COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e IV (Difesa)

S O M M A R I O

SEDE REFERENTE

Mercoledì 2 agosto 2017. — Presidenza del presidente della IV Commissione Francesco Saverio GAROFANI. – Interviene il sottosegretario di Stato per la difesa Domenico Rossi.

La seduta comincia alle 14.05.

Sulla pubblicità dei lavori.

Francesco Saverio GAROFANI, *presidente*, avverte che è pervenuta la richiesta che della seduta sia data pubblicità anche mediante gli impianti audiovisivi a circuito chiuso. Non essendovi obiezioni, ne dispone l'attivazione.

Norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica.
C. 3677 Artini.

(Esame e rinvio).

Le Commissioni iniziano l'esame.

Emanuele FIANO (PD), *relatore per la I Commissione*, osserva che la proposta di legge in esame consta di 24 articoli ed è volta a dettare norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica.

Precisa, quindi, che nella sua relazione esporrà il quadro normativo di riferimento della proposta di legge, mentre il relatore per la IV Commissione, deputato Artini, descriverà il contenuto della proposta medesima.

Ricorda che l'architettura istituzionale italiana per la sicurezza cibernetica è attualmente delineata nel decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante i nuovi indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. Tale provvedimento sostituisce integralmente, pur riprendendone l'impostazione generale, il precedente decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, adottato dal Governo Monti, in linea con analoghe iniziative intraprese a livello europeo nel campo della protezione cibernetica.

Contribuiscono a definire la cornice complessiva dell'attuale sistema di sicu-

rezza cibernetica il Quadro strategico nazionale per la sicurezza dello spazio cibernetico del dicembre 2013 ed il Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017. Il primo di questi due documenti, adottato dal Presidente del Consiglio dei ministri su proposta del Comitato Interministeriale per la Sicurezza della Repubblica (Cisr), rappresenta il Documento di lungo periodo contenente l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, e di quelli nazionali operanti al di fuori del territorio del Paese, l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacità del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza. A sua volta il Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017, adottato, dal Presidente del Consiglio dei ministri su deliberazione del Cisr, rappresenta il documento di breve periodo attraverso il quale sono definiti gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale. Il Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017 sostituisce integralmente il precedente Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2013.

Di estrema rilevanza per la valutazione dell'architettura nazionale per la sicurezza dello spazio cibernetico sono infine le Relazioni annuali sulla politica dell'informazione per la sicurezza predisposte dal Governo e trasmesse al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007. Alla relazione è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica.

Nel nuovo assetto strategico delineato nel citato decreto del 17 febbraio 2017, al Presidente del Consiglio dei ministri è affidata l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza. In tale funzione emana le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema di sicurezza cibernetica e, in particolare, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale.

In presenza di situazioni di crisi che coinvolgono aspetti di sicurezza nazionale il Comitato Interministeriale per la Sicurezza della Repubblica (Cisr), presieduto dal Presidente del Consiglio e composto dall'Autorità delegata e dai ministri degli Affari esteri e della cooperazione internazionale, dell'Interno, della Difesa, della Giustizia, dell'Economia e delle finanze e dello Sviluppo economico, partecipa alle determinazioni del Presidente del Consiglio con funzioni di consulenza e di proposta, nonché di deliberazione. Il CISR, inoltre, esprime parere sulle direttive del Presidente, sorveglia l'attuazione del Piano Nazionale, approva le linee di indirizzo per favorire la collaborazione fra gli attori istituzionali e stabilisce gli obbiettivi in materia di protezione cibernetica nazionale. A supporto del CISR opera il cosiddetto « CISR tecnico » presieduto dal Direttore generale del DIS.

A sua volta spetta al Direttore generale del DIS il compito di definire linee di azione che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità. Per la realizzazione di tali iniziative, il direttore generale del DIS predisporrà gli opportuni moduli organizzativi anche attraverso il coinvolgimento del mondo accademico e della

ricerca ed avvalendosi di risorse di eccellenza e della collaborazione di imprese del settore.

Spetta, invece, al DIS nel suo complesso, coadiuvato dalle Agenzie (AISE e AISI), raccogliere le informazioni finalizzate alla protezione dello spazio cibernetico nazionale e formulare analisi, valutazioni e previsioni della minaccia cibernetica. Inoltre, è consentito al DIS e alle agenzie l'accesso agli archivi informatici delle pubbliche amministrazioni e dei soggetti erogatori di servizi pubblici secondo le modalità previste dal decreto del Presidente del Consiglio dei ministri n. 4 del 2009.

A supporto del Presidente del Consiglio per gli aspetti relativi alla prevenzione e all'approntamento rispetto a situazioni di crisi, opera il Nucleo per la sicurezza cibernetica (Nsc), originariamente istituito presso l'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri ed ora collocato all'interno del DIS. Il Nucleo organismo è chiamato a svolgere una serie di attività nella fase di gestione delle crisi di natura cibernetica, con particolare riferimento agli aspetti relativi alla prevenzione di situazioni di crisi cibernetica e all'attivazione delle procedure di allertamento. Il Nucleo è presieduto da un vice direttore generale del DIS, designato dal direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.

Con particolare riferimento al campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica, spetta al Nucleo per la sicurezza cibernetica: promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale; mantenere attiva, 24 ore su 24 e 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica; valutare e promuovere procedure di condivisione delle informazioni, anche con gli operatori privati interessati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi; acquisire le comunicazioni circa i casi di violazione o dei tentativi di violazione della sicurezza o di perdita dell'integrità dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), nonché dalle strutture del Ministero della difesa e dai *Computer Emergency Response Team* (CERT); promuovere e coordinare, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica; costituire punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE e le altre organizzazioni internazionali e gli altri Stati, ferme restando le specifiche competenze del Ministero dello sviluppo economico, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa e di altre amministrazioni previste dalla normativa vigente, assicurando comunque in materia ogni necessario raccordo. Peraltro, nel campo dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo per la sicurezza cibernetica: riceve, anche dall'estero, le segnalazioni di eventi cibernetici e diramа gli allarmi alle amministrazioni e agli operatori privati; valuta se l'evento assume dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richiede l'assunzione di decisioni coordinate in sede interministe-

riale; informa tempestivamente il Presidente del Consiglio, per il tramite del Direttore Generale del DIS, sulla situazione in atto.

Tra gli attori dell'architettura nazionale preposta a garantire la sicurezza cibernetica e la sicurezza informatica nazionale, il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 include, oltre ai soggetti pubblici, anche gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali e quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici. Tali soggetti sono tenuti a comunicare al Nucleo per la sicurezza cibernetica, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti. fornire informazioni agli organismi di informazione per la sicurezza che consentono ad essi l'accesso ai *Security Operations Center* (SOC) aziendali e ad altri eventuali archivi informatici di specifico interesse ai fini della sicurezza cibernetica; collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Infine, un elemento di novità del decreto del 2017 è la previsione normativa che impegna il Ministro dello sviluppo economico a promuovere l'istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità su prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche.

Massimo ARTINI (Misto-AL-TIpI), *relatore per la IV Commissione,* riferisce che il contenuto della proposta di legge è stato redatto in epoca antecedente all'approvazione del recente « decreto Gentiloni » che ha delineato il nuovo assetto istituzionale in materia di protezione delle infrastrutture cibernetiche ampiamente illustrato dal collega Fiano.

Si augura che il confronto parlamentare sul contenuto della proposta di legge sia particolarmente ampio e costruttivo così da poter giungere non solo alla definizione di un testo ampiamente condiviso, ma soprattutto all'elaborazione di un provvedimento normativo di rango legislativo – il primo in assoluto – in grado di assicurare un efficace sistema di difesa del *cyber-space*, in linea con quanto richiesto sia a livello europeo, sia in ambito Nato.

Osserva, quindi, che la rilevanza del tema concernente la sicurezza cibernetica è nota a tutti.

Come sottolineato anche nel Libro bianco per la sicurezza internazionale e la difesa, gli effetti di attacchi cibernetici alle reti e ai servizi informatici possono essere particolarmente distruttivi per i Paesi occidentali e, se di successo, comportare effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali.

Analoga preoccupazione si evince anche dalla lettura delle Relazioni annuali sulla politica dell'informazione per la sicurezza che il Governo presenta al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007.

Già nella Relazione sulla politica dell'informazione per la sicurezza relativa all'anno 2009 la *cyber-security* veniva definita come « un fondamentale campo di sfida per l'intelligence (...) un fattore di rischio di prima grandezza, direttamente proporzionale al grado di sviluppo raggiunto dalle tecnologie dell'informazione ».

A questa prima analisi hanno fatto seguito – nelle Relazioni presentate al Parlamento negli anni successivi – ulteriori riflessioni, che secondo un livello crescente di intensità hanno considerato la minaccia cibernetica come una « sfida crescente per le politiche di sicurezza degli Stati », un obiettivo informativo prioritario dell'attività d'intelligence nazionale », « la sfida più impegnativa per il sistema Paese in virtù dei peculiari tratti caratterizzanti che attengono tanto al dominio digitale nel quale viene condotta, quanto alla sua

natura diffusa e transnazionale, quanto ancora agli effetti potenziali in grado di produrre ricadute peggiori di quelle ipotizzabili a seguito di attacchi convenzionali e di incidere sull'esercizio di libertà essenziali per il sistema democratico ».

Da qui la necessità di presidiare lo spazio cibernetico al pari dei tradizionali domini operativi, concetto questo ribadito anche nel Vertice Nato di Varsavia del luglio 2015 che ha definito lo spazio cibernetico come il quinto dominio operativo accanto ai tradizionali domini di terra, aria, e mare.

Ciò premesso, la proposta di legge in esame, è composta da 24 articoli e reca disposizioni che riguardano sia le competenze della Commissione Difesa nell'ambito della protezione cibernetica, sia più in generale l'architettura strategica nazionale in materia di sicurezza cibernetica.

Nel settore della difesa specifiche competenze vengono assegnate al Segretario generale della Difesa, direttore nazionale degli armamenti (articolo 4) che dovrà provvedere a: promuovere lo sviluppo della ricerca tecnologica nel campo della sicurezza cibernetica, considerata di interesse militare, secondo gli indirizzi impartiti dal Ministro della difesa; assicurare la piena integrazione delle attività di ricerca militare nel settore cibernetico con quelle previste dal Programma nazionale per la ricerca; predisporre e attuare, nell'ambito della propria competenza, le misure necessarie per agevolare e incrementare lo scambio delle informazioni tra i soggetti utilizzatori delle tecnologie e i soggetti operanti nelle attività di sviluppo o di produzione delle medesime; promuovere iniziative di cooperazione sinergica tra centri di ricerca, università, imprese industriali e operatori finanziari nazionali, con l'eventuale partecipazione di analoghe istituzioni, imprese e operatori esteri, allo scopo di favorire il raggiungimento della piena sovranità cibernetica nazionale e una maggiore integrazione nell'ambito dell'Unione europea.

A sua volta l'articolo 6 della proposta di legge novella l'articolo 10 del codice dell'ordinamento militare al fine di attribuire al Ministro della difesa la specifica competenza in merito all'emanazione di direttive in materia di sicurezza cibernetica, mentre l'articolo 7 modifica l'articolo 89 del codice dell'ordinamento militare, al fine di prevedere tra i compiti delle Forze armate anche quello relativo al concorso nella protezione dello spazio cibernetico.

Da un punto di vista operativo la proposta di legge prevede poi una disciplina particolarmente dettagliata in merito allo svolgimento di contromisure cibernetiche, da riferirsi a quelle azioni mirate di risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale.

Al riguardo, si prevede l'inserimento nel codice del nuovo articolo 89-*bis* volto a definire il procedimento decisionale relativo all'avvio di questa tipologia di operazioni militari cibernetiche e le garanzie funzionali previste per il personale che vi è preposto.

Per quanto concerne l'autorizzazione il primo passaggio procedurale è rappresentato dalla delibera del Consiglio dei ministri in ordine all'utilizzo delle contromisure cibernetiche. Tale deliberazione dovrà essere adottata previa comunicazione al Presidente della Repubblica anche eventualmente convocando il Consiglio supremo di difesa, ove se ne ravvisi la necessità. Successivamente, il Governo dovrà comunicare al Comitato parlamentare per la sicurezza della Repubblica « le misure deliberate ».

In relazione alle garanzie funzionali, il comma 3 del nuovo articolo 89-*bis* richiama quanto previsto dall'articolo 17 della legge 3 agosto 2007, n. 124 che attualmente reca la particolare guarentigia prevista per il personale dei servizi di informazione per la sicurezza. Ai sensi di tale norma non è punibile il personale dei Servizi di informazione per la sicurezza « che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizio ».

Ai sensi del comma 5 del nuovo articolo 89-*bis* la scriminante non opera

per i crimini di genocidio, crimini contro l'umanità, crimini di guerra, e crimini di aggressione, previsti dagli articoli 5 e seguenti dello Statuto della Corte penale internazionale.

Sempre con riferimento al tema della difesa cibernetica la proposta di legge delinea le caratteristiche essenziali del nuovo Comando operativo cibernetico (CIOC), istituito nell'ambito dello stato maggiore della difesa e posto alle dipendenze del Ministro della difesa che, con proprio decreto, da adottare entro quattro mesi dalla data di entrata in vigore della legge, ne definirà le attribuzioni, la struttura e l'organizzazione (articolo 16).

Il CIOC viene identificato dalla proposta di legge in esame quale organismo istituzionalmente deputato ad operare nel settore della sicurezza militare, in coordinamento con il DIS e il RIS. Al CIOC spetta la direzione delle soprarichiamate operazioni relative alle contromisure cibernetiche previste dall'articolo 89-*bis*.

Spetta, a sua volta al CERT difesa organizzare il sistema di protezione dei sistemi cibernetici delle Forze armate ed esercitare le funzioni di punto di riferimento nazionale per i rapporti con le organizzazioni internazionali e con altri Stati, nell'ambito della sicurezza cibernetica nel settore militare.

Da un punto di vista organizzativo il CERT-Difesa viene collocato alle dipendenze del CIOC con la finalità di fornire informazioni sugli eventi cibernetici nel settore cibernetico militare. A tal fine con decreto del Ministro della difesa, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, è definita l'organizzazione del CERT-Difesa nell'ambito del CIOC.

Gli articoli da 9 a 16 della proposta di legge delineano il nuovo assetto istituzionale in materia di protezione cibernetica, individuando i diversi soggetti con competenze in tale ambito ed i relativi compiti.

Al riguardo gli organi richiamati dall'articolo 9 della proposta di legge sono: il Presidente del Consiglio dei ministri, il Comitato interministeriale per la sicurezza della Repubblica (CISR), il Dipartimento delle informazioni per la sicurezza (DIS), il Nucleo per la sicurezza cibernetica (NSC), il Comando interforze operativo cibernetico (CIOC), il CERT nazionale, il CERT-PA, il CERT-Difesa, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche (CNAIPIC) e l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM).

Si tratta di organismi già operativi nell'ambito della protezione cibernetica e regolamentati da precise disposizioni normative, con la sola eccezione del Comando interforze operativo cibernetico (CIOC) in via di implementazione le cui caratteristiche fondamentali sono state illustrate dal Capo di Stato maggiore della difesa, generale Claudio Graziano, nel corso di una sua audizione presso la Commissione Difesa della Camera lo scorso 25 gennaio.

In particolare, nel nuovo assetto delineato dalla proposta di legge al Presidente del Consiglio dei ministri spetta il compito di coordinare le politiche dell'informazione per la sicurezza e di impartire le direttive e, sentito il CISR, emanare ogni disposizione necessaria per l'organizzazione e per il funzionamento del sistema nazionale di sicurezza cibernetica.

Al Presidente del Consiglio dei ministri viene, inoltre, conferito il potere di nominare e revocare il direttore del NSC, sentito il CISR. Ai sensi del successivo articolo 13, l'incarico ha durata biennale e deve essere conferito ad a un soggetto dotato di adeguata qualificazione, appartenente al DIS, al Ministero della difesa, al Ministero dell'interno o al Ministero dello sviluppo economico.

Spetta sempre al Presidente del Consiglio dei ministri il compito di determinare, di concerto con i Ministri dell'economia e delle finanze, dell'interno e della difesa, l'ammontare annuo delle risorse finanziarie destinate all'attività del sistema nazionale di sicurezza cibernetica a valere sul Fondo di cui all'articolo 20 della proposta di legge.

Ai sensi dell'articolo 11 della proposta di legge il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può

delegare le funzioni che non sono ad esso attribuite in via esclusiva a un Ministro senza portafoglio o a un Sottosegretario di Stato.

Spetta, invece al Ministro degli affari esteri e della cooperazione internazionale il compito di nominare, sentita l'AISE, il Direttore per l'analisi cibernetica internazionale (DACI), con il compito di fornire ai competenti organi politici un'analisi geopolitica complessiva rispetto agli eventi cibernetici. L'AISE collabora con il DACI per l'analisi degli eventi cibernetici pertinenti agli interessi italiani all'estero (articolo 12).

Per quanto concerne, invece, le competenze del CERT nazionale, ai sensi dell'articolo 14 della proposta di legge tale organismo è tenuto ad attivare un'Istituzione di un sistema di sistema *InfoSharing* unico che consenta di memorizzare dati con distinte autorizzazioni all'accesso in relazione al livello di segretezza del dato inserito, nel rispetto delle disposizioni della legge 3 agosto 2007, n. 124.

Secondo quanto previsto dall'articolo 14 della proposta di legge spetta sempre al CERT nazionale definire il sistema di accesso e il mantenimento del sistema di *InfoSharing* unico. La definizione delle caratteristiche tecniche relative alla conservazione e all'accesso alle informazioni classificate è a sua volta effettuata d'intesa con il CNAIPIC, il CERT-Difesa e il DIS.

Per quanto concerne, invece, l'esercizio delle funzioni di pubblica sicurezza nell'ambito del nuovo sistema nazionale di sicurezza cibernetico, tale potere viene riconosciuto dall'articolo 15 della proposta di legge in capo al Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche (CNAIPC), in coordinamento con il con il Cert nazionale.

In particolare spetta al CNAIPC, entro sei mesi dalla data di entrata in vigore della legge, definire l'elenco delle infrastrutture strategiche e fornire le linee guida per l'eventuale integrazione del medesimo. In via permanente il CNAIPC provvede, in presenza di un evento cibernetico di gravità tale da poter evolvere in una crisi cibernetica nazionale, a disporre, su richiesta del Presidente del Consiglio dei ministri o dell'Autorità delegata l'interruzione dei pubblici servizi. Provvede, inoltre, alla condivisione con gli altri soggetti del sistema nazionale di sicurezza cibernetica delle notizie necessarie alla risoluzione della crisi cibernetica o dell'evento cibernetico potendo a tal fine provvedere nel più breve tempo possibile alla rimozione dei dati e degli elementi classificati.

L'articolo 17 individua i soggetti istituzionalmente competenti al trattamento dei dati classificati.

Al riguardo, fermo restando il principio generale in forza del quale il DIS esercita la gestione e il trattamento dei dati classificati nel settore della sicurezza cibernetica con gli strumenti e secondo le modalità e le procedure stabiliti dalla legge 3 agosto 2007, n. 124, si prevede altresì che il CERT-Difesa e il CNAIPIC collaborino con il DIS per il trattamento dei dati classificati nel campo della sicurezza cibernetica.

Per quanto concerne il controllo parlamentare, l'articolo 19 fissa il principio generale in forza del quale tutti gli schemi di decreto da adottarsi ai sensi della proposta di legge in esame (articoli 16, 20 e 22) devono essere sottoposti al previo parere delle Commissioni parlamentari competenti per materia, con le modalità e nelle forme stabilite dai regolamenti parlamentari. Il termine per l'espressione del parere è di trenta giorni dalla richiesta. Ove tale termine decorra senza che le Commissioni si siano pronunciate, i decreti potranno essere comunque emanati. Analoga procedura è prevista per l'esame parlamentare delle linee guida comuni.

A sua volta l'articolo 20 prevede l'istituzione nello stato di previsione del Ministero dell'economia e delle finanze, per il successivo trasferimento al bilancio autonomo della Presidenza del Consiglio dei ministri, di un Fondo per la sicurezza cibernetica.

Spetta al Presidente del Consiglio dei ministri, con decreto da emanare entro sessanta giorni dalla data di entrata in

vigore della legge, di concerto con il Ministro della difesa, dello sviluppo economico, dell'interno e dell'economia e delle finanze, definire le modalità di impiego delle somme del fondo. Per quanto concerne la copertura finanziaria, il successivo articolo 21 prevede la riduzione del fondo di cui all'articolo 1, comma 965, della legge 28 dicembre 2015, n. 208.

Al riguardo, ricorda che la legge di stabilità per l'anno 2016 ha istituito nello stato di previsione del Ministero dell'economia e delle finanze un fondo con una dotazione finanziaria di 150 milioni di euro per l'anno 2016 per il potenziamento degli interventi e delle dotazioni strumentali in materia di protezione cibernetica e di sicurezza informatica nazionali nonché per le spese correnti connesse ai suddetti interventi. Si è previsto che un decimo della dotazione finanziaria del fondo è destinato al rafforzamento della formazione del personale del servizio polizia postale e delle comunicazioni, nonché all'aggiornamento della tecnologia dei macchinari e delle postazioni informatiche.

Da ultimo l'articolo 22 autorizza il Governo a modificare il DPCM del 24 gennaio del 2013 che, come sottolineato all'inizio della relazione è stato integralmente abrogato dal recente DPCM del 17 febbraio 2017.

Conclude sollecitando i colleghi che avessero l'intenzione di presentare proposte di legge vertenti sulla stessa materia a predisporre i testi in tempo per consentirne l'abbinamento alla ripresa dei lavori delle Camere dopo la pausa estiva, in modo da poter procedere speditamente ad una riforma che senza dubbio ha carattere strategico per il Paese.

Francesco Saverio GAROFANI, *presidente*, nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

Istituzione del Dipartimento della difesa civile non armata e nonviolenta presso la Presidenza del Consiglio dei ministri.
C. 3484 Marcon.

(Seguito dell'esame e rinvio).

Le Commissioni proseguono l'esame, rinviato nella seduta del 13 luglio 2017.

Francesco Saverio GAROFANI, *presidente*, nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 14.15.