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

Informazioni sugli atti di riferimento

A.C.	2100
Titolo:	Conversione in legge del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
Iniziativa:	Governativa
Iter al Senato:	Sì
Commissioni competenti:	I Affari costituzionali, IX Trasporti
Sede:	referente

Contenuto

L'articolo 1 rimette, al comma 2, a un DPCM l'individuazione dei soggetti da includere nel perimetro di sicurezza nazionale cibernetica istituito dal comma 1. Tra tali soggetti possono rientrare amministrazioni pubbliche (quindi sia amministrazioni statali che regionali e locali) ed enti e operatori nazionali, pubblici e privati, le cui reti e sistemi informativi e informatici sono necessari per l'esercizio di una funzione essenziale dello Stato ovvero 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 – anche parziali – o uso improprio possono pregiudicare la sicurezza nazionale. Il DPCM sarà adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica entro quattro mesi dalla data di entrata della legge di conversione del decreto in esame. 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 rilevanti. Tale elenco dovrà essere aggiornato con cadenza almeno annuale.

Il successivo comma 3 demanda invece ad un ulteriore DPCM la determinazione di un duplice profilo: le procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro e le misure di sicurezza. Tra le misure di sicurezza merita segnalare le politiche di mitigazione e gestione degli incidenti e loro prevenzione; la protezione fisica e logica dei dati informativi; l'integrità delle reti e dei sistemi informativi.

Il comma 6 dell'articolo 1 rimette invece ad un regolamento di esecuzione, da emanarsi entro 10 mesi dalla data di entrata in vigore del decreto-legge la definizione delle procedure, delle modalità e dei termini ai quali devono attenersi i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

Il comma 7 dell'articolo 1 individua, nell'ambito delle politiche di sicurezza cibernetica, alcuni compiti che il Centro di valutazione e certificazione nazionale (CVCN), già istituito dal decreto del Ministro dello sviluppo economico del 15 febbraio 2019. Tra tali compiti merita segnalare la partecipazione all'elaborazione delle misure di sicurezza; lo svolgimento di attività di valutazione del rischio; l'elaborazione di schemi di certificazione cibernetica.

I commi da 9 a 11 dell'articolo 1 stabiliscono infine un articolato sistema sanzionatorio, mentre il comma 12 individua nella Presidenza del Consiglio l'autorità competente all'accertamento e all'irrogazione delle sanzioni pecuniarie amministrative.

L'articolo 2 autorizza il Ministero dello sviluppo economico ad assumere a tempo indeterminato, con incremento della vigente dotazione organica nel limite delle unità eccedenti, in aggiunta alle ordinarie facoltà assunzionali, un contingente massimo di 77 unità di personale per lo svolgimento delle funzioni del Centro di valutazione e certificazione nazionale (CVCN), prevedendo che il Ministero, fino al completamento delle procedure di assunzione, possa avvalersi, a tale scopo, di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni; autorizza, inoltre, la Presidenza del Consiglio ad assumere fino a dieci unità di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione, avvalendosi, nelle more di tali assunzioni, di esperti o di personale di altre amministrazioni pubbliche.

L'articolo 3 detta disposizioni di raccordo tra il decreto in commento e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla tecnologia 5G.

L'articolo 4 estende l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori ad alta intensità tecnologica (cd. *golden power*), contenute nel decreto legge n. 21 del 2012. Tra le altre cose, si chiarisce che, in seno alla verifica sulla sussistenza di un pericolo per la sicurezza e l'ordine pubblico, è compreso anche il possibile pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti.

L'articolo 5 dispone circa alcune attribuzioni emergenziali in capo alla Presidenza del Consiglio, in caso di rischio grave o crisi di natura cibernetica. In particolare, si prevede che il Presidente del Consiglio - su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) - possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi posti nel perimetro di sicurezza nazionale cibernetica

L'articolo 6 dispone in merito alla copertura finanziaria del provvedimento.

Per ulteriori elementi si rinvia al dossier-schede di lettura n. 203 sul provvedimento.

Profili attinenti al riparto di competenze tra Stato e regioni

Il contenuto del provvedimento appare riconducibile alla materia della *sicurezza dello Stato* di **esclusiva competenza statale** (art. 117, secondo comma, lettera *d* Cost.).

Senato: Nota breve n. 136
Camera: Nota Questioni regionali n. 61
7 ottobre 2019

Camera	Servizio Studi Osservatorio sulla legislazione	osservatorio@camera.it - 066760-3855	CD_legislazione