

DECRETO-LEGGE 21 settembre 2019, n. 105

Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. (19G00111)

(GU n.222 del 21-9-2019)

Vigente al: 22-9-2019

IL PRESIDENTE DELLA REPUBBLICA

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

Considerata la straordinaria necessita' 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 finalita' 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 piu' elevate ed aggiornate misure di sicurezza adottate a livello internazionale;

Ritenuta, altresi', la necessita' di prevedere, in coerenza con il predetto sistema, il raccordo con le disposizioni in materia di valutazione della presenza di fattori di vulnerabilita' che potrebbero compromettere l'integrita' 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 altresi' la straordinaria necessita' ed urgenza di disporre anche dei piu' idonei strumenti d'immediato intervento che consentano di affrontare con la massima efficacia e tempestivita' eventuali situazioni di emergenza in ambito cibernetico;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 19 settembre 2019;

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, degli affari esteri e della cooperazione internazionale, della giustizia, per la pubblica amministrazione e per l'innovazione tecnologica e la digitalizzazione;

E m a n a
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, e' 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 attivita' 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 attivita' 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 attivita' 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 attivita' 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 attivita' 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), e' 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 attivita' di ispezione e verifica svolte ai sensi del comma 6, lettera c), e' 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), e' 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 incapacita' 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 attivita' 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 attivita' 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, e' punito con la reclusione da uno a cinque anni e all'ente, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, si applica la sanzione pecuniaria fino a 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 9, 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 puo' costituire causa di responsabilita' 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 regolarita' dei servizi di telecomunicazione, quale autorità di contrasto nell'esercizio delle attivita' 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 decreto puo' avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la 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 e' 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 regolarita' 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 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 regolarita' 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 e' 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 professionalita' necessaria per lo svolgimento delle funzioni del CVCN, di cui all'articolo 1, commi 6 e 7, il Ministero dello sviluppo economico e' autorizzato ad assumere a tempo indeterminato, con incremento della vigente dotazione organica nel limite delle unita' eccedenti, in aggiunta alle ordinarie facolta' assunzionali, un contingente massimo di settantasette unita' di personale, di cui sessantasette di area terza e dieci di area seconda, nel limite di spesa di 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 unita' 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, puo' 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 unita' di personale di cui al comma 1. Nei limiti complessivi della stessa quota il Ministero dello sviluppo economico puo' 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 unita', 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 e' autorizzata ad assumere con contratti di lavoro a tempo indeterminato, in aggiunta alle ordinarie facolta' assunzionali e con corrispondente incremento della dotazione organica, un contingente massimo di dieci unita' di personale non dirigenziale, da inquadrare nella Categoria funzionale A, parametro retributivo F1, nel limite di spesa di euro 640.000 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 unita' 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, puo' avvalersi, entro il limite del 40 per cento delle unita' 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, nonche' 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 piu' 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 possibilita' da parte delle amministrazioni di avvalersi delle modalita' 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 vulnerabilita' che potrebbero compromettere l'integrita' 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, e' 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 e' 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, puo' 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 proporzionalita', la disattivazione, totale o parziale, di uno o piu' 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 3.200.000 per l'anno 2019, euro 6.495.000 per ciascuno degli anni dal 2020 al 2023, ed euro 4.395.000 annui a decorrere dall'anno 2024, si provvede:

a) quanto a euro 4.395.000 annui a decorrere dal 2020, mediante corrispondente riduzione delle proiezioni 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 350.000 annui a decorrere dall'anno 2020 e l'accantonamento relativo al Ministero dell'economia e delle finanze, per euro 4.045.000 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 e' autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 7

Entrata in vigore

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana e sara' presentato alle Camere per la conversione in legge.

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

Dato a Napoli, addi' 21 settembre 2019

MATTARELLA

Conte, Presidente del Consiglio dei ministri

Gualtieri, Ministro dell'economia e delle finanze

Patuanelli, Ministro dello sviluppo economico

Guerini, Ministro della difesa

Lamorgese, Ministro dell'interno

Di Maio, Ministro degli affari
esteri e della cooperazione
internazionale

Bonafede, Ministro della giustizia

Dadone, Ministro per la pubblica
amministrazione

Pisano, Ministro per l'innovazione
tecnologica e la digitalizzazione

Visto, il Guardasigilli: Bonafede