.000 per l'anno 2019 e a euro 2.100.000 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 e gravante sugli stanziamenti assegnati all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione (IT – CTI).

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito

[X] POSITIVO [ ] NEGATIVO

Il Ragioniere Generale dello Stato

23 LUG. 2019

ANALISI TECNICO-NORMATIVA

Parte I – ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO.

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di Governo.

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.

L'intervento normativo è coerente con l'impegno del Governo di adottare, accanto alle azioni volte ad accrescere la digitalizzazione del Paese, fattore imprescindibile di sviluppo e di crescita, tutte le misure necessarie per assicurare elevati livelli di sicurezza informatica di reti, sistemi informativi e servizi informatici di interesse strategico, al fine di prevenire che dalla presenza di possibili vulnerabilità possano derivare pregiudizi per la sicurezza nazionale. Vengono a tale fine previste la definizione di adeguate misure di sicurezza, procedure per la tempestiva informazione agli organi competenti degli incidenti informatici, disposizioni per un *procurement* più sicuro di prodotti, processi e servizi ICT destinati alle suddette infrastrutture.

2) Analisi del quadro normativo nazionale.

Il disegno di legge integra organicamente, in una prospettiva di sicurezza nazionale, il quadro normativo vigente in tema di sicurezza cibernetica.

Il decreto legislativo 7 marzo 2005, n.82. all'art. 14-bis, ha assegnato all'Agenzia per l'Italia Digitale il compito di promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione, attribuendole inoltre, ai sensi dell'art. 29 dello stesso decreto, il compito di qualificare e accreditare i soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, nonché i soggetti che intendono svolgere l'attività di conservatore di documenti informatici.

Il decreto legislativo 15 settembre 2003, n.259, modificato dalla legge 20 novembre 2017, n.167, all'articolo 16-bis, ha sancito l'obbligo per le imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico di adottare adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché di comunicare al Ministero dello sviluppo economico ogni significativa violazione della sicurezza o perdita dell'integrità delle reti.

Il decreto legislativo 18 maggio 2018, n.65 che ha recepito la direttiva (UE) 2016/1148 del 6 luglio 2016, agli articoli 12 e 14, ha previsto obblighi di adozione di misure tecniche e organizzative in capo agli operatori di servizi essenziali (OSE) ed ai fornitori di servizi digitali (FSD), al fine di prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali e dei servizi digitali e obblighi di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. Inoltre, all'articolo 8, ha istituito il Gruppo di intervento per la sicurezza informatica in caso di incidente -

CSIRT italiano - a cui è stato attribuito anche il compito di svolgere le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

La legge 3 agosto 2007, n.124, modificata e integrata dalla legge 7 agosto 2012, n.133, all'articolo 4, comma 3, lettera d-bis), ha attribuito al Dipartimento delle informazioni per la sicurezza il compito di coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Il DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" prevede la definizione di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico, adottato sulla base del previgente DPCM 24 gennaio 2013, nell'ambito del quale è stato richiesto il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese. Con DPCM 27 gennaio 2014 è stato inoltre adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica, sostituito dal DPCM del 31 marzo 2017, con il quale è stato indicato l'indirizzo operativo di revisionare e consolidare la legislazione esistente in materia di sicurezza informatica e di definire un quadro giuridico adeguato per supportare le attività di sicurezza in materia cyber.

Lo stesso DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali", nell'abrogare il DPCM del 24 gennaio 2013, ha attribuito all'organismo collegiale di coordinamento – CISR-tecnico – di cui all'articolo 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 26 ottobre 2012, n. 2, recante l'organizzazione ed il funzionamento del Dipartimento delle informazioni per la sicurezza, il compito di supportare il CISR- nello svolgimento delle funzioni di proposta, deliberazione e controllo nel settore della sicurezza informatica nazionale.

Il Decreto del Ministro dello sviluppo economico 12 dicembre 2018, in attuazione degli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, ha individuato adeguate misure di natura tecnico - organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente e ha definito i casi in cui le violazioni della rete o la perdita dell'integrità sono da considerarsi significative, ai fini della notifica da parte dei fornitori di reti e servizi di comunicazione alle competenti Autorità.

Il Decreto del Ministro dello sviluppo economico 15 febbraio 2019, in attuazione dell'articolo 11 del DPCM 12 febbraio 2017, ha istituito presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione il Centro di Valutazione e Certificazione Nazionale – CVCN per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

3) Incidenza delle norme proposte sulle leggi e sui regolamenti vigenti.

Il disegno di legge introduce nuove disposizioni procedurali volte ad istituire il perimetro di sicurezza nazionale cibernetica e a disciplinarne il funzionamento. Prevede, altresì, disposizioni di coordinamento per i soggetti (OSE, FSD e operatori 'Telco') che siano, ad un tempo, sottoposti agli obblighi stabiliti dal decreto legislativo 18 maggio 2018, n. 65 e dal decreto legislativo 1° agosto

2003, n. 259 e inclusi nel perimetro, sia riguardo alle misure di sicurezza, per cui è stabilito che i soggetti osservino quelle già previste dai citati ambiti normativi ove di livello almeno equivalente, sia riguardo alle procedure di notifica, con l'intento di evitare duplicazioni.
Restano fermi i ruoli e le funzioni già previste nella legge 3 agosto 2007, n. 124 per gli organismi di informazione e sicurezza.
Il disegno di legge:

- integra i poteri di proposta del CISR, previsti dall'articolo 5 della legge n.124/2007 e dall'articolo 4 del DPCM 17 febbraio 2017 in materia di sicurezza dello spazio cibernetico, prevedendone l'estensione con riferimento agli ambiti relativi al perimetro;
- disciplina il ruolo del "CISR tecnico" attribuendo all'organo collegiale il compito di: , provvedere all'elaborazione dei criteri in base ai quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco di reti, sistemi e servizi rilevanti (per tale funzione, sarà integrato con un rappresentante di AgID); esprimere un parere sulla proposta del Centro di valutazione e certificazione nazionale (CVCN) di adozione di 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.;
- integra le funzioni di AgID e del MiSE, ai quali vengono attribuiti: l'elaborazione – d'intesa con il Ministero della difesa, il Ministero dell'interno e il Dipartimento delle informazioni per la sicurezza, sentito il Ministero dell'economia e delle finanze – delle misure di sicurezza (da adottare con DPCM su proposta del CISR) per garantire elevati livelli di sicurezza delle reti, sistemi e servizi rilevanti; –, poteri ispettivi e sanzionatori;
- attribuisce nuovi compiti al CVCN per ciò che concerne l' l'approvvigionamento di prodotti, processi e servizi ICT e associate infrastrutture ;
- definisce un sistema di raccordo tra AgID, MiSE, DIS e 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;
- prevede disposizioni di coordinamento volte a semplificare la procedura di notifica degli incidenti aventi impatto su reti, sistemi e servizi rilevanti 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;*
- introduce un sistema sanzionatorio articolato in sanzioni amministrative, sanzioni interdittive, sanzioni penali associate a fattispecie di reato di nuova istituzione nonché, per i dipendenti dei soggetti pubblici inclusi nel perimetro, responsabilità disciplinare e amministrativo-contabile.

Rispetto alla normativa vigente, il disegno di legge prevede misure rivolte ai soggetti inclusi nel perimetro, finalizzate a rendere più sicuro il *procurement* di forniture di beni e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti. Le suddette misure, per quel che concerne le procedure di appalto dei soggetti pubblici, non incidono direttamente sulle disposizioni previste dal decreto legislativo 18 aprile 2016, n. 50, poiché disciplinano una fase endoprocedimentale di carattere speciale – che si colloca tuttavia nell'ambito dell'ordinaria procedura di affidamento – volta alla verifica delle caratteristiche tecniche di un bene o di un servizio ICT. Tale verifica si sostanzia nell'espletamento, da parte del CVCN, di una valutazione, basata su un'analisi del rischio, anche in relazione all'ambito di impiego che può concludersi, entro 30 giorni, e in un'ottica di gradualità, con l'imposizione di prescrizioni di utilizzo al committente, di condizioni e di test *hardware* e *software*. Le citate previsioni fanno salvi 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 stabiliscono i casi di deroga relativamente alle forniture di beni e di

servizi ICT cui sia indispensabile procedere in sede estera (da disciplinare mediante DPR), nonché per quelle necessarie per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati. Per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi e servizi rilevanti del Ministero della difesa è previsto che il Dicastero proceda attraverso un proprio Centro di valutazione in raccordo con AgID e Ministero dello sviluppo economico per i profili di rispettiva competenza.

4) Analisi della compatibilità dell'intervento con i princìpi costituzionali.

Il provvedimento è stato predisposto nel rispetto dei princìpi costituzionali.

5) Analisi della compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Non si ravvisano elementi di incompatibilità. La disciplina in tema di perimetro di sicurezza nazionale cibernetica, attenendo alla materia "sicurezza dello Stato", è rimessa alla potestà legislativa esclusiva dello Stato ai sensi dell'art. 117, comma 2, lettera d), della Costituzione.

6) Verifica della compatibilità con i princìpi di sussidiarietà, differenziazione e adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Non si ravvisano elementi di incompatibilità.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

E' delineata un'architettura normativa snella; in particolare, l'attuazione è demandata, con scadenze temporali diversificate (segnatamente, sei e dodici mesi), a tre decreti del Presidente del Consiglio dei ministri (DPCM), da adottarsi su proposta del CISR, e ad un regolamento, da emanare ai sensi dell'articolo 17, comma 1 della legge 23 agosto 1988, n. 400.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Non si ha notizia di iniziative normative analoghe, attesa, peraltro, l'ampiezza e la sistematicità dell'intervento normativo proposto.

9) Indicazione delle linee prevalenti della giurisprudenza, ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

Parte II – CONTESTO NORMATIVO DELL'UNIONE EUROPEA E INTERNAZIONALE.

1) Analisi della compatibilità dell'intervento con l'ordinamento dell'Unione europea.

Non si ravvisano elementi di incompatibilità poiché la materia della "sicurezza nazionale", ai sensi dell'articolo 4, paragrafo 2, del Trattato sull'Unione europea, resta di esclusiva competenza di ciascuno Stato membro. La disciplina in esame appare complementare rispetto al quadro ordinamentale introdotto con la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, recepita nell'ordinamento interno con il decreto legislativo 18 maggio 2018, n. 65, stabilendo, per finalità di sicurezza nazionale, nuovi e più elevati livelli di tutela e di sicurezza per reti, sistemi e servizi rilevanti. Analoghe considerazioni valgono anche per quanto riguarda la compatibilità del disegno di legge con il regolamento (UE) 2019/881 del 17 aprile 2019, cd. Cybersecurity Act.

2) Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

3) Analisi della compatibilità dell'intervento con gli obblighi internazionali.

Il provvedimento non presenta profili di incompatibilità con gli obblighi internazionali.

4) Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

5) Indicazione delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

6) *Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto* da parte di altri Stati membri dell'Unione europea.

Non vi sono elementi da segnalare

Parte III. – ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO.

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

Lo schema di disegno di legge in tema di perimetro non contiene nuove disposizioni definitorie.

2) Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi.

Lo schema di disegno di legge fa corretto riferimento alla legislazione nazionale vigente.

3) Ricorso alla tecnica della novella legislativa per introdurre modificazioni e integrazioni a disposizioni vigenti.

Si è fatto ricorso alla tecnica della novella normativa, indicando testualmente la parte della norma da modificare. L'uso peraltro limitato della tecnica di novella legislativa è in funzione di esigenze di coordinamento e chiarimento normativo.

4) Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.

Non vi sono elementi da segnalare.

5) Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

Non vi sono elementi da segnalare.

6) Verifica della presenza di deleghe aperte sul medesimo oggetto, anche di carattere integrativo o correttivo.

Non vi sono elementi da segnalare.

7) Indicazione degli eventuali atti successivi attuativi; verifica della congruità dei termini previsti per la loro adozione.

Per l'attuazione delle misure, il disegno di legge prevede l'adozione, con scadenze temporali diversificate e congrue rispetto alle incombenze istruttorie, di tre decreti del Presidente del Consiglio dei ministri (DPCM) adottati su proposta del CISR, e di un regolamento da emanare ai sensi dell'articolo 17, comma 1 della legge 23 agosto 1988, n. 400.
In particolare, con DPCM del Presidente del Consiglio dei ministri, da adottarsi entro sei mesi dalla data di entrata in vigore della legge in argomento, saranno individuate le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati inclusi nel perimetro e saranno definiti i criteri in base ai quali tali soggetti predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi e dei servizi rilevanti.
Con DPCM del Presidente del Consiglio dei ministri, da adottarsi entro dodici mesi dalla data di entrata in vigore della legge in argomento, saranno definite le procedure secondo cui i soggetti inclusi nel perimetro notificheranno gli incidenti aventi impatto su reti, sistemi e servizi rilevanti e saranno stabilite misure volte a garantire elevati livelli di sicurezza delle medesime reti, sistemi e servizi rilevanti.
Con DPCM del Presidente del Consiglio dei ministri, da adottarsi entro dodici mesi dalla data di entrata in vigore della legge in argomento, saranno definiti i criteri in base ai quali il CVCN procede all'accreditamento di laboratori di cui avvalersi per l'espletamento delle attività previste dal decreto, volte alla verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note dei prodotti, processi, servizi ICT da acquisire, destinati a essere impiegati sulle reti, sui sistemi rilevanti e per l'espletamento dei servizi rilevanti.

Con regolamento, da adottarsi, entro dodici mesi dalla data di entrata in vigore della legge in argomento, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, saranno disciplinate le procedure, le modalità e i termini con cui: i soggetti inclusi nel perimetro che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati su reti e sistemi rilevanti e per l'espletamento di servizi rilevanti, diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati, ne danno comunicazione al CVCN; verranno svolte le attività affidate al CVCN e, per gli ambiti di competenza, al Centro di valutazione operante presso il Ministero della difesa; i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti assicureranno 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 *hardware* e *software*; AgID e MiSE svolgeranno attività di ispezione e verifica in relazione agli obblighi previsti dal disegno di legge.

8) Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche, con correlata indicazione nella relazione tecnica della sostenibilità dei relativi costi.

Per la predisposizione dell'intervento normativo sono stati considerati i dati in possesso delle Amministrazioni coinvolte nell'attuazione delle disposizioni del presente disegno di legge.

DISEGNO DI LEGGE

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'individuazione 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 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 codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi della lettera *a)*, trasmettono tali elenchi all'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 all'AgID, se provenienti da un soggetto pubblico o di cui all'articolo 29 del codice dell'amministrazione elettronica, di cui al 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 di *Information and Communications Technology (ICT)*, anche mediante definizione di caratteristiche e requisiti di carattere generale; all'elaborazione di tali misure provvedono, secondo gli ambiti di competenza delineati dalla presente legge, il Ministero

dello sviluppo economico e l'AgID, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

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 medesimi 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) fatti salvi le previsioni dell'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, accertamento e 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 trenta giorni, imporre condizioni e test di *hardware* e *software*; in tale ipotesi, i relativi bandi di gara o contratti sono integrati con 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 l'AgID e il Ministero dello sviluppo economico per i profili di rispettiva competenza; resta fermo che per lo svolgimento delle attività di prevenzione, accertamento e 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 alla lettera *a)* del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o all'AgID, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì all'AgID le analoghe segnalazioni del Centro di valutazione del Ministero della difesa;

c) l'AgID, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera *a)*, e il Ministero dello sviluppo economico, per i soggetti pri-

vati di cui alla medesima lettera, 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 codice delle comunicazioni elettroniche, di cui al 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)*, del presente articolo; le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dalla presente legge sono definite dall'AgID, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera *a)*, del presente articolo, e dal Ministero dello sviluppo economico per i soggetti privati di cui alla medesima lettera, 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 codice di cui al 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 codice di cui al 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:

a) il mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera *a)*, nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza di cui al comma 3, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

d) la mancata comunicazione di cui al comma 5, lettera *a)*, nei termini prescritti, è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in violazione delle condizioni imposte dal CVCN o in assenza del superamento dei *test* di cui al comma 5, lettera *a)*, è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

f) la mancata collaborazione per l'effettuazione delle attività di *test* di cui al

comma 5, lettera *a)*, da parte dei soggetti di cui al medesimo comma 5, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

g) il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dall'AgID in esito alle attività di ispezione e verifica svolte ai sensi del comma 5, lettera *c)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

h) il mancato rispetto delle prescrizioni di cui al comma 6, lettera *b)*, è punito con la sanzione amministrativa pecuniaria 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–ICT, 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)*, o al comma 5, lettera *a)*, o delle attività ispettive e di vigilanza previste dal comma 5, lettera *c)*, fornisce informazioni, dati o fatti non rispondenti al vero, allo scopo di ostacolare o condizionare l'espletamento dei medesimi procedimenti o attività, ovvero allo stesso scopo omette di comunicare, nei termini prescritti, 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 privato, responsabile ai sensi del decreto legislativo 8 giugno

2001, n. 231, si applica la sanzione pecuniaria fino a quattrocento 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 codice di cui al decreto legislativo 7 marzo 2005, n. 82, individuati ai sensi del comma 2, lettera *a)*, del presetne articolo, e il Ministero dello sviluppo economico, per i soggetti privati di cui alla medesima lettera.

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.

13. Per i dipendenti dei soggetti pubblici individuati ai sensi del comma 2, lettera *a)*, la violazione delle disposizioni di cui al presente articolo può costituire causa 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. Al decreto legislativo 18 maggio 2018, n. 65, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 5, dopo il primo periodo è aggiunto il seguente: « 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 »;

b) all'articolo 8, comma 9, le parole: « a far data dalla entrata in vigore del » sono sostituite dalle seguenti: « a decorrere dalla data indicata dal »;

c) all'articolo 9, comma 3, 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 ».

16. 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.

17. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui al comma 5 è autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024.

Art. 2.

(Personale per esigenze di funzionamento del CVCN e dell'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 cinquantasette unità reclutate dal Dipartimento della funzione pubblica della Presidenza del Consiglio dei Ministri, 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 unità dedicate all'assolvimento delle 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 per cento 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 che non risulti impiegato in compiti operativi o specialistici con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa fino a un massimo di venti unità, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico del Ministero dello sviluppo economico, ai sensi dell'articolo 1777 del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e dell'articolo 2, comma 91, della legge 24 dicembre 2007, n. 244.

3. Per lo svolgimento delle nuove funzioni come previste all'articolo 1, l'AgID è autorizzata ad assumere con contratti di la-

voro a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di dieci 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 unità dedicate all'assolvimento delle 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 per cento 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 17, e 2, commi 1 e 3, per complessivi euro 4.373.000 per l'anno 2019, euro 6.367.000 per ciascuno degli anni dal 2020 al 2023, ed euro 4.267.000 annui a decorrere dall'anno 2024, si provvede:

a) quanto a euro 1.173.000 per l'anno 2019 e a euro 4.267.000 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 quanto a euro 474.000 per l'anno 2019 e a euro 350.000 annui a decorrere dall'anno 2020 e l'accantonamento relativo al Ministero dell'economia e delle finanze, quanto a euro 699.000 per l'anno 2019 e a euro 3.917.000 annui a decorrere dall'anno 2020;

b) quanto a euro 3.200.000 per l'anno 2019 e a euro 2.100.000 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.

€ 4,00