X COMMISSIONE PERMANENTE

(Attività produttive, commercio e turismo)

S O M M A R I O

SEDE CONSULTIVA

Martedì 15 ottobre 2019. — Presidenza del vicepresidente Luca CARABETTA. – Interviene il sottosegretario di Stato per lo sviluppo economico, Mirella Liuzzi.

La seduta comincia alle 13.30.

Sui lavori della Commissione.

Luca CARABETTA, *presidente*, comunica che nella serata di ieri il Ministro dello sviluppo economico, Stefano Patuanelli, ha trasmesso alla presidenza della Commissione una lettera con cui ha rappresentato la oggettiva difficoltà di presenziare alla sua audizione sulle linee programmatiche prevista per oggi per la concomitanza della scadenza del termine per la presentazione dell'offerta per la cessione delle attività aziendali facenti capo alle Società in amministrazione straordinaria Alitalia-Società Aerea italiana Spa ed Alitalia Cityliner Spa. Nella medesima lettera il ministro si è dichiarato disponibile a svolgere l'audizione nella giornata di giovedì 24 ottobre. L'audizione del Ministro è stata conseguentemente sconvocata.

Giorgia ANDREUZZA (LEGA) ritiene che la richiesta di slittamento dell'audizione formulata dal Ministro non sia rispettosa nei confronti della Commissione e dell'organizzazione dei suoi lavori. Auspica, inoltre, che non vi siano ulteriori rinvii dell'audizione medesima.

DL 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
C. 2100 Governo.
(Parere alle Commissioni riunite I e IX).

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento.

Maria Laura PAXIA (M5S), *relatrice*, illustra la relazione, oggetto del provvedimento.

Il decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, oggetto del disegno di legge di conversione C. 2100, all'esame, in sede consultiva, della X Commissione, è composto di 7 articoli.

L'articolo 1 concerne il perimetro di sicurezza nazionale cibernetico. In particolare, il comma 1 istituisce il suddetto

perimetro, 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. Il comma 1 fa riferimento ad amministrazioni pubbliche, nonché ad enti e operatori nazionali, pubblici e privati (investendo così le aree d'interesse della X Commissione), le cui reti e sistemi informativi e informatici sono necessari per l'esercizio di una funzione essenziale dello Stato e per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e il cui malfunzionamento, interruzione, 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, secondo criteri analoghi a quelli definiti nel comma 1. 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. Tale elenco dovrà essere aggiornato con cadenza almeno annuale. Entro sei mesi dall'entrata in vigore del DPCM, gli elenchi così predisposti sono inviati: alla Presidenza del Consiglio dei ministri dai soggetti pubblici e 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; al Ministero dello sviluppo economico dai soggetti privati che rientrano nel perimento 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 Dipartimento delle informazioni per la sicurezza (DIS), e all'organo per la regolarità e sicurezza dei servizi di telecomunicazione presso il Ministero dell'interno. Il comma 3 demanda ad un DPCM, da adottare entro dieci mesi dalla conversione del decreto-legge, la definizione delle procedure per la segnalazione, da parte dei soggetti del perimetro di sicurezza nazionale cibernetica, degli incidenti aventi impatto su reti, sistemi informativi e sistemi e delle misure volte a garantirne elevati livelli di sicurezza Nello specifico, i soggetti interessati devono notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, che inoltra tempestivamente tali notifiche al DIS. Il DIS assicura l'ulteriore trasmissione all'organo del Ministero dell'interno preposto alla sicurezza e regolarità dei servizi di telecomunicazioni e, in determinati casi, alla Presidenza del Consiglio dei ministri ovvero al Ministero dello sviluppo economico. Per quanto riguarda le misure di sicurezza, 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 in modo da agire su: politiche di sicurezza, struttura organizzativa e gestione del rischio; mitigazione e gestione degli incidenti e loro prevenzione; protezione fisica e logica e dei dati informativi; integrità delle reti e dei sistemi informativi; gestione operativa; monitoraggio, *test* e controllo; formazione e consapevolezza; affidamento di forniture, sistemi e servizi di tecnologie dell'informazione e della comunicazione. Il comma 4 dispone che l'elaborazione delle suddette misure di sicurezza è realizzata, secondo l'ambito di propria competenza, dal Ministero per lo sviluppo economico e dalla Presidenza del Consiglio, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e finanze e il DIS. Il comma 5 prevede un aggiornamento almeno biennale delle previsioni dei DPCM di cui ai commi 2 e 3. Il comma 6 rimette ad un regolamento di esecuzione, da emanarsi ai sensi dell'articolo 17, comma 1, della legge 400 del 1988,

entro dieci mesi dalla data di entrata in vigore del decreto-legge, la definizione delle procedure, delle modalità e dei termini alle quali devono attenersi i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, 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, diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati. 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 qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica. L'autorizzazione di spesa per la copertura finanziaria relativa alla realizzazione, all'allestimento e al funzionamento del CVCN è stabilita dal comma 19. 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 (interessando così direttamente le competenze della X Commissione), inclusi nel perimetro di sicurezza nazionale cibernetica. La lettera *a)* prevede che tali soggetti, se inclusi nel perimetro di sicurezza nazionale cibernetica, osservino le misure di sicurezza previste dalle disposizioni vigenti, allorché siano di livello almeno equivalente a quelle adottate con il DPCM attuativo del decreto-legge. Nel caso che non vi sia equivalenza nel livello di sicurezza, le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal decreto-legge sono da definirsi, a seconda dei soggetti interessati, dalla Presidenza del Consiglio dei ministri e dal Ministero dello sviluppo economico. La Presidenza del Consiglio dei ministri e il Ministero dello sviluppo si raccordano, ove necessario, con le autorità NIS *(Network and Information Security)* competenti, di cui all'articolo 7 del decreto legislativo n. 65 del 2018. La lettera *b)* dispone che i soggetti interessati 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 sistema sanzionatorio per i casi di violazione degli obblighi previsti dal decreto-legge. In particolare il comma 9 disciplina una serie di illeciti amministrativi, con sanzioni amministrative pecuniarie scaglionate in relazione alla gravità della condotta. Nel dettaglio sono punite le seguenti fattispecie: il mancato adempimento degli obblighi di predisposizione e di aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informativi; il mancato adempimento dell'obbligo di notifica degli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici; l'inosservanza delle misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica; la mancata collaborazione per l'effettuazione delle attività di test da parte dei fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici; il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di verifica e ispezione; il mancato rispetto delle prescrizioni di utilizzo dettate dal CVCN; la mancata comunicazione dell'intendimento di provvedere 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; l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici su menzionati, in violazione delle condizioni imposte dal CVCN o in assenza del superamento del test di *hardware* e *software*. Ai sensi del comma 10, in caso di inottemperanza alle condizioni o in assenza dell'esito favorevole dei

test di *hardware* e software, il contratto non produce effetto ovvero cessa di produrre effetti ed è fatto divieto alle parti di darvi, anche provvisoriamente, esecuzione. La violazione di tale divieto comporta, per coloro che abbiano disposto l'affidamento del contratto, la sanzione amministrativa accessoria della incapacità ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione. 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 compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici e dei procedimenti relativi all'affidamento di forniture di beni, sistemi e servizi ICT o delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico, forniscono informazioni, dati o fatti non rispondenti al vero oppure 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, che reca 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. Il comma 12 individua nella Presidenza del Consiglio dei ministri e nel Ministero dello sviluppo economico le autorità competenti all'accertamento delle violazioni e all'irrogazione delle sanzioni, mentre il comma 13 richiama l'osservanza delle disposizioni contenute nel capo I, sezioni I e II, della legge n. 689 del 1981. 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 possono incorrere in responsabilità disciplinare e amministrativo-contabile. Il comma 15 prevede che le autorità titolari delle attribuzioni configurate dal decreto-legge assicurino gli opportuni raccordi con il DIS e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. 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). Il comma 17 reca due novelle al decreto legislativo n. 65 del 2018. che 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 concerne l'elenco nazionale degli operatori di servizi essenziali, che l'articolo 4, comma 5, del citato decreto legislativo n. 65 ha istituito presso il Ministero dello sviluppo economico. Con la novella si prevede che il suddetto Ministero trasmetta l'elenco 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 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. Il comma 18 dispone 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.

L'articolo 2 reca misure concernenti il personale, finalizzate a esigenze di funzionamento del Centro di valutazione e certificazione nazionale (CVCN) e della Presidenza del Consiglio dei ministri. Il comma 1 autorizza il MISE ad assumere a tempo indeterminato un contingente massimo di 77 unità di personale, di cui 67 di area terza e 10 di area seconda per lo svolgimento delle funzioni del CVCN. Il comma 2 prevede che, fino al completa-

mento delle procedure di assunzione, il MISE, può avvalersi, per le esigenze del CVCN di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni, con alcune esclusioni, in posizione di fuori ruolo o di comando o altro analogo istituto, per un massimo del 40 per cento delle unità di personale da assumere. Nei limiti complessivi della stessa quota il MISE può avvalersi, in posizione di comando, di personale fino a un massimo di 20 unità. Il comma 3 autorizza la Presidenza del Consiglio ad assumere fino a 10 unità di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione. 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. Il comma 5 dispone che il reclutamento del personale di cui ai commi 1 e 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 o il ricorso alla Commissione per l'attuazione del Progetto di Riqualificazione delle Pubbliche Amministrazioni (RIPAM). È fatta comunque salva la facoltà per le amministrazioni di avvalersi delle modalità semplificate e delle misure di riduzione dei tempi di accesso al pubblico impiego.

L'articolo 3 reca disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5 G. Il comma 1 stabilisce che le disposizioni del decreto 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 su la tecnologia 5G, rispetto ai quali è prevista dall'articolo 1-*bis* del decreto-legge in materia di poteri 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),* ove dispone la previsione di un obbligo di comunicazione al CVCN. Il comma 2 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 del CVCN e del Centro di valutazione del Ministero della difesa. Il comma 3 prevede una disciplina transitoria, con 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, anche con prescrizioni di sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza.

L'articolo 4 reca disposizioni in materia di infrastrutture e tecnologie critiche ed estende l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori ad alta intensità tecnologica (il cosiddetto *golden power*), contenute nel decreto-legge n. 21 del 2012, che viene contestualmente novellato, ed è di particolare interesse per la X Commissione. Il comma 1 amplia il perimetro dei beni che possono essere inclusi nell'ambito di applicazione della suddetta 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. Il comma 2 prevede che, 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. Il medesimo comma chiarisce che la 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 e stabilisce che, a seguito della 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.

L'articolo 5, composto di un unico comma, concerne le determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica. L'articolo, in particolare, prevede che il Presidente del Consiglio, su deliberazione del 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. L'intervento deve risultare indispensabile e realizzarsi per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità. Si prevede che l'attribuzione del Presidente del Consiglio operi nel caso che 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.

L'articolo 6 reca la copertura finanziaria del provvedimento.

L'articolo 7, infine, in base al dettato costituzionale dispone che il decreto-legge entri in vigore il giorno successivo a quello della sua pubblicazione in *Gazzetta Ufficiale*.

Luca CARABETTA, *presidente*, nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 13.40.