IV COMMISSIONE PERMANENTE

(Difesa)

S O M M A R I O

DELIBERAZIONE DI RILIEVI SU ATTI DEL GOVERNO

Martedì 30 giugno 2020. — Presidenza del vicepresidente Roger DE MENECH. — Interviene il sottosegretario di Stato per la difesa, Angelo Tofalo.

La seduta comincia alle 12.45.

Sulla pubblicità dei lavori.

Roger DE MENECH, *presidente*, avverte che la pubblicità della seduta sarà garantita anche mediante l'impianto audiovisivo a circuito chiuso.

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

(Rilievi alle Commissioni riunite I e IX).

(Esame e rinvio).

La Commissione inizia l'esame dello schema.

Roger DE MENECH, *presidente*, ricorda che l'atto del Governo è all'esame, in sede primaria, delle Commissioni riunite Affari costituzionali e Trasporti e che l'Ufficio di Presidenza della Commissione Difesa ha deliberato di richiedere al Presidente della Camera l'autorizzazione a esprimere i propri rilievi. L'autorizzazione è stata accordata.

Roberto ROSSINI (M5S), *relatore*, introduce l'esame dello schema di decreto del Presidente del Consiglio osservando che esso è stato adottato ai sensi 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. Ricorda che il citato decreto-legge, esaminato da questa Commissione in sede consultiva in due tornate, il 22 ottobre e il 12 novembre 2019, ha istituito il cosiddetto « perimetro di sicurezza nazionale cibernetica », al 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. Prima di illustrare nel dettaglio il contenuto del provvedimento in esame evidenzia che il medesimo, così come il richiamato decreto-legge n. 105 del 2019, si inseriscono nel solco di una serie di iniziative normative avviate da tempo in ambito nazionale, europeo e internazionale e volte a rafforzare la sicurezza cibernetica di taluni *asset* strategici dei singoli Paesi, rispetto a eventi di natura volontaria o accidentale che potrebbero comprometterne o alterarne il funzionamento. Tale rafforzamento degli strumenti di sicurezza cibernetica è da collegare alla rapida e pressoché ininterrotta evoluzione delle tecnologie dell'informazione e della comunicazione (*information and communication technology*, ICT) grazie alle quali vengono erogati in misura crescente servizi essenziali per la collettività e strategici per il Paese. In ambito europeo la cosiddetta direttiva NIS del 6 luglio 2016 ha previsto una serie di disposizioni volte a favorire 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 18 maggio 2018, che – nel definire l'architettura strategica nazionale in materia di sicurezza cibernetica – ha individuato i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. Successivamente, il decreto-legge n. 105 del 2019 ha istituito il richiamato « perimetro di sicurezza nazionale cibernetica » e previsto misure volte a garantire i necessari *standard* di sicurezza nonché disposizioni per un procurement più sicuro di prodotti, processi e servizi ICT destinati alle suddette infrastrutture. L'attuazione della normativa sul perimetro di sicurezza è demandata, con scadenze temporali diversificate, a quattro decreti del Presidente del Consiglio dei ministri e ad un regolamento. Lo schema di decreto in esame è quello a scadenza più ravvicinata. Esso è volto a dare attuazione a due previsioni del decreto-legge n. 105 del 2019. In particolare – in esecuzione di quanto disposto dall'articolo 1, comma 2, lettera *a*) – definisce 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. In attuazione di quanto disposto, invece, dalla lettera *b*) stabilisce i criteri con i quali i soggetti inclusi nel perimetro sono tenuti a predisporre e aggiornare l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. Da un punto di vista procedurale lo schema in esame è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), tra i cui membri vi è anche un rappresentante del Ministero della difesa. Sul testo è stato acquisito il parere del Consiglio di Stato reso nella adunanza della Sezione consultiva per gli atti normativi del 21 maggio 2020. A loro volta, le competenti Commissioni parlamentari sono chiamate ad esprimere il proprio parere entro il 4 luglio 2020. A tal proposito ricorda che la necessità di sottoporre a parere parlamentare lo schema di decreto in esame era stata espressamente richiesta da questa Commissione lo scorso 22 ottobre, in sede di espressione del parere sul decreto-legge n. 105 del 2019. Tale condizione era stata successivamente recepita dalle Commissioni affari costituzionali e trasporti nel corso dell'esame in sede referente del decreto-legge. Ricorda, invece, che la puntuale elencazione dei soggetti inclusi nel « perimetro » è rimessa ad un « atto amministrativo » non soggetto a pubblicazione e rispetto al quale è espressamente escluso il diritto di accesso. Al riguardo, fa presente che tale regime giuridico non era originariamente contemplato dal decreto-legge n. 105 del

2019 che, viceversa, affidava al Decreto del Presidente del Consiglio dei ministri anche l'individuazione dei soggetti inclusi nel « perimetro ». La scelta di non pubblicizzare il provvedimento recante la puntuale individuazione dei soggetti facenti parte del « perimetro » è da collegare, quindi, ad una successiva novella legislativa disposta dall'articolo 27 del decreto-legge n. 162 del 2019 e motivata dal Governo alla luce di particolari profili di sensibilità del richiamato elenco, sotto il profilo della sicurezza nazionale. Da un punto di vista sistematico lo schema di decreto, che si compone complessivamente di 12 articoli, è suddiviso in quattro Capi, di cui il Capo II e il Capo III dedicati, rispettivamente, alla definizione delle « Modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, ed alla definizione dei « Criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e di servizi informatici ». Il Capo I e il Capo IV sono invece dedicati, rispettivamente, all'individuazione delle « Definizioni e criteri generali » ed alla definizione delle « Disposizioni sulla tutela delle informazioni, transitorie e finali ». Nel dettaglio, l'articolo 1 contiene le definizioni impiegate nel testo dello schema. A loro volta gli articoli 2 e 3 contribuiscono a delineare le modalità per l'individuazione dei soggetti inclusi nel perimetro oggetto del successivo Capo II. In particolare, l'articolo 2 fornisce le definizioni di funzione e servizio essenziale, concetti questi introdotti dal decreto-legge n. 105 del 2019, il quale all'articolo 1, comma 2, lett. *a*), oltre a demandare al Decreto del Presidente del Consiglio dei ministri l'adozione puntuale delle modalità e criteri procedurali per l'individuazione dei soggetti del perimetro *cyber*, definisce direttamente alcuni di questi criteri. In particolare stabilisce che, ai fini dell'individuazione, 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. Sulla base di tale indicazione legislativa l'articolo 2, lettera *a*) dello schema provvede a definire il concetto di funzione essenziale prevedendo che si verifichi tale circostanza quando l'ordinamento attribuisce ad un soggetto compiti rivolti ad 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. A sua volta l'articolo 2, lettera *b*), definisce il concetto di servizio essenziale in connessione con lo svolgimento di una serie tassativa di attività descritte dalla richiamata lettera e tra le quali rilevano, in particolare, le attività strumentali all'esercizio di funzioni essenziali dello Stato. Con riferimento poi all'individuazione dei settori di attività in cui operano i soggetti da inserire nel perimetro di sicurezza cibernetica, l'articolo 3, comma 1, reca un elenco di settori prioritari tra i quali è ricompreso espressamente quello della difesa. Per quanto concerne, poi le modalità di individuazione dei soggetti inclusi nel perimetro di sicurezza cibernetica, l'articolo 4, dispone che spetti alle amministrazioni competenti: identificare le funzioni e i servizi essenziali 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 amministrazioni valutano, quanto agli effetti di una interruzione della funzione o servizio essenziale, l'estensione territoriale, il numero e la tipologia di utenti potenzialmente interessati, i livelli di servizio garantiti e le possibili ricadute economiche. Per quanto riguarda, invece, gli effetti della compromissione dello svolgimento della funzione o servizio essenziale, le competenti amministrazioni valutano le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati, tenendo

conto della loro tipologia, quantità e sensibilità e dello scopo cui sono destinati. In ultimo, le amministrazioni valutano la possibile mitigazione, in relazione al tempo necessario per ripristinare lo svolgimento in condizioni di sicurezza e alla possibilità che la funzione o il servizio essenziale possano o meno essere assicurati, anche temporaneamente, con modalità prive di supporto informatizzato ovvero anche parzialmente da altri soggetti. Le competenti 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. Infine, individuano i soggetti che svolgono le funzioni o servizi essenziali citati. Inoltre, 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. Per quanto riguarda il nostro settore, come prima ricordato, tale attività è svolta dal Ministero della Difesa. A sua volta, 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'elenco dei soggetti è formalizzato in un decreto del Presidente del Consiglio dei ministri, di natura non regolamentare, adottato e aggiornato su proposta del CISR. 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 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.). L'articolo 6 dispone l'istituzione di un Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR. Il Tavolo è presieduto da un vice direttore del DIS ed è composto da due rappresentanti di ciascuna amministrazione CISR e un rappresentante per ciascuna delle due agenzie di informazioni. Il Tavolo, che si riunisce periodicamente e comunque almeno una volta ogni 6 mesi, 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. L'articolo 7 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. Per quanto riguarda il concetto di « bene ICT'', 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 una nozione funzionale. Gli elenchi dei beni ICT vengono aggiornati con cadenza almeno annuale. L'articolo 8 prevede che l'architettura e la componentistica relative ai richiamati 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, mentre l'articolo 9 prevede i tempi e le procedure per la trasmissione degli elenchi dei beni ICT. L'articolo 10 reca disposizioni per la tutela delle informazioni. A tal proposito, si prevede che l'elenco dei soggetti inclusi nel perimetro nazionale 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 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 3 agosto 2007, n. 124. L'articolo 11 reca le disposizioni transitorie, mentre l'articolo 12 contiene, infine, la clausola di invarianza finanziaria. Tutto ciò considerato, si riserva di avanzare, nella prossima seduta, una proposta di parere favorevole, dichiarandosi disponibile ad ascoltare opinioni e suggerimenti dei colleghi.

Il sottosegretario Angelo TOFALO si riserva di intervenire in sede di replica.

Roger DE MENECH, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 13.