COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e IX (Trasporti, poste e telecomunicazioni)

S O M M A R I O

SEDE REFERENTE

Martedì 1º ottobre 2019. — Presidenza del presidente della I Commissione Giuseppe BRESCIA. — Interviene il sottosegretario di Stato per i rapporti con il Parlamento Gianluca Castaldi.

La seduta comincia alle 13.40.

DL 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
C. 2100 Governo.

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento.

Giuseppe BRESCIA, *presidente*, avverte che le Commissioni riunite I e IX avviano nella seduta odierna l'esame, in sede referente, del disegno di legge C. 2100, di conversione del decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Ricorda al riguardo che nella riunione del 25 settembre scorso la Conferenza dei Presidenti di gruppo ha fissato per lunedì 21 ottobre prossimo l'avvio della discussione in Assemblea sul provvedimento. Avverte quindi che nella seduta di giovedì 3 ottobre prossimo comincerà il ciclo di audizioni deliberato ai fini dell'istruttoria legislativa sul provvedimento, il quale si concluderà nel corso della prossima settimana.

Rammenta altresì che nella mattina di giovedì 3 ottobre è convocata una riunione congiunta degli Uffici di presidenza, integrati dai rappresentanti dei gruppi, delle Commissioni riunite, al fine di definire l'ulteriore organizzazione dei lavori sul provvedimento.

Invita quindi relatori, Fiano per la I Commissione e Scagliusi per la IX Commissione, a illustrare il contenuto del provvedimento in esame.

Emanuele FIANO (PD), *relatore per la I Commissione*, rileva come le Commissioni siano chiamate ad esaminare, in sede referente, il disegno di legge C. 2100, di conversione del decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Innanzitutto rileva come la finalità del provvedimento sia quella di garantire, per le finalità di sicurezza nazionale, l'integrità e la sicurezza delle reti – anche inerenti ai servizi di comunicazione elet-

tronica a banda larga basati sulla tecnologia 5G e dei dati che vi transitano – nonché 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. L'obiettivo dell'intervento legislativo, inoltre, è di disporre di più idonei strumenti d'immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza in ambito cibernetico.

Passando ad illustrare il contenuto delle disposizioni del decreto – legge relative a materie di prevalente competenza della I Commissione, rileva come l'articolo 1, comma 1, istituisca il perimetro di sicurezza nazionale cibernetica, al fine di assicurare la sicurezza di reti, sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale.

In particolare, il comma 1 fa riferimento ad amministrazioni pubbliche, nonché ad enti e operatori nazionali, pubblici e privati le cui reti e sistemi informativi e informatici:

sono necessari per l'esercizio di una funzione essenziale dello Stato;

sono necessari per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

il cui malfunzionamento, interruzione – anche parziali – o uso improprio possono pregiudicare la sicurezza nazionale.

Il comma 2 demanda l'individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica ad un decreto del Presidente del Consiglio dei ministri, adottato 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 decreto-legge.

Ricorda, in proposito, che il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza.

Rammenta, inoltre, che il decreto legislativo 18 maggio 2018, n. 65, pone le misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. In particolare, al Presidente del Consiglio dei ministri compete l'adozione – sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR) – della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

Ai sensi della lettera a) del comma 2 il decreto del Presidente del Consiglio dei ministri individua i soggetti inclusi nel perimetro secondo i seguenti criteri:

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;

l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici il cui malfunzionamento, interruzione o esercizio improprio può costituire un pericolo per la sicurezza nazionale.

Resta ferma, per gli organismi di informazione e sicurezza, la specifica disciplina di cui alla legge 3 agosto 2007, n. 124 (recante « Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto »).

Ricorda, al riguardo, che la legge n. 124 del 2007 stabilisce che il Sistema di

informazione per la sicurezza della Repubblica è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità delegata (Ministro senza portafoglio o Sottosegretario di Stato) ove istituita, dal Dipartimento delle informazioni per la sicurezza (DIS), dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI).

Ai sensi della lettera *b)* del comma 2 il medesimo DPCM dovrà fissare i criteri che i soggetti inclusi nel perimetro dovranno seguire nel compilare l'elenco delle reti, dei sistemi e dei servizi (comprensivo dell'architettura e della componentistica) rilevanti ai fini della presente disciplina. Tale elenco dovrà essere aggiornato con cadenza almeno annuale.

L'organismo tecnico di supporto al CISR, integrato da un rappresentante della Presidenza del Consiglio dei ministri, collabora nella predisposizione di tali criteri, adottando « opportuni moduli organizzativi ».

Entro sei mesi dall'entrata in vigore del DPCM di cui qui si tratta, gli elenchi così predisposti sono inviati:

alla Presidenza del Consiglio dei ministri dai soggetti pubblici;

sempre alla Presidenza del Consiglio dei ministri dai soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale oppure dai soggetti che intendono svolgere l'attività di conservatore di documenti informatici, rispettivamente qualificati ovvero accreditati dall'AgID (si tratta dei soggetti individuati dall'articolo 29 del Codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005);

al Ministero dello sviluppo economico dai soggetti privati che rientrano nel perimetro di sicurezza ed individuati dallo stesso DPCM.

Quindi, la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano i rispettivi elenchi:

al DIS, Dipartimento delle informazioni per la sicurezza, organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea e designato, dall'articolo 7 del decreto legislativo n. 65 del 2018, quale punto di contatto unico per tali questioni, anche per le attività di prevenzione, preparazione e gestioni delle crisi svolte dal Nucleo per la sicurezza cibernetica;

all'organo per la regolarità e sicurezza dei servizi di telecomunicazione presso il Ministero dell'interno il quale assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno 9 gennaio 2008, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate (articolo 7-*bis* del decreto-legge n. 144 del 2005, recante « Misure urgenti per il contrasto del terrorismo internazionale »).

Il comma 3 demanda ad un DPCM la determinazione di un duplice profilo:

le procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica;

le misure di sicurezza.

Per quanto riguarda le procedure di segnalazione – di cui alla lettera *a)* – degli incidenti su reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica, i relativi soggetti (amministrazioni pubbliche, nonché enti oppure operatori nazionali, pubblici e privati) devono notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano.

Il CSIRT procede poi a inoltrare tempestivamente tali notifiche al Dipartimento delle informazioni della sicurezza (DIS).

La trasmissione è prevista anche qualora siano interessate attività demandate al Nucleo per la sicurezza cibernetica.

Il medesimo DIS assicura indi una duplice ulteriore trasmissione:

all'organo del Ministero dell'interno preposto alla sicurezza e regolarità dei servizi di telecomunicazioni;

alla Presidenza del Consiglio dei ministri (se le notifiche degli incidenti giungano da un soggetto pubblico – o da un soggetto fornitore di servizi fiduciari qualificati o svolgente l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, ai sensi dell'articolo 29 del Codice dell'amministrazione digitale, decreto legislativo n. 82 del 2005) ovvero al Ministero dello sviluppo economico (se le notifiche giungano da un soggetto privato del perimetro di sicurezza nazionale cibernetica).

Per quanto riguarda le misure di sicurezza – di cui alla lettera *b)* – esse devono assicurare elevati livelli di sicurezza delle reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica.

In particolare, siffatte misure devono essere definite sì da agire su più versanti:

politiche di sicurezza, struttura organizzativa e gestione del rischio;

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

protezione fisica e logica e dei dati informativi;

integrità delle reti e dei sistemi informativi;

gestione operativa (compresa la continuità del servizio);

monitoraggio, test e controllo;

formazione e consapevolezza;

affidamento di forniture, sistemi e servizi di tecnologie dell'informazione e della comunicazione (ICT nell'acronimo inglese: Information and Communication Technology).

Il comma 4 determina i soggetti ministeriali preposti all'elaborazione delle misure di sicurezza. In particolare, l'elaborazione delle misure di sicurezza è realizzata, secondo l'ambito di propria competenza, dal Ministero per lo sviluppo economico e dalla Presidenza del Consiglio. È prevista l'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e finanze, il Dipartimento delle informazioni per la sicurezza.

Il comma 5 prevede l'aggiornamento – almeno biennale – di quanto previsto dal menzionato DPCM.

Il comma 6 rimette ad un regolamento da emanarsi, con decreto del Presidente del Consiglio dei ministri, entro 10 mesi dalla data di entrata in vigore del decreto-legge, la definizione delle procedure, delle modalità e dei termini alle quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, ai sensi del decreto del Presidente del Consiglio dei ministri di cui al comma 2, 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 individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico secondo quanto previsto dalla lettera *b)* del comma 2, diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati.

In particolare il comma 6, alla lettera *a)*, stabilisce che i soggetti sopra indicati danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso l'ISCTI (Istituto Superiore della Comunicazioni e delle Tecnologie dell'Informazione) dal Ministro dello sviluppo economico, dell'intendimento di provvedere all'affidamento di tali forniture.

La lettera *b)* prevede che i fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici individuati nell'elenco che deve essere trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico (secondo quanto previsto dalla lettera *b)* del comma 2), 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, sostenendone gli oneri.

La lettera *c)* prevede che la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, secondo la ripartizione di competenza indicata nelle precedenti disposizioni, svolgano attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera *b)*, dal comma 3 e dalla lettera *a)* del comma 6 senza che ciò comporti accesso a dati o metadati personali e amministrativi, impartendo, se necessario, specifiche prescrizioni.

Il comma 7 individua alcuni compiti del Centro di valutazione e certificazione nazionale (CVCN), con riferimento all'approvvigionamento di prodotti, processi, servizi di tecnologie dell'informazione e della comunicazione (ICT) e associate infrastrutture, qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica. Si ricorda che il Centro di valutazione e certificazione nazionale è stato istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019.

In base al comma 7 il CVCN:

contribuisce all'elaborazione delle misure di sicurezza, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT (lettera *a*);

svolge attività di valutazione del rischio e di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, prescrizioni di utilizzo al committente (lettera *b*);

elabora e adotta (previo conforme avviso dell'organismo tecnico di supporto al Comitato interministeriale per la sicurezza della Repubblica – CISR) schemi di certificazione cibernetica, qualora gli schemi di certificazione esistenti non siano ritenuti, per ragioni di sicurezza nazionale, adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica (lettera *c*).

Ai fini delle attività di cui alla lettera *b*), il CVCN si avvale anche di laboratori che esso stesso accredita, secondo criteri di accreditamento che saranno stabiliti con DPCM entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge.

Tale DPCM è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR).

Per le esigenze delle amministrazioni centrali dello Stato, sono impiegati i laboratori eventualmente istituiti presso le medesime amministrazioni, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il comma 8 determina alcuni obblighi per:

gli operatori dei servizi essenziali;

i fornitori di servizi digitali;

le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica.

In particolare, la disposizione prevede – alla lettera *a)* – che tali soggetti – se inclusi nel perimetro di sicurezza nazionale cibernetica – osservino le misure di sicurezza previste dalle disposizioni vigenti (decreto legislativo n. 65 del 2018 e decreto legislativo n. 259 del 2003), allorché esse siano « di livello almeno equivalente » a quelle adottate con l'apposito DPCM (comma 3, lettera *b*) attuativo del decreto-legge).

Se tuttavia non vi sia equivalenza nel livello di sicurezza, le eventuali misure

aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto-legge devono essere definite:

dalla Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli che forniscano servizi fiduciari qualificati o attività di gestore di posta elettronica certificata o di gestore dell'identità digitale o di conservatore di documenti informatici (di cui all'articolo 29 del decreto legislativo n. 82 del 2005, codice dell'amministrazione digitale,);

dal Ministero dello sviluppo economico (che si avvale anche del Centro di valutazione e di certificazione nazionale – CVCN) per i soggetti privati.

La Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico (il quale è autorità NIS per il settore energia, sotto-settori energia elettrica, gas e petrolio, e per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD, nonché per i servizi digitali) si raccordano, ove necessario, con le autorità NIS competenti.

La lettera *b)* del comma 8 del pari dispone in merito ad alcuni obblighi in capo ai soggetti sopra ricordati.

In particolare, dispone che essi assolvano l'obbligo di notifica degli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici del perimetro di sicurezza nazionale cibernetica.

I commi da 9 a 11 recano un articolato sistema sanzionatorio per i casi di violazione degli obblighi previsti dal decreto-legge.

In particolare, il comma 9 disciplina una serie di illeciti amministrativi. Le sanzioni amministrative pecuniarie irrogate sono scaglionate in relazione alla gravità della condotta.

Il comma 11 punisce con la pena della reclusione da uno a cinque anni coloro che, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2 lettera *b)* (procedimento di compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici) e di cui al comma 6, lettera *a)* (procedimenti relativi all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi) o delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico, di cui al comma 6, lettera *c)*:

forniscono informazioni, dati o fatti non rispondenti al vero rilevanti per l'aggiornamento degli elenchi su ricordati o ai fini delle comunicazioni previste nei casi di affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, o per lo svolgimento delle attività ispettive e di vigilanza;

omettono di comunicare i predetti dati, informazioni o elementi di fatto.

All'ente privato, responsabile ai sensi del decreto legislativo 8 giugno 2001, n. 231, recante la disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, si applica la sanzione pecuniaria fino a quattrocento quote.

In proposito segnala l'opportunità di inserire tale reato nell'ampio catalogo di reati presupposto già contemplati dal decreto legislativo n. 231 del 2001.

Il comma 12 individua le autorità competenti all'accertamento delle violazioni e all'irrogazione delle sanzioni previste dai commi precedenti.

Al riguardo rileva l'opportunità di specificare che si fa riferimento alle sole sanzioni amministrative, posto che evidentemente l'accertamento del delitto di cui al comma 11 compete all'autorità giudiziaria.

La autorità competenti vengono individuate:

nella Presidenza del Consiglio dei ministri, per le amministrazioni pubbliche, gli enti e gli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale (in base al comma 2, lettera *a)*, nonché per i soggetti qualificati o accreditati per fornire servizi fiduciari o attività di gestore di posta elettronica certificata o

di gestore dell'identità digitale (in base all'articolo 29 del decreto legislativo n. 82 del 2005);

nel Ministero dello Sviluppo economico, per gli operatori nazionali privati inclusi nel perimetro di sicurezza nazionale (in base al comma 2, lettera *a*).

La Presidenza del Consiglio e il MISE sono dunque le autorità chiamate a vigilare sul rispetto degli obblighi previsti dai commi 2, 3, 6 e 7 dell'articolo 1 e a irrogare le sanzioni amministrative pecuniarie.

Per l'accertamento delle violazioni e l'irrogazione delle sanzioni si applica il procedimento disciplinato dalla legge n. 689 del 1981.

Rileva come allo stato attuale non sia possibile circoscrivere il campo delle amministrazioni pubbliche che potranno essere sanzionate dalla Presidenza del Consiglio e chiamate al pagamento di sanzioni amministrative pecuniarie: a ciò provvederà infatti il DPCM che delineerà il perimetro dei soggetti tenuti al rispetto della disciplina sulla sicurezza nazionale cibernetica; tra tali soggetti potrebbero ad esempio essere ricompresi i ministeri o le regioni e province autonome. Le amministrazioni pubbliche sanzionate potranno opporsi quindi all'ordinanza-ingiunzione di pagamento davanti al giudice ordinario.

Il comma 14 specifica che per la violazione delle disposizioni dell'articolo 1, i dipendenti delle amministrazioni pubbliche, degli enti e degli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale (in base al comma 2, lettera *a*) possono incorrere in responsabilità disciplinare e amministrativo-contabile. Si tratta di violazioni che determinano infatti a carico del datore di lavoro una responsabilità amministrativa per il pagamento di una sanzione pecuniaria.

Come già ricordato, le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dall'articolo 1 del decreto-legge in esame sono individuati – entro 4 mesi – con DPCM, su proposta del CISR (ai sensi del comma 2 lettera *a*).

Il comma 15 prevede che le autorità titolari delle attribuzioni quali configurate dal decreto-legge assicurino « gli opportuni raccordi » con il Dipartimento delle informazioni per la sicurezza (DIS) e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Il comma 16 prevede che la Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni attinenti al perimetro di sicurezza cibernetica, possa avvalersi dell'Agenzia per l'Italia Digitale (AGID), che è l'organismo tecnico del Governo che ha il compito di garantire, sulla base degli indirizzi del Presidente del Consiglio o del Ministro delegato, la realizzazione gli obiettivi dell'Agenda Digitale Italiana.

Il comma 17 reca due novelle al decreto legislativo n. 65 del 2018 (il quale ha dato attuazione alla direttiva UE 2016/1148, recante misure per un livello elevato di sicurezza delle reti e dei sistemi informativi nell'Unione).

La prima novella – recata dalla lettera *a)* – attiene alla identificazione degli operatori di servizi essenziali (la quale è oggetto dell'articolo 4 del decreto legislativo n. 65).

Più specificamente, la novella concerne l'elenco nazionale degli operatori di servizi essenziali, che l'articolo 4, comma 5, del decreto legislativo n. 65 ha istituito presso il Ministero dello sviluppo economico.

Al riguardo si viene ora a prevedere che quel Ministero trasmetta l'elenco nazionale di servizi essenziali al punto di contatto unico nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

La seconda novella – recata dalla lettera *b)* – prevede che anche l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione sia parte del network chiamato a collaborare per l'adempimento degli obblighi di cui al decreto legislativo n. 65 in materia di sicurezza delle reti e dei sistemi informativi (composto dalle autorità competenti

NIS, dal punto di contatto unico e dal CSIRT italiano, ai sensi dell'articolo 9 del medesimo decreto legislativo n. 65).

Il comma 18 dispone, a sua volta, che gli eventuali adeguamenti delle reti, dei sistemi informativi e dei servizi informatici, che amministrazioni pubbliche, enti pubblici ed operatori pubblici debbano intraprendere, per ottemperare alle prescrizioni di sicurezza come definite dal decreto-legge, siano effettuati con le risorse finanziarie disponibili a legislazione vigente.

Il comma 19 prevede l'autorizzazione di spesa per la copertura finanziaria relativa alla realizzazione, all'allestimento e al funzionamento del CVCN di cui ai commi 6 e 7 dell'articolo 1.

L'articolo 2, al comma 1, autorizza il MISE ad assumere a tempo indeterminato, con incremento della vigente dotazione organica nel limite delle unità eccedenti, in aggiunta alle ordinarie facoltà assunzionali, un contingente massimo di 77 unità di personale, di cui 67 di area terza e 10 di area seconda, nel limite di spesa di euro 3.005.000 annui a decorrere dal 2020, tenuto conto dell'esigenza di disporre di personale in possesso della professionalità necessaria per lo svolgimento delle funzioni del Centro di valutazione e certificazione nazionale (CVCN), di cui all'articolo 1, commi 6 e 7.

Il comma 2 prevede che, fino al completamento delle procedure di assunzione, il MISE, 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 n. 165 del 2001, 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 n. 127 del 1997, e dell'articolo 70, comma 12, del decreto legislativo n. 165 del 2001, per un massimo del 40 per cento delle unità di personale da assumere in base al comma 1.

Nei limiti complessivi della stessa quota il MISE può inoltre avvalersi, in posizione di comando, di personale che non risulti impiegato in compiti operativi o specialistici con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa fino a un massimo di 20 unità, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico del MISE, ai sensi dell'articolo 1777 del codice dell'ordinamento militare (decreto legislativo n. 66 del 2010) e dell'articolo 2, comma 91, della legge n. 244 del 2007.

Il comma 3 autorizza la Presidenza del Consiglio ad assumere fino a dieci unità di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione.

In particolare, la norma autorizza la Presidenza del Consiglio dei ministri ad assumere – a tempo indeterminato – un contingente massimo di dieci unità di personale non dirigenziale (da inquadrare nella categoria funzionale A, parametro retributivo F1) per le funzioni in materia di digitalizzazione.

Le nuove assunzioni sono in aggiunta alle ordinarie facoltà assunzionali; pertanto si ha un corrispondente incremento della dotazione organica.

L'autorizzazione di spesa è nel limite di 640.000 euro annui, a decorrere dall'anno 2020.

Il comma 4 autorizza la Presidenza del Consiglio – nelle more delle assunzioni sopra ricordate – ad avvalersi di esperti o di personale di altre amministrazioni pubbliche.

Più in dettaglio, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale (anche nell'ambito dell'Alleanza atlantica), una prima autorizzazione è ad avvalersi di personale non dirigenziale appartenente ad altre pubbliche amministrazioni.

Rimane escluso il personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche.

L'autorizzazione è ad avvalersi nel limite del 40 per cento delle unità previste dal comma 3 (ossia fino a quattro), di personale di altre pubbliche amministrazioni.

Le unità prescelte sono collocate in posizione di fuori ruolo, di comando o di altro analogo istituto.

Una seconda, concorrente autorizzazione è ad avvalersi di esperti e consulenti, i quali debbono essere in possesso di particolare e comprovata specializzazione in materia informatica.

Al riguardo segnala l'opportunità di approfondire se il numero massimo degli esperti e consulenti che possono essere nominati in base al comma 4 sia ricompreso nel limite del 40 per cento (quindi nel limite di quattro) ovvero se sia inteso come corrispondente al numero di unità determinate dal precedente comma 3 (massimo dieci) detratte le unità (massimo quattro) di personale appartenente ad altre amministrazioni pubbliche.

Gli esperti e consulenti sono nominati ai sensi dell'articolo 7, comma 6, del decreto legislativo n. 165 del 2001.

Il comma 5 dispone che il reclutamento del personale necessario al funzionamento del CVCN (di cui al comma 1) e allo svolgimento delle funzioni di digitalizzazione della Presidenza del Consiglio (di cui al comma 3) avviene attraverso l'espletamento di uno o più concorsi pubblici, anche in deroga a specifiche previsioni normative che dispongono:

il ricorso a concorsi pubblici unici per le amministrazioni dello Stato, anche ad ordinamento autonomo, le agenzie e gli enti pubblici non economici (ex articolo 4, c. 3-*quinquies* e 3-*sexies*, del decreto-legge n. 101 del 2013);

il ricorso alla Commissione per l'attuazione del Progetto di Riqualificazione delle Pubbliche Amministrazioni (RIPAM) per lo svolgimento delle procedure selettive delle restanti amministrazioni (ai sensi dell'articolo 35, comma 5, del decreto legislativo n. 165 del 2001).

La disposizione fa comunque salva la facoltà per le amministrazioni di avvalersi delle modalità semplificate e delle misure di riduzione dei tempi di accesso al pubblico impiego previste dall'articolo 3 della legge n. 56 del 2019.

Emanuele SCAGLIUSI (M5S), *relatore per la IX Commissione*, illustrando il contenuto delle disposizioni del decreto-legge relative a materie di competenza della IX Commissione, rileva come l'articolo 3 detti disposizioni di raccordo tra il decreto – legge e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla tecnologia 5G.

In particolare, il comma 1 stabilisce che le disposizioni del decreto – legge si applicano ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, anche per i contratti o gli accordi – ove conclusi con soggetti esterni all'Unione europea – relativi ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G, rispetto ai quali è prevista dall'articolo 1-*bis* del decreto-legge in materia di poter speciali n. 21 del 2012, espressamente richiamato, una notifica alla Presidenza del Consiglio dei ministri al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni.

In ragione di ciò è esclusa l'applicazione dell'articolo 1, comma 6, lettera *a)*, che dispone la previsione di un obbligo di comunicazione al CVCN con riferimento 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 indicati nell'elenco da predisporre ai sensi dell'articolo 1, comma 2, lettera *b)* del decreto-legge all'esame.

Il comma 2 detta norme in materia di esercizio dei poteri speciali. Esso stabilisce che dalla data di entrata in vigore del regolamento previsto dall'articolo 1,

comma 6, i poteri speciali 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), (ossia il CVCN e il Centro di valutazione del Ministero della Difesa) sulla base della disciplina prevista in attuazione del predetto regolamento.

Il comma 3 stabilisce una disciplina transitoria, prevedendo la possibilità di ridefinire, nel termine di sessanta giorni dalla data di entrata in vigore del predetto regolamento, le condizioni o le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati con i provvedimenti di esercizio dei poteri speciali relativi a soggetti inclusi nel perimetro di sicurezza nazionale, al fine di garantire livelli di sicurezza equivalenti a quelli previsti dal decreto-legge in esame, anche con prescrizioni di sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza.

L'articolo 4 estende l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori ad alta intensità tecnologica (cosiddetto golden power), contenute nel decreto-legge n. 21 del 2012.

Più in dettaglio:

al comma 1 viene ampliato il perimetro dei beni che possono essere inclusi nell'ambito di applicazione di tale disciplina, nel caso in cui sussista un pericolo per la sicurezza e l'ordine pubblico, attraverso il rinvio alle norme europee; ai fini della verifica del pericolo, viene ricompreso il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti;

ai sensi del comma 2, fino all'entrata in vigore delle norme secondarie che individuano puntualmente i settori rilevanti, sono assoggettati a notifica al Governo gli acquisti, da parte di soggetti esterni all'Unione europea, di partecipazioni in società che detengono specifici beni e rapporti, fra cui le infrastrutture e le tecnologie critiche legate alla gestione dei dati e alla cybersicurezza, nonché le infrastrutture finanziarie; tale notifica in particolare riguarda gli acquisti rilevanti, ovvero in grado di determinare l'insediamento stabile dell'acquirente, in ragione dell'assunzione del controllo della società;

sempre ai sensi del comma 2, a seguito della predetta notifica, il Governo può, sulla base di specifici criteri, esercitare poteri speciali imponendo condizioni e impegni diretti a garantire la tutela degli interessi essenziali dello Stato, nonché opponendosi all'acquisto della partecipazione.

Ricorda, al riguardo, che, per salvaguardare gli assetti proprietari delle società operanti in settori reputati strategici e di interesse nazionale, il legislatore ha organicamente disciplinato, con il decreto-legge 15 marzo 2012, n. 21 – come successivamente modificato nel tempo – la materia dei poteri speciali esercitabili dal Governo anche per aderire alle indicazioni e alle censure sollevate in sede europea.

L'articolo 5 dispone circa alcune attribuzioni emergenziali in capo al Presidente del Consiglio, in caso di rischio grave o crisi di natura cibernetica.

In particolare, si prevede che il Presidente del Consiglio – su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) – possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi posti nel perimetro di sicurezza nazionale cibernetica.

Il predetto intervento disattivatore deve risultare indispensabile e realizzarsi per il tempo strettamente necessario all'eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità.

Tale attribuzione del Presidente del Consiglio è prevista operare allorché si verifichi un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi del

perimetro di sicurezza nazionale cibernetica, e comunque nei casi di crisi cibernetica.

In merito si ricorda che situazione di crisi cibernetica è – secondo la definizione reca dall'articolo 2, comma 1, lettera *o)*, del DPCM del 17 febbraio 2017 – una « situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale ».

L'articolo 6, comma 1, reca la quantificazione degli oneri associati alle disposizioni dell'articolo 1, comma 19, e dell'articolo 2, commi 1 e 3, pari a:

3.200.000 euro per l'anno 2019,

6.495.000 euro per ciascuno degli anni dal 2020 al 2023,

4.395.000 euro annui a decorrere dall'anno 2024.

Il medesimo comma 1 indica quindi le seguenti coperture:

a) quanto a 4.395.000 euro annui a decorrere dall'anno 2020, si dispone la 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 MEF per l'anno 2019, allo scopo parzialmente utilizzando:

l'accantonamento relativo al Ministero dello sviluppo economico (MISE) quanto a euro 350.000 annui a decorrere dall'anno 2020;

l'accantonamento relativo al MEF quanto a euro 4.045.000 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 delle risorse del Fondo per il rilancio degli investimenti delle Amministrazioni centrali dello Stato, istituito dalla legge di bilancio per il 2019 (legge n. 145 del 2018), da imputare sulla quota parte del fondo attribuita al Ministero dello sviluppo economico.

Il comma 2 autorizza il Ministro dell'economia e delle finanze ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

L'articolo 7 dispone che il decreto-legge entri in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*. Il decreto-legge è dunque vigente dal 22 settembre 2019.

Giuseppe BRESCIA, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 14.