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

ATTI DEL GOVERNO

Mercoledì 17 giugno 2020. — Presidenza del presidente della IX Commissione Alessandro MORELLI. — Interviene il sottosegretario di Stato per i rapporti con il Parlamento Gianluca Castaldi.

La seduta comincia alle 11.30.

Schema di decreto del Presidente del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica.
Atto n. 177.

(Esame, ai sensi dell'articolo 143, comma 4, del regolamento, e rinvio).

Le Commissioni iniziano l'esame dello schema di decreto all'ordine del giorno.

Alessandro MORELLI, *presidente,* ricorda che il termine per l'espressione del parere da parte delle Commissioni riunite sul provvedimento in titolo è fissato al 4 luglio 2020.

Emanuele SCAGLIUSI (M5S), *relatore per la IX Commissione,* anche a nome del collega Cattoi, relatore per la I Commissione, rileva preliminarmente come il provvedimento si inserisca in un contesto globale nel quale, in considerazione dell'accresciuta esposizione alle minacce cibernetiche, si è imposta la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela.

Al riguardo segnala che a livello di Unione europea la direttiva (UE) 2016/1148 del 6 luglio 2016 ha introdotto misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta direttiva NIS – *Network and Information Security*) al fine di conseguire un « livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea ». La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 2018, che detta quindi la cornice legislativa delle 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 NIS.

Per quanto riguarda il quadro normativo nazionale, rileva come lo schema di decreto del Presidente del Consiglio in esame sia stato adottato in attuazione

dell'articolo 1, comma 2, del decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, il quale è stato adottato appunto al fine di assicurare, in particolare, un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Ricorda, altresì, che il predetto decreto-legge n. 105 del 2019 ha istituito il perimetro di sicurezza nazionale cibernetica, con il fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato o 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, o dall'utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

L'attuazione della disciplina del perimetro di sicurezza cibernetica è articolata in diverse fasi.

La prima di queste è realizzata dallo schema di decreto in esame, che, in attuazione di quanto disposto dall'articolo 1, comma 2, del decreto-legge n. 105, provvede a definire le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge (secondo quanto previsto dall'articolo 1, comma 2, lettera *a*) nonché a definire i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica (secondo quanto previsto dall'articolo 1, comma 2, lettera *b*).

In proposito, ricorda che l'articolo 27 del decreto-legge n. 162 del 2019 ha modificato l'originaria formulazione dell'articolo 1, comma 2, lettera *a)*, del decreto-legge n. 105 del 2019, introducendovi contestualmente un nuovo comma 2-*bis*. A seguito delle modifiche è stata affidata – secondo le procedure previste dal decreto-legge n. 105 del 2019 e, quindi, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) e previo parere delle competenti Commissioni parlamentari – ad un decreto del Presidente del Consiglio dei ministri (di cui all'articolo 1, comma 2), la definizione delle modalità e dei criteri procedurali di individuazione dei soggetti da includere nel perimetro.

Evidenzia, altresì, che la puntuale elencazione dei soggetti inclusi nel perimetro ed individuati ai sensi dello stesso decreto del Presidente del Consiglio dei ministri è rimessa ad un « atto amministrativo », da adottare da parte del Presidente del Consiglio dei ministri, su proposta del CISR, entro 30 giorni dalla data di entrata in vigore del predetto decreto del Presidente del Consiglio dei ministri (ai sensi del nuovo comma 2-*bis*). Per tale atto amministrativo è espressamente escluso il diritto di accesso e viene specificato come lo stesso non sia soggetto a pubblicazione. Dell'avvenuta iscrizione nell'elenco viene data, separatamente e senza ritardo, comunicazione a ciascun soggetto.

Segnala, inoltre, che tale modifica rispetto all'impianto iniziale del decreto-legge n. 105 del 2019, che affidava l'individuazione dei soggetti inclusi interamente al DPCM, si è resa opportuna, secondo quanto evidenziato nella relazione illustrativa, in quanto l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, considerato nella sua interezza, presenta particolari profili di sensibilità sotto il profilo della sicurezza. Ciò in quanto, dalla sua conoscenza, è possibile

ricostruire il quadro complessivo delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati dalle cui reti, sistemi informativi e servizi informatici dipende l'esercizio di funzioni essenziali dello Stato ovvero la prestazione di servizi essenziali 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.

Evidenzia inoltre che lo schema di DPCM in esame, come prescritto dalla norma che ne costituisce il presupposto, è stato adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR). Sul testo è stato acquisito il parere del Consiglio di Stato, reso nell'adunanza della Sezione consultiva per gli atti normativi del 21 maggio 2020. Segnala, altresì, che l'articolo 1, comma 4-*bis* del decreto-legge n. 105 del 2019 prevede che lo schema di decreto sia trasmesso anche al Comitato parlamentare per la sicurezza della Repubblica (Copasir).

Passando a sintetizzare il contenuto dello schema di decreto, che si compone di 12 articoli, suddivisi in 4 capi, evidenzia come l'articolo 1 contenga le definizioni impiegate nel testo dello schema, alcune delle quali provvedono a chiarire concetti introdotti dal decreto-legge n. 105 del 2019, la cui individuazione puntuale è necessaria alla sua attuazione.

Tra le definizioni si richiamano in particolare le seguenti:

pregiudizio per la sicurezza nazionale: danno o pericolo di danno all'indipendenza, integrità o alla sicurezza della Repubblica e delle istituzioni democratiche, ovvero agli interessi politici, militari, economici, scientifici e industriali conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale (lettera *f*);

compromissione: la perdita di sicurezza o di efficacia dello svolgimento di una funzione essenziale dello Stato o di un servizio essenziale, connessa al malfunzionamento, all'interruzione, anche parziali, ovvero all'utilizzo improprio di reti, sistemi informativi e servizi informatici (lettera *g*);

incidente: evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici (lettera *h*);

rete, sistema informativo (lettera i):

1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera *dd)*, del decreto legislativo n. 259 del 2003 (ossia sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata);

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale;

3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione, compresi i programmi di cui al numero 2);

servizio informatico: il servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi Informativi, ivi incluso quello di *cloud computing* (lettera *l*);

bene ICT: un insieme di reti, sistemi informativi e servizi informatici, o parti di

essi, di qualunque natura considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali (lettera *m*);

parte minimale di un bene ICT: una parte di un bene ICT, tale che la compromissione di essa comporta la compromissione del bene ICT ai fini dello svolgimento di una funzione essenziale dello Stato o dell'erogazione di un servizio essenziale (lettera *n*);

architettura e componentistica: l'insieme delle architetture realizzate e dei componenti usati a livello di rete, dati e *software*, ivi inclusi la distribuzione su piattaforme di cloud computing, nonché le procedure e i flussi informativi per l'accesso, acquisizione, trasmissione, conservazione, elaborazione e recupero dei dati necessari all'espletamento dei servizi informatici (lettera *o*);

analisi del rischio: un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale, e conseguentemente di trattare tale rischio individuando ed implementando idonee misure di sicurezza (lettera *aa*).

Richiama anche la definizione di amministrazione dello Stato, per la quale la lettera *e)* dell'articolo 1, comma 1, fa rinvio alle amministrazioni di cui all'articolo 8, comma 1, della legge 124 del 2015 (legge di delega di riforma della pubblica amministrazione approvata nella scorsa legislatura), in luogo del consueto riferimento all'articolo 1, comma 2, del decreto legislativo n. 165 del 2001 (recante Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche). Come rilevato anche dal Consiglio di Stato nel suo parere, tale scelta sembrerebbe motivata dal fatto che la nozione ricavabile dalla legge n. 124 del 2015 è più selettiva rispetto a quella, più ampia, desumibile dal decreto legislativo n. 165 del 2001.

Segnala quindi che gli articoli 2 e 3 dello schema contribuiscono a delineare le modalità per l'individuazione dei soggetti inclusi nel perimetro oggetto del successivo Capo II dello schema stesso.

In particolare sottolinea che l'articolo 2 fornisce una definizione di funzione essenziale e di servizio essenziale.

Si tratta di due concetti introdotti dal decreto-legge n. 105 del 2019, che, all'articolo 1, comma 2, lettera *a)*, oltre a demandare al DPCM l'adozione puntuale delle modalità e criteri procedurali per l'individuazione dei soggetti del perimetro *cyber*, provvede a definire direttamente alcuni di questi criteri ed in particolare stabilisce che ai fini dell'individuazione si debba procedere sulla base dei seguenti criteri:

il soggetto deve esercitare una funzione essenziale dello Stato o assicurare un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato (articolo 1, comma 1, lettera *a)*, numero 1), del citato decreto-legge n. 105);

l'esercizio di tale funzione o la prestazione di tale servizio deve dipendere da reti, sistemi informativi e servizi informatici (articolo 1, comma 1, lettera *a)*, numero 2) del decreto-legge n. 105).

Inoltre, il decreto-legge n. 105 ha introdotto un terzo criterio generale, secondo il quale l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici (ai sensi dell'articolo 1, comma 1, lettera *a)*, numero 2-*bis*).

In questo quadro l'articolo 2, lettera *a)* dello schema di decreto provvede a definire il concetto di funzione essenziale, prevedendo che un soggetto esercita una funzione essenziale se l'ordinamento gli attribuisca compiti rivolti a assicurare:

la continuità dell'azione di Governo e degli Organi costituzionali;

la sicurezza interna ed esterna e la difesa dello Stato;

le relazioni internazionali;

la sicurezza e l'ordine pubblico;

l'amministrazione della giustizia;

la funzionalità dei sistemi economico e finanziario, e dei trasporti.

Rileva, in particolare, come il riferimento alla « continuità dell'azione degli Organi costituzionali » sia suscettibile di ulteriore approfondimento alla luce delle previsioni del decreto-legge n. 105 del 2019 (che non ne fanno espresso richiamo) e di quanto evidenziato dal Consiglio di Stato nel parere reso sullo schema di DPCM.

Nel parere del Consiglio di Stato si evidenzia, in proposito, come il riferimento agli Organi costituzionali – che non è contenuto nell'articolo 1 del decreto-legge n. 105 del 2019 – richiede « un chiarimento e una precisazione, atteso che (certamente) non è consentito al decreto in esame di imporre adempimenti in capo agli Organi costituzionali, che godono, in quanto tali, di una propria speciale autonomia e indipendenza organizzativa e funzionale. Deve in primo luogo chiarirsi che nella nozione qui fornita (e dunque, successivamente, nel relativo elenco) dei soggetti sottoposti al particolare regime di coordinamento e controllo introdotto dal perimetro di sicurezza nazionale cibernetica (con annessi obblighi e adempimenti), non possono includersi, *sic et simpliciter*, gli « Organi costituzionali », pena il rischio di una lesione della loro sfera di autonomia e indipendenza costituzionalmente garantita. Conseguentemente la disposizione sopra trascritta deve essere letta, correttamente, ponendo l'accento sul riferimento ai soggetti che svolgono « compiti rivolti ad assicurare la continuità dell'azione degli Organi costituzionali », e non sul riferimento agli Organi costituzionali in quanto tali. Occorre tuttavia precisare che, indubbiamente, anche gli Organi costituzionali (anzi, essi in primo luogo e per certi aspetti più degli altri) svolgono (per definizione) una « funzione essenziale dello Stato » (inteso qui come ordinamento e non come mero apparato, ovviamente, così come è altrettanto vero che un perimetro di sicurezza nazionale cibernetica non sembra poter prescindere dal tema della sicurezza cibernetica che presidia le funzioni essenziali di tali organi, se non altro a fini di coordinamento e di (auspicabile) razionalità ed efficienza ed efficacia dell'intero sistema. Alla luce di queste considerazioni la Sezione ritiene necessario che nel testo del decreto in esame sia inserita un'integrazione volta a chiarire che le previsioni in esso contenute non devono e non possono in alcun modo ledere l'autonomia propria degli Organi costituzionali e che eventuali esigenze di coordinamento, di cooperazione e di sinergia, nel quadro del perimetro di sicurezza nazionale cibernetica, potranno opportunamente essere definite e sviluppate secondo le modalità da definirsi mediante accordi e intese con gli Organi costituzionali medesimi ».

L'articolo 2, lettera *b)*, dello schema definisce il concetto di servizio essenziale in connessione con le seguenti attività svolte dal soggetto interessato:

attività strumentali all'esercizio di funzioni essenziali dello Stato;

attività necessarie per l'esercizio e il godimento dei diritti fondamentali;

attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;

attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

L'articolo 3, comma 1, individua i settori di attività in cui operano i soggetti da inserire nel perimetro di sicurezza cibernetica.

Si tratta di un elenco di settori prioritari, che in base al principio di gradua-

lità sopra richiamato potrà essere esteso ad altri settori in sede di aggiornamento.

I settori di attività individuati dalla norma sono i seguenti: governativo, quale settore concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR.

Per quanto riguarda le amministrazioni dello Stato occorre fare riferimento alla definizione di cui all'articolo 1, comma 1, lettera *e)*, che fa rinvio all'articolo 8, comma 1, della legge n. 124 del 2015, mentre le amministrazioni CISR sono costituite da quelle ivi rappresentate ai sensi dell'articolo 5 della legge n. 125 del 2007 e richiamate dall'articolo 1, comma 1, lettera *d)* dello schema, ossia: Presidente del Consiglio dei ministri, Ministro degli affari esteri, Ministro dell'interno, Ministro della difesa, Ministro della giustizia, Ministro dell'economia e delle finanze e Ministro dello sviluppo economico; difesa; spazio e aerospazio; energia; telecomunicazioni; economia e finanza; trasporti; servizi digitali; tecnologie critiche, di cui all'articolo 4, paragrafo 1, lettera *b)*, del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo.

Si tratta delle tecnologie critiche e prodotti a duplice uso quali definiti nell'articolo 2, punto 1, del regolamento (CE) n. 428/2009 del Consiglio, tra cui l'intelligenza artificiale, la robotica, i semiconduttori, la cybersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie, enti previdenziali e lavoro.

Evidenzia, inoltre, che l'articolo 3, comma 2, dello schema individua, per ciascun settore di attività di cui sopra, le amministrazioni che dovranno in concreto individuare i soggetti inclusi nel perimetro (ai sensi dell'articolo 5) secondo le modalità di cui all'articolo 4.

Le amministrazioni individuate sono le seguenti:

amministrazioni CISR, ciascuna nell'ambito di rispettiva competenza per il settore governativo;

Ministero della difesa per il settore difesa;

Presidenza del Consiglio dei ministri, per il settore spazio e aerospazio, in quanto soggetto cui è attribuita dalla legge 11 gennaio 2018, n. 7 l'alta direzione, la responsabilità politica generale e il coordinamento delle politiche dei Ministeri relative ai programmi spaziali e aerospaziali, nell'interesse dello Stato;

Ministero dello sviluppo economico, per i settori energia, telecomunicazioni e servizi digitali, per quest'ultimo in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione (ossia il Dipartimento per la trasformazione digitale istituito con il DPCM 19 giugno 2019, quale struttura di supporto del Ministro per la innovazione tecnologica e la digitalizzazione);

Ministero dell'economia e delle finanze, per il settore economia e finanze;

Ministero delle infrastrutture e dei trasporti, per il settore dei trasporti;

struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per il settore tecnologie critiche, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca;

Ministero del lavoro, per il settore enti previdenziali e lavoro.

L'articolo 4 definisce le modalità ed i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

A tal fine il comma 1 dispone che spetta alle amministrazioni competenti (di cui all'articolo 3, comma 2, dello schema), in relazione ai settori di attività di competenza:

identificare le funzioni e i servizi essenziali – di diretta pertinenza o esercitati da soggetti vigilati o da operatori pubblici e privati – che dipendono da reti,

sistemi informativi o servizi informatici la cui interruzione o compromissione possa « arrecare un pregiudizio per la sicurezza nazionale »;

valutare diversi profili tenendo conto della rilevanza di ciascun criterio in relazione ai settori di attività.

In particolare, le competenti amministrazioni sono chiamate a valutare, per quanto riguarda gli effetti di una interruzione della funzione o servizio essenziale, elementi quali l'estensione territoriale, il numero e la tipologia di utenti potenzialmente interessati, i livelli di servizio garantiti, le possibili ricadute economiche. Per quanto riguarda gli effetti della compromissione dello svolgimento della funzione o servizio essenziale, le amministrazioni sono tenute a valutare le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati con riferimento alla tipologia e quantità degli stessi, alla loro sensibilità e allo scopo cui sono destinati.

Le amministrazioni sono tenute altresì a valutare la possibile mitigazione – rispetto all'interruzione o alla compromissione dello svolgimento della funzione o servizio essenziale – avuto riguardo al tempo necessario per ripristinare lo svolgimento in condizioni di sicurezza, tenendo altresì conto della possibilità che la funzione o il servizio essenziale possano essere assicurati con modalità prive di supporto informatizzato, anche temporaneamente, ovvero parzialmente da altri soggetti.

Le amministrazioni individuano le funzioni o servizi essenziali per i quali sulla base dei suddetti criteri e delle conseguenti valutazioni – in caso di interruzione o compromissione – « il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime » ed operano una graduazione in scala crescente: individuano quindi i soggetti che svolgono tali funzioni o servizi essenziali.

In fase di prima applicazione sono individuati i soggetti titolari di tali funzioni o servizi per i quali un'interruzione delle relative attività comporterebbe il mancato svolgimento della funzione o del servizio.

Riferisce, altresì, che l'articolo 5 dispone in ordine alla formazione dell'elenco dei soggetti inclusi nel perimetro. A tal fine, le amministrazioni interessate, in relazione ai settori di attività di competenza, predispongono una lista di soggetti. Tale elenco provvisorio è trasmesso al CISR e al CSIR tecnico.

L'elencazione dei soggetti è formalizzato in un decreto del Presidente del Consiglio dei ministri, di natura non regolamentare, adottato e aggiornato su proposta del CISR.

In proposito ricorda che l'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019 fa riferimento, ai fini della formalizzazione dell'elenco ad un atto amministrativo del Presidente del Consiglio. L'elenco, come previsto dal decreto-legge n. 105 del 2019, non è pubblicato e non è accessibile.

Il Dipartimento delle informazioni per la sicurezza (DIS) ne dà comunicazione: alle amministrazioni interessate che a loro volta informano ciascun soggetto incluso nel perimetro; alla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione, per i soggetti pubblici e per i soggetti che forniscono servizi fiduciari qualificati o svolgono l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale o svolgono l'attività di conservatore di documenti informatici (di cui all'articolo 29 del codice dell'amministrazione digitale adottato con il decreto legislativo n. 82 del 2005), e al Ministero dello sviluppo economico, per quelli privati; al Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (C.N.A.I.P.I.C.) organo del Ministero dell'interno competente per la sicurezza e la regolarità dei servizi di telecomunicazione del Ministero dell'interno, istituito dal DM 9 gennaio 2008, in attuazione di quanto disposto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005.

Illustra quindi l'articolo 6 che dispone, al comma 1, l'istituzione di un Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR.

In particolare, ai sensi del comma 3, il CISR si avvale del Tavolo per l'esercizio delle funzioni istruttorie correlate all'articolo 5 (elencazione dei soggetti inclusi nel perimetro) e per il supporto ad ogni altra attività attribuita al CISR o al CISR tecnico dal decreto-legge n. 105 del 2019.

Ai sensi del comma 2 il Tavolo è presieduto da un vice direttore del DIS ed è composto da: due rappresentanti di ciascuna amministrazione CISR; un rappresentante per ciascuna delle due agenzie di informazioni;

Ricorda, in particolare, che il Sistema di informazione per la sicurezza della Repubblica è composto: dal Presidente del Consiglio dei ministri; dall'eventuale Autorità delegata dal Presidente del Consiglio; dal Comitato interministeriale per la sicurezza della Repubblica (CISR); dal Dipartimento delle informazioni per la sicurezza (DIS); dall'Agenzia informazioni e sicurezza esterna (AISE); dall'Agenzia informazioni e sicurezza interna (AISI); da due rappresentanti dei ministeri di volta in volta interessati che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare.

È previsto che il Tavolo si riunisca periodicamente, e comunque almeno una volta ogni 6 mesi, e può essere convocato di iniziativa del presidente o su richiesta di almeno un componente.

Possono essere chiamati a partecipare alle riunioni rappresentanti di altre pubbliche amministrazioni, enti e operatori pubblici e privati.

Non sono dovuti gettoni di presenza, compensi o rimborsi spese o altri emolumenti per la partecipazione alle riunioni. La partecipazione costituisce, in base alla disposizione, « dovere d'ufficio » (sembra doversi intendere per i rappresentanti di soggetti pubblici).

Evidenzia che l'articolo 7, in attuazione di quanto previsto dall'articolo 1, comma 2, lettera *b)*, del decreto-legge n. 105 del 2019, definisce i criteri per la predisposizione e l'aggiornamento degli elenchi di beni ICT di rispettiva pertinenza, da parte dei soggetti inclusi nel perimetro di sicurezza nazionale.

La richiamata lettera *b)* del comma 2 dell'articolo 1 del decreto-legge n. 105 prevede infatti che siano definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e dei relativi obblighi, predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007.

All'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR (Comitato interministeriale per la sicurezza della Repubblica), integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco, i soggetti pubblici e quelli qualificati e accreditati a svolgere servizi fiduciari qualificati o 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 7 marzo 2005, n. 82), nonché quelli privati, di cui al comma 2-*bis*, 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.

Ricorda, inoltre, che in base all'articolo 1, comma 5, del decreto-legge n. 105 del 2019, il DPCM sarà oggetto di aggiornamento, con le medesime modalità di adozione del decreto originario, con cadenza almeno biennale.

Per quanto riguarda il concetto di « bene ICT », rammenta che questo è definito nell'articolo 1, comma 1, lettera *m)*, dello schema, come « un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali » secondo quindi una nozione funzionale.

Gli elenchi dei beni ICT vengono aggiornati con cadenza almeno annuale, secondo i criteri definiti nello stesso articolo 7, comma 2, in base ai quali, ricevuta la comunicazione di essere inclusi nel perimetro di sicurezza nazionale i soggetti, in esito all'analisi del rischio ed in applicazione del criterio di gradualità per ogni funzione essenziale o servizio essenziale, dovranno:

a) individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale, valutando l'impatto di un eventuale incidente sul bene ICT e le dipendenze con altri reti e sistemi informativi, informatici o infrastrutture fisiche di altri soggetti, compresi quelli utilizzati per fini di manutenzione e gestione;

b) predisporre l'elenco dei beni ICT, individuando, ove possibile, le parti minimali di ciascun bene ICT, che sono definite alla lettera *n)* dell'articolo 1 dello schema come « una parte di un bene ICT, tale che la compromissione di essa comporta la compromissione del bene ICT ai fini dello svolgimento di una funzione essenziale dello Stato o dell'erogazione di un servizio essenziale ».

Segnala, quindi, che, in fase di prima applicazione, si prevede, in ossequio al principio di gradualità, siano conferiti i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento, adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, per l'attuazione da parte del DIS delle disposizioni impartite dal Presidente del Consiglio dei Ministri, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza.

L'articolo 8 prevede che l'architettura e la componentistica relative ai beni ICT individuati negli elenchi, siano descritte conformemente ad un modello predisposto e periodicamente aggiornato dal DIS, che ne cura la comunicazione ai soggetti interessati. Il modello è predisposto sentito il CISR tecnico e contiene l'indicazione degli elementi utili alla descrizione dei beni ICT e delle relative dipendenze, nonché le informazioni per la trasmissione degli elenchi, disciplinata dal successivo articolo 9.

L'articolo 9 prevede i tempi e le procedure per la trasmissione degli elenchi dei beni ICT, disponendo che i soggetti che rientrano nel perimetro nazionale, entro sei mesi dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco, trasmettano gli elenchi di beni ICT.

La trasmissione deve avvenire, anche per i successivi aggiornamenti degli elenchi, tramite una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al NSC, e deve essere comprensiva della descrizione dell'architettura e della componentistica, secondo un modello predisposto dal DIS, nonché dell'analisi del rischio.

La trasmissione stessa deve avvenire rispettivamente, alla struttura della Presidenza del Consiglio dei ministri per l'innovazione tecnologica e la digitalizzazione e al Ministero dello sviluppo economico.

In merito ricorda che il Codice delle comunicazioni elettroniche (di cui al decreto legislativo n. 259 del 2003) prevede, all'articolo 16-*bis*, l'obbligo per le imprese che forniscono reti pubbliche di telecomunicazione o servizi di comunicazione elettronica accessibili al pubblico di adottare adeguate misure di natura tecnica e organizzativa per garantire la sicurezza di tali reti e servizi, nonché di comunicare al Ministero dello sviluppo economico ogni significativa violazione della sicurezza o perdita dell'integrità delle reti. In attuazione di tale previsione, il decreto del MISE 12 dicembre 2018 ha individuato adeguate misure di natura tecnico-organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica e ha definito i casi in cui le violazioni della rete o la perdita dell'integrità sono da considerarsi significative, ai fini della notifica da parte dei fornitori di reti e servizi di comunicazione alle competenti Autorità.

Il comma 2 dell'articolo 9 dello schema prevede che la struttura della Presidenza del Consiglio per l'innovazione tecnologica e il Ministero dello sviluppo economico, per i profili di competenza, accedano alla piattaforma ai fini dello svolgimento delle attività di ispezione e verifica indicate: dall'articolo 1, comma 6, lettera *c)*, del decreto-legge n. 105 del 2019, secondo il quale la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, secondo la ripartizione di competenza indicata nelle disposizioni del decreto-legge, svolgono attività di ispezione e verifica 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 inseriti nell'elenco, connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte dalle strutture specializzate in tema di protezione di reti e sistemi, nei casi in cui siano espressamente previste dalla legge, 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, dall'articolo 1, comma 12, del decreto-legge n. 105 del 2019, il quale prevede che per le attività di accertamento delle violazioni e irrogazione delle sanzioni amministrative, la Presidenza del Consiglio dei ministri è competente nei confronti delle amministrazioni pubbliche, degli enti e degli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale, 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 sono individuati i compiti delle autorità competenti, mentre il Ministero dello Sviluppo economico è competente per gli operatori nazionali privati inclusi nel perimetro di sicurezza nazionale.

In merito ricorda che l'articolo 6, comma 1 del decreto-legge n. 105 del 2019 ha rimesso ad un regolamento da emanarsi con decreto del Presidente del Consiglio dei ministri, entro 10 mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, 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.

Il comma 3 dell'articolo 9 dello schema specifica che la struttura della Presidenza del Consiglio dei ministri per l'innovazione

tecnologica e la digitalizzazione, in relazione alle reti, ai sistemi informativi e ai servizi informatici connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, accede alla piattaforma limitatamente alle informazioni necessarie, individuate dal modello, per lo svolgimento delle attività di accertamento delle violazioni e irrogazione delle sanzioni amministrative.

Il comma 4 specifica inoltre che l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (di cui all'articolo 7-*bis* del decreto-legge n. 144 del 2005), accede per il tramite della piattaforma digitale agli elenchi dei beni ICT e fornisce alla stessa piattaforma gli elenchi di pertinenza del Ministero.

L'articolo 10 reca disposizioni per la tutela delle informazioni, prevedendo che l'elenco dei soggetti inclusi nel perimetro nazionale di cui all'articolo 5, comma 2, e gli elenchi dei beni ICT, comprensivi della descrizione dell'architettura e della componentistica, nonché dell'analisi del rischio, siano sottoposti ad idonee misure di sicurezza, previste con decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell'articolo 1, comma 3, del decreto-legge n. 105 del 2019, quindi su proposta del CISR, fatta salva l'adozione delle misure di sicurezza previste in caso di attribuzione agli elenchi di classifiche di segretezza ai sensi dell'articolo 42 della legge n. 124 del 2007.

Il comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019 dispone che con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative, adottato su proposta del CISR, siano stabilite le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici rientranti nell'elenco di cui si tratta.

Ricorda in proposito che il comma 4-*bis* dell'articolo 1 del decreto-legge n. 105 prevede che gli schemi dei decreti di cui al comma 3 siano altresì trasmessi alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il decreto può essere comunque adottato. I medesimi schemi sono altresì trasmessi al Comitato parlamentare per la sicurezza della Repubblica.

Evidenzia, inoltre, che l'articolo 11 reca le disposizioni transitorie, prevedendo che i soggetti inclusi nel perimetro osservino, in relazione alle reti, ai sistemi informativi e ai servizi informatici, di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, gli obblighi, in materia di notifica degli incidenti, di misure di sicurezza, nonché di affidamento delle forniture, di cui all'articolo 1, commi 1 e 6, del decreto-legge n. 105 del 2019, a decorrere dalle date indicate dal DPCM previsto dall'articolo 1, comma 3, del medesimo decreto-legge n. 105, da emanare entro 10 mesi e che riguarda sia le procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica che le misure di sicurezza, nonché dal regolamento di cui all'articolo 1, comma 6, dello stesso decreto-legge, sempre da adottare entro dieci mesi, per la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT.

Il comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019 prevede infatti che con decreto del Presidente del Consiglio dei ministri, siano definite le procedure secondo cui i soggetti rientranti nel perimetro notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, che inoltra tali notifiche, tempestivamente, al Dipartimento delle in-

formazioni per la sicurezza (DISE) anche per le attività demandate al Nucleo per la sicurezza cibernetica.

Spetta poi al DISE trasmettere tali notifiche all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo n. 82 del 2005, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato.

L'articolo 12 contiene la clausola di invarianza finanziaria.

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

La seduta termina alle 11.40.