PROVVEDIMENTO URGENTE IN DIRAMAZIONE

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

Presidenza del Consiglio dei Ministri
DAGL 0008773 P-
del 19/09/2019

24890293

52615/10.3.1

Roma 19 SET. 2019

A TUTTI I CAPI
UFFICIO LEGISLATIVO
LORO SEDI

Al Ragioniere Generale dello Stato
R O M A

OGGETTO: schema di decreto-legge recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
(PRESIDENZA)

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

d'ordine del
PRESIDENTE DEL CONSIGLIO DEI MINISTRI

IL PRESIDENTE DELLA REPUBBLICA

VISTI gli articoli 77 e 87, quinto comma, della Costituzione;

CONSIDERATA la straordinaria necessità ed urgenza, nell'attuale quadro normativo ed a fronte della realizzazione in corso di importanti e strategiche infrastrutture tecnologiche, anche in relazione a recenti attacchi alle reti di Paesi europei, di disporre, per le finalità di sicurezza nazionale, di un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale;

RITENUTA, altresì, la necessità di prevedere, in coerenza con il predetto sistema, il raccordo con le disposizioni in materia di valutazione della presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e dei dati che vi transitano, ai sensi dell'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

CONSIDERATA altresì la straordinaria necessità ed urgenza di disporre anche dei più idonei strumenti d'immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza in ambito cibernetico;

VISTA la deliberazione del Consiglio dei ministri, adottata nella riunione del...;

Sulla proposta del Presidente del Consiglio dei ministri, di concerto con i Ministri dell'economia e delle finanze, dello sviluppo economico, della difesa, dell'interno, per la pubblica amministrazione e per l'innovazione tecnologica e la digitalizzazione, degli affari esteri e della giustizia;

EMANA
il seguente decreto-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 quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):

a) 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; alla predetta individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, 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 dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale;

b) sono definiti i criteri in base ai quali i soggetti di cui alla precedente lettera a) predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al presente comma, 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, nonché quelli privati, individuati ai sensi della lettera a) trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico; la Presidenza del Consiglio dei ministri 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 dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, 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 alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b), relative:

1) alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

4. All'elaborazione delle misure di cui al comma 3, lettera b), provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, 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.

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

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

a) fatti salvi 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 e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto 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 dal presente decreto, attraverso un proprio Centro di valutazione in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza; resta fermo che per lo svolgimento delle attività di prevenzione, accertamento e di repressione dei reati e nei casi in cui si deroga all'obbligo di cui alla presente lettera, sono utilizzati reti, sistemi informativi e servizi informatici conformi ai livelli di sicurezza di cui al comma 3, lettera b), qualora non incompatibili con gli specifici impieghi cui essi sono destinati;

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

c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale 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 privati 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 alla Presidenza del Consiglio dei ministri per i profili di competenza.

7. 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 6, 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 dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, 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.

8. 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 dal presente decreto sono definite dalla Presidenza del Consiglio dei ministri, 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 la Presidenza del Consiglio dei ministri 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.

9. 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 6, 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 6, 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 6, lettera a), da parte dei soggetti di cui al medesimo comma 6, 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 dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica svolte ai sensi del comma 6, 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 7, lettera b), è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

10. In caso di inottemperanza alle condizioni o in assenza dell'esito favorevole dei test di cui al comma 6, lettera a), il contratto non produce ovvero cessa di produrre effetti, secondo quanto previsto dalle condizioni ad esso apposte. L'esecuzione comunque effettuata in violazione di quanto previsto al primo periodo comporta, oltre alla sanzione di cui al comma 9, lettera e), la sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.

11. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la 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.

12. Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni sono la Presidenza del Consiglio dei ministri, 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 presente articolo, e il Ministero dello sviluppo economico, per i soggetti privati di cui alla medesima lettera.

13. 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.

14. 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.

15. Le autorità titolari delle attribuzioni di cui al presente decreto 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.

16. La Presidenza del Consiglio dei Ministri, per lo svolgimento delle funzioni di cui al presente può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oner finanza pubblica.

17. 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 Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di c all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legg 31 luglio 2005, n. 155.»;

b) 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,».

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

19. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 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 della Presidenza del Consiglio dei ministri)

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, commi 6 e 7, il Ministero dello sviluppo economico è autorizzato ad assumere a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di cinquantasette unità [...], 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 del Trattato dell'atlantico del nord, 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 e 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 funzioni in materia di digitalizzazione, la Presidenza del Consiglio dei ministri 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 dieci unità di personale non dirigenziale, da inquadrare nella Categoria funzionale A, parametro retributivo F1, nel limite di spesa di euro 692.972 annui a decorrere dall'anno 2020.

4. Fino al completamento delle procedure di cui al comma 3, la Presidenza del Consiglio dei ministri, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nel quadro del Trattato dell'Atlantico del Nord, 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 9, comma 5-*ter*, del decreto legislativo 30 luglio 1999, n. 303, 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 da espletare anche in deroga all'articolo 4, commi 3-*quinquies* e 3-*sexies*, del decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla legge 30 ottobre 2013, n. 125, e all'articolo 35, comma 5, del decreto legislativo 30 marzo 2001, n. 165. Resta in ogni caso ferma la possibilità da parte delle amministrazioni di avvalersi delle modalità semplificate e delle misure di riduzione dei tempi di reclutamento previste dall'articolo 3 della legge 19 giugno 2019, n. 56.

ART. 3
(Disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5G)

1. Le disposizioni di cui al presente decreto, fatta eccezione per quanto previsto dall'articolo 1, comma 6, lettera a), si applicano ai soggetti di cui all'articolo 1, comma 2, lettera a), anche nei casi in cui sono tenuti alla notifica di cui all'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56.

2. Dalla data di entrata in vigore del regolamento previsto dall'articolo 1, comma 6, i poteri speciali di cui all'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, sono esercitati previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, da parte dei centri di valutazione di cui all'articolo 1, comma 6, lettera *a*), sulla base della disciplina prevista in attuazione del predetto regolamento.

3. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui all'articolo 1, comma 6, le condizioni e le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei ministri, adottati ai sensi dell'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, in data anteriore alla data di entrata in vigore del medesimo regolamento, qualora attinenti alle reti, ai sistemi informativi e ai servizi informatici inseriti negli elenchi di cui all'articolo 1, comma 2, lettera b), possono essere modificate o integrate, con la procedura di cui al comma 2, con misure aggiuntive necessarie al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal presente decreto, anche prescrivendo, ove

necessario, la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza.

ART. 4

(Disposizioni in materia di infrastrutture e tecnologie critiche)

1. All'articolo 2, comma 1-*ter*, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, dopo le parole «per la sicurezza e l'ordine pubblico,» sono inserite le seguenti: «compreso il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti, i beni e i rapporti di rilevanza strategica per l'interesse nazionale, ulteriori rispetto a quelli individuati nei regolamenti di cui all'articolo 1, comma 1, e al comma 1 del presente articolo, nei settori di cui all'articolo 4, paragrafo 1, del regolamento (UE) n. 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, inclusi».

2. Sino alla data di entrata in vigore del primo regolamento di cui all'articolo 2, comma 1-ter, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, fatta salva l'applicazione degli articoli 1 e 2 del citato decreto-legge, è soggetto alla notifica di cui al comma 5 dell' articolo 2 del medesimo decreto-legge n. 21 del 2012 l'acquisto a qualsiasi titolo, da parte di un soggetto esterno all'Unione europea, di partecipazioni in società che detengono beni e rapporti nei settori di cui all'articolo 4, paragrafo 1, lettere a) e b), del regolamento (UE) n. 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società la cui partecipazione è oggetto dell'acquisto, ai sensi dell'articolo 2359 del codice civile e del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58. Si applicano le disposizioni di cui all'articolo 2, commi 6 e 7, del decreto-legge n. 21 del 2012.

ART. 5

(Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica)

1. Il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi di cui all'articolo 1, comma 2, lettera b), e comunque nei casi di crisi cibernetica di cui al decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017 pubblicato nella Gazzetta Ufficiale n. 87 del 13 aprile 2017, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, ai sensi dell'articolo 7-*bis* del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, può comunque disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

ART. 6

(*Copertura finanziaria*)

1. Agli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi euro 4.202.000 per l'anno 2019, euro 6.547.972 per ciascuno degli anni dal 2020 al 2023, ed euro 4.447.972 annui a decorrere dall'anno 2024, si provvede:

a) quanto a euro 1.002.000 per l'anno 2019 e a euro 4.447.972 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 528.000 per l'anno 2019 e a euro 4.097.972 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.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

RELAZIONE ILLUSTRATIVA

La pervasività assunta dalle minacce alle reti, ai sistemi informativi e ai servizi informatici necessari 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 concreta la possibilità che dal malfunzionamento, interruzione, anche parziale, ovvero utilizzo improprio di tali reti, sistemi informativi e servizi informatici derivi un pregiudizio per la sicurezza nazionale.

Per tale ragione, e in considerazione della rapida evoluzione tecnologica, emerge la necessità e l'urgenza 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, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure 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.

E' emersa, inoltre, la necessità ed urgenza di integrare ed adeguare il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo di cui all'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, al fine di apprestare idonee misure di tutela alle reti, ai sistemi informativi ed ai servizi strategici di comunicazione a banda larga basati sulla tecnologia 5G, ai sensi del richiamato articolo 1-*bis*.

L'impianto normativo sul perimetro di sicurezza nazionale cibernetica è improntato 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 tre decreti del Presidente del Consiglio dei ministri (DPCM), adottati su proposta del CISR, e a un regolamento da emanare ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400;
- possibilità di agevole aggiornamento dei citati DPCM, per rispondere a una duplice finalità: mantenere la normativa al passo con l'evoluzione tecnologica e consentire un graduale ampliamento del novero dei soggetti da includere nel perimetro;

- coinvolgimento del CISR quale proponente dei DPCM applicativi. Ciò, in quanto si tratta di provvedimenti che dettano misure rivolte alla tutela della sicurezza nazionale in campo cibernetico. In questo ambito, il CISR si avvale, quale supporto a fini istruttori, del 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, in coerenza con i più aggiornati orientamenti in materia, che vanno emergendo a livello internazionale, 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 di *information and communication technology* (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 regolamento 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 della Presidenza del Consiglio dei ministri – per le amministrazioni pubbliche e i soggetti di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, inclusi nel perimetro – in coerenza con le funzioni già esercitate da tali soggetti istituzionali alla luce delle norme vigenti. Ciò in considerazione, in particolare, che il MiSE opera quale: autorità competente con poteri ispettivi e sanzionatori (per i settori energia, infrastrutture digitali e per i servizi digitali) e depositario dell'elenco degli operatori di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva europea NIS; autorità di riferimento con poteri ispettivi e sanzionatori verso i fornitori di servizi di comunicazione elettronica ai sensi del decreto legislativo 1° agosto 2003, n. 259, e correlate disposizioni attuative; organismo di certificazione e sicurezza informatica presso cui è stato istituito il CVCN ai sensi dell'articolo 11 del DPCM 17 febbraio 2017;
- disciplina dei compiti del CVCN nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti;
- semplificazione della procedura di notifica di incidente per i soggetti (OSE, FSD e operatori "Telco") che siano ad un tempo inclusi nel perimetro e sottoposti agli obblighi stabiliti dal decreto legislativo 18 maggio 2018, n. 65, o dal decreto legislativo 1° agosto 2003, n. 259, prevedendo che le segnalazioni effettuate secondo la presente disciplina valgano anche quale adempimento degli analoghi obblighi previsti dai suddetti ambiti normativi;

- istituzione di un sistema di vigilanza e controllo sul rispetto degli obblighi introdotti – prevedendo che la Presidenza del Consiglio dei ministri e il MiSE svolgano attività di ispezione e verifica e impartiscano, ove necessario, le opportune prescrizioni – e 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, prevedendo 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 alla Presidenza del Consiglio dei ministri 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 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;

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

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

Il comma 3 demanda a un DPCM – da adottare su proposta del CISR entro dieci mesi dalla data di entrata in vigore della ~~presente~~ legge di conversione del presente decreto – 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 alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, ovvero al MiSE, se effettuate da un soggetto privato;

b) delle misure volte a garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi rilevanti, che devono essere rispettate dai soggetti inclusi nel perimetro.

Al riguardo, il comma 4 dispone che all'elaborazione di tali misure provvedono, secondo gli ambiti di competenza delineati dal presente disegno di legge, il Ministero dello sviluppo economico la Presidenza del Consiglio dei ministri, 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 5 prevede che all'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si provveda secondo le modalità di cui ai medesimi commi con cadenza almeno biennale.

Il comma 6 demanda a un regolamento – da emanare ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto – la definizione di procedure, modalità e termini con cui:

a) i soggetti inclusi nel perimetro, per l'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi e per l'espletamento dei servizi rilevanti, sono tenuti a darne comunicazione al CVCN che – entro 30 giorni – può imporre condizioni, quali una certificazione di sicurezza informatica, e test di hardware e software sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità. In questo caso, i relativi bandi di gara o contratti devono essere integrati di clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto 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 regolamento 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 la Presidenza del Consiglio dei ministri e il 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 alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici o a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82. Analogamente procede, informandone la Presidenza del Consiglio dei ministri e il Centro di valutazione del Ministero della difesa;

c) il MiSE e la Presidenza del Consiglio dei ministri, negli ambiti rispettivamente assegnati loro nel perimetro, svolgono attività di ispezione e verifica in relazione a quanto previsto dalla presente legge, senza che ciò comporti accesso a dati o metadati personali e amministrativi, impartendo, se necessario, prescrizioni. In tale contesto, in considerazione delle specificità, è stato previsto che per le reti, i sistemi e i servizi rilevanti connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica siano svolte, senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, 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 alla Presidenza del Consiglio dei ministri per i profili di competenza.

Il comma 7 stabilisce i compiti assunti dal CVCN nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti:

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

b) svolgimento delle attività di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, anche prescrizioni di utilizzo al committente. Al riguardo, è previsto che il CVCN si avvale anche di laboratori accreditati dal medesimo CVCN secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato su proposta del CISR entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, 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 8 stabilisce modalità di raccordo e semplificazione in materia di osservanza di misure di sicurezza e di assolvimento dell'obbligo di notifica di incidenti per i soggetti inclusi nel perimetro e, al contempo, tenuti al rispetto delle prescrizioni di cui al decreto legislativo 18 maggio 2018, n. 65, o al decreto legislativo 1 agosto 2003, n. 259 e correlate disposizioni attuative.

Viene, in particolare, stabilito che i soggetti inclusi nel perimetro osservino le misure di sicurezza stabilite dai citati decreti legislativi, ove di livello almeno equivalente a quelle adottate in applicazione della presente legge. Le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti sono definite, in relazione agli ambiti di

competenza nel perimetro, dalla Presidenza del Consiglio dei ministri 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 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 9 a 14 disciplinano un articolato sistema sanzionatorio per i casi di violazione degli obblighi previsti dal presente decreto. In particolare, è previsto che:

- sia punito con la pena della reclusione da uno a cinque anni chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la 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
- 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 la Presidenza del Consiglio dei ministri;
- 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, il contratto non produce ovvero cessa di produrre effetti, secondo quanto previsto dalle condizioni ad esso apposte.. L'esecuzione comunque effettuata in violazione di quanto previsto comporta, oltre alla sanzione amministrativa pecuniaria, 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 15 stabilisce che le autorità titolari delle attribuzioni di cui al presente decreto 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 16 prevede che la Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni di cui al presente decreto possa avvalersi dell'Agenzia per l'Italia Digitale (AgID), sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente.

Il comma 17 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 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 decreto, 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 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 decreto prevede interventi per far fronte ad esigenze di personale specializzato per lo svolgimento delle funzioni del CVCN e della Presidenza del Consiglio dei ministri, come previsto dall'articolo 1.

Il MISE è autorizzato ad assumere a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di 57 unità, 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 MISE, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nel quadro del Trattato dell'Atlantico del nord, 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.

Per lo svolgimento delle funzioni in materia di digitalizzazione, la Presidenza del Consiglio dei ministri 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 dieci unità di personale non dirigenziale, da inquadrare nella Categoria funzionale A, parametro retributivo F1, nel limite di spesa di euro 692.972 annui a decorrere dall'anno 2020. Fino al completamento delle procedure di cui al comma 3, la Presidenza del Consiglio dei ministri, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nel quadro del Trattato dell'Atlantico del Nord, 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 9, comma 5-ter, del decreto legislativo 30 luglio 1999, n. 303, 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 di cui ai commi 1 e 3 avviene mediante uno o più concorsi pubblici da espletare anche in deroga all'articolo 4, commi 3-quinquies e 3-sexies, del decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla legge 30 ottobre 2013, n. 125, e all'articolo 35, comma 5, del decreto legislativo 30 marzo 2001, n. 165. Resta in ogni caso ferma la possibilità da parte delle amministrazioni di avvalersi delle modalità semplificate e delle misure di riduzione dei tempi di reclutamento previste dall'articolo 3 della legge 19 giugno 2019, n. 56.

L'articolo 3 del decreto contiene disposizioni di raccordo tra il presente decreto e la normativa in materia di esercizio dei poteri speciali da parte del Governo sui servizi di comunicazione a banda larga basati sulla tecnologia 5G.

In particolare, il comma 1 prevede che ai soggetti inclusi nel perimetro che siano tenuti alla notifica di cui all'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, convertito con modificazioni dalla legge 11 maggio 2012, n. 56 si applichino le disposizioni del presente decreto ad eccezione di quella in materia di procurement disciplinata all'articolo 1, comma 6, lettera a).

Al riguardo, il comma 2 del medesimo articolo stabilisce che, nell'ambito dell'istruttoria prevista dal DL n. 21/2012, la valutazione degli elementi indicanti la presenza di fattori di vulnerabilità, che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, venga effettuata, dalla data di entrata in vigore del regolamento previsto dall'articolo 1, comma 6, del presente provvedimento, da parte dei centri di valutazione descritti in tale comma.

Infine, il comma 3 reca una disciplina transitoria volta a consentire di poter modificare o integrare le condizioni o prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con i provvedimenti di esercizio dei poteri speciali nei confronti di eventuali soggetti inclusi nel perimetro al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal presente decreto, anche prescrivendo, ove necessario la sostituzione di apparati o prodotti che risultino gravemente inadeguati sotto il profilo della sicurezza.

L'articolo 4 intende coordinare l'attuazione del Regolamento europeo n. 452/2019 sul controllo degli investimenti esteri, con l'art. 2, comma 1-ter, del decreto-legge 15 marzo 2012, n. 21, dotando la Presidenza del Consiglio e le Amministrazioni coinvolte della possibilità di applicare con immediatezza la disciplina dei poteri speciali con riferimento ad infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione degli articoli 1 e 2, del decreto-legge 15 marzo 2012, n. 21.

L'articolo si compone di due commi. Il primo comma integra il comma 1-ter dell'articolo 2, del decreto-legge n. 21/2012, in modo da specificare che, nell'ambito della verifica in ordine alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico, è compreso anche il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti. Inoltre, il comma integra l'oggetto dei regolamenti di cui al comma 1-ter, in modo da chiarire che l'individuazione riguarda beni e rapporti ulteriori rispetto a quelli già individuati ai sensi degli articoli 1 e 2 del decreto-legge n. 21/2012, e relativi ai settori individuati quali rilevanti ai fini della sicurezza e ordine pubblico, dall'art. 4, comma 1, del Regolamento europeo n. 452/2019, inclusi i settori ad alta intensità tecnologica elencati al comma 1-ter dell'articolo 2 del decreto-legge n. 21/2012. Il secondo comma, in considerazione della necessità e urgenza di dotarsi nell'immediatezza di strumenti di intervento in relazione ai settori sensibili individuati dal Regolamento europeo n. 452/2019, prevede che, nelle more dell'attuazione del comma 1-ter sopra citato, sia soggetto alla notifica di cui al comma 5 dell'articolo 2 del decreto-legge 15 marzo 2012, n. 21, l'acquisto a qualsiasi titolo da parte di un soggetto esterno all'Unione europea di partecipazioni di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società la cui partecipazione è oggetto dell'acquisto, in società che detengono beni e rapporti nei settori di cui all'art. 4, comma 1, lettere a)-b), del Regolamento (UE) n. 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019.

Si tratta dei seguenti settori: a) infrastrutture critiche, siano esse fisiche o virtuali, tra cui l'energia, i trasporti, l'acqua, la salute, le comunicazioni, i media, il trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie, e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture; b) tecnologie critiche e prodotti a duplice uso quali definiti nell'articolo 2, punto 1, del regolamento (CE) n. 428/2009 del Consiglio, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cibersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie.

A tali procedimenti si applicano le disposizioni di cui ai commi 6 e 7, dell'articolo 2, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56.

L'articolo 5 reca disposizioni improntate alla finalità di assicurare con urgenza gli strumenti giuridici necessari, anche sotto il profilo della gestione dell'emergenza cibernetica, a garantire un elevato livello di sicurezza di reti, sistemi informativi e servizi informatici inseriti negli elenchi previsti dalla normativa in materia di perimetro di sicurezza nazionale cibernetica. A tale riguardo, integra la previsione di cui all'articolo 7-bis del decreto-legge 30 ottobre 2015, n. 174, convertito con legge 11 dicembre 2015, n. 198, che disciplina

l'attività del CISR in caso di crisi, con funzioni di consulenza, proposta e deliberazione, a supporto delle determinazioni del Presidente del Consiglio dei ministri in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale.

La norma prevede che il Presidente del Consiglio, in presenza di un rischio grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi informatici inseriti negli elenchi richiamati, nonché nei casi di crisi cibernetica dichiarata ai sensi della disciplina dell'architettura nazionale cyber (decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017) possa disporre previa deliberazione del CISR, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi e o per l'espletamento dei servizi interessati.

L'articolo 6 concerne la copertura finanziaria degli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi euro 4.202.000 per l'anno 2019, euro 6.547.972 per ciascuno degli anni dal 2020 al 2023, e euro 4.447.972 annui a decorrere dall'anno 2024.

Il decreto non è corredato di relazione AIR in quanto rientrante nel caso di esclusione di cui all'articolo 6, comma 1, lettera c), D.P.C.M. 15 settembre 2017, n. 169.

RELAZIONE TECNICA

Il decreto-legge reca disposizioni urgenti per affrontare con la massima efficacia e tempestività situazioni di emergenza in ambito cibernetico, anche in relazione a recenti attacchi alle reti di Paesi europei, delineando per le finalità di sicurezza nazionale un sistema di organi, procedure e misure, che consenta una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, in linea con le più elevate ed aggiornate misure di sicurezza adottate a livello internazionale, a fronte della realizzazione in corso di importanti e strategiche infrastrutture tecnologiche.

In particolare, 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 quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto – 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 (articolo 1, comma 2, lettera a));
- la definizione, con lo stesso DPCM suindicato, in base ai parametri 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 legge n. 124 del 2007 (articolo 1, comma 2, lettera b));
- la definizione, con altro decreto del Presidente del Consiglio dei ministri, adottato sempre su proposta del CISR, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, 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 – alla Presidenza del Consiglio dei ministri, che si avvale dell'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 (articolo 1, comma 3, lettera 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 (articolo 1, comma 3, lettera b)), alla cui elaborazione provvedono, secondo gli ambiti di competenza delineati dal presente decreto, la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, 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 (articolo 1, comma 4);

Con regolamento da adottarsi, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, inoltre (articolo 1, comma 6):

- 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 Ministero dello sviluppo economico, che, sulla base di una valutazione del rischio, in un'ottica di gradualità, 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 la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico; 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 (articolo 1, comma 6, lettera a));
- vengono previste attività di ispezione e verifica, in capo alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico, 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 (articolo 1, comma 6, lettera 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 del decreto del Presidente del Consiglio dei ministri (articolo 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'articolo 1, comma 4) provvedono nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente, secondo gli ambiti di competenza delineati dal presente decreto, la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, 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 della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico, 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 Ministero dello sviluppo economico connessi al funzionamento del perimetro, ciò determinerà l'espletamento delle seguenti attività:

- svolgimento dell'attività di ispezione e verifica (articolo 1, comma 6, lettera c));
- svolgimento dell'attività di accertamento delle violazioni e di irrogazione delle sanzioni amministrative previste (articolo 1, comma 12);
- l'esercizio di nuovi compiti assunti dal CVCN, in particolare, nell'ambito dell'approvvigionamento ICT destinato a reti, sistemi e servizi rilevanti (articolo 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 (articolo 1, comma 7, lettera b), nonché condizioni e test di hardware e software (art. 1, comma 6, lettera a). Gli oneri relativi allo svolgimento delle attività di test sono a carico dei soggetti individuati quali fornitori di beni, sistemi e servizi (articolo 1, comma 6, 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 Ministero dello sviluppo economico nell'ambito delle risorse finanziarie, umane e strumentali previste 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 (art. 1, comma 19).

Per le spese di personale necessarie per espletamento delle attività del CVCN, il Ministero dello sviluppo economico è autorizzato ad assumere a tempo indeterminato, in aggiunta alle ordinarie facoltà assunzionali e con corrispondente incremento della dotazione organica vigente, 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 (articolo 2, comma 1).
L'onere totale a regime conseguente al reclutamento del predetto contingente di personale, che trova copertura all'articolo 6, 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.

Il comma 2 dell'articolo 2 prevede che, fino al completamento delle procedure di cui al precedente 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 del Trattato dell'Atlantico del nord, 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

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 quanto concerne i nuovi compiti della Presidenza del Consiglio dei Ministri, 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 6, lettera c));
- svolgimento dell'attività di accertamento delle violazioni e di irrogazione delle sanzioni amministrative previste (art. 1, comma 12).

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 nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Per lo svolgimento delle funzioni di cui al presente decreto la Presidenza del Consiglio dei ministri può avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposte convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica (articolo 1, comma 16) .

L'articolo 2, comma 3, dispone che, per lo svolgimento delle funzioni in materia di digitalizzazione, la Presidenza del Consiglio dei ministri 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 dieci unità di personale non dirigenziale, da inquadrare, nella categoria funzionale A, parametro retributivo F1.

L'onere totale a decorrere dal 1° gennaio 2020, conseguente al reclutamento del predetto contingente di personale, che trova copertura all'articolo 6, è pari a euro 692.972 ed è, nel dettaglio, illustrato nella tabella seguente:

CONTINGENTE DI PERSONALE NON DIRIGENZIALE

- 10 unità di personale non dirigenziale appartenenti alla categoria A posizione economica F1

TRATTAMENTO ECONOMICO FONDAMENTALE

	Unità	Stipendio e vacanza contrattuale	Indennità di presidenza	13ª mensilità	Totale lordo dipendente	oneri a carico dell'Amm.ne	Costo unitario con oneri		Costo 10 unità
categ. A - pos.ec.F1	10	22.782,24	7.548,00	1.898,52	32.228,76	12.369,40	44.598,16		445.981,58

TRATTAMENTO ECONOMICO ACCESSORIO

	Unità	Aliquota oraria lorda straord	Ore straordinario annue (25 ore mensili)	Costo straordinario dipendente compresi oneri	F.U.P.(Fiscalità) a.l.+ Ind. Spec. Org. (art.18) a.l. comprensivo degli oneri	Costo unitario con oneri		Costo 10 unità
categ. A - pos.ec.F1	10	14,19	300	5.649,04	19.050,00	24.699,04		246.990,39

TOTALE COSTO COMPLESSIVO 10 UNITA'	692.971,97

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. di riferimento.

Il comma 4 dell'articolo 2 prevede che, fino al completamento delle procedure di cui al precedente comma 3, la Presidenza del Consiglio dei ministri, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito del Trattato dell'Atlantico del nord, 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 9, comma 5-ter, del decreto legislativo 30 luglio 1999, n. 303, 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 7, lettera b)).

L'articolo 3 reca disposizioni di raccordo con le norme in materia di esercizio dei poteri speciali da parte del Governo sui servizi di comunicazione a banda larga basati sulla tecnologia 5G. In particolare, si stabilisce che, nell'ambito dell'istruttoria sui poteri speciali, la valutazione degli elementi indicanti la presenza di fattori di vulnerabilità, che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, venga effettuata, dalla data di entrata in vigore del regolamento previsto dall'articolo 1, comma 6, del presente decreto, da parte dei centri di valutazione descritti in tale comma. Si prevede altresì la modifica o integrazione delle prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con i provvedimenti di esercizio dei poteri speciali nei confronti di eventuali soggetti inclusi nel perimetro al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal presente decreto, anche prescrivendo, ove necessario, la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza. Trattasi di norma ordinamentale sulle procedure attuative che si inserisce nell'impianto già delineato dai precedenti articoli. Lo svolgimento dei compiti di cui al presente articolo è conseguentemente attuato dalle competenti amministrazioni e strutture specializzate nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

L'articolo 4 è volto a dare una prima attuazione al regolamento europeo n. 452/2019 sul controllo degli investimenti esteri, dotando la Presidenza del Consiglio e le Amministrazioni coinvolte della possibilità di applicare la disciplina dei poteri speciali con riferimento ad infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione degli articoli 1 e 2 del decreto-legge 15 marzo 2012, n. 21. Trattasi di norma ordinamentale sulle procedure attuative che si inserisce nell'impianto già delineato dai precedenti articoli. Lo svolgimento dei compiti istruttori di cui al presente articolo è attuato, sulla basi di procedure già consolidate, dalle competenti amministrazioni e strutture specializzate nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

L'articolo 5 prevede che il Presidente del Consiglio, in presenza di un rischio grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi informatici inclusi nel perimetro, nonché nei casi di crisi cibernetica (di cui al decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017), previa deliberazione del Comitato

interministeriale per la sicurezza della Repubblica, può comunque disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati. Trattasi di norma ordinamentale che non comporta nuovi o maggiori oneri a carico della finanza pubblica.

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

L'articolo 6 prevede che agli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi euro 4.202.000 per l'anno 2019, euro 6.547.972 per ciascuno degli anni dal 2020 al 2023, ed euro 4.447.972 annui a decorrere dall'anno 2024, si provvede:

a) quanto a euro 1.002.000 per l'anno 2019 e a euro 4.447.972 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 528.000 per l'anno 2019 e a euro 4.097.972 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.