Camera dei deputati
Servizio Studi
XVIII Legislatura

PROVVEDIMENTO D.L. 105/2019: perimetro di sicurezza cibernetica

11 novembre 2019

Il decreto-legge 21 settembre 2019, n. 105, recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica" (ultima parte aggiunta nel corso del'esame parlamentare) è stato esaminato dalla Camera dei deputati in prima lettura (C. 2100) e trasmesso al Senato della Repubblica, con modificazioni, il 24 ottobre 2019 **(**S. 1570**)**.

Nel corso dell'esame al Senato sono state apportate ulteriori modificazioni rispetto al testo approvato dalla Camera (C. 2100-B, trasmesso alla Camera l'8 novembre 2019). In particolare, sono state oggetto di modifica le disposizioni di cui all'articolo 1, commi 6 e 7, 9 e 19 e di cui all'articolo 6, comma 1 del decreto-legge.

Tali modifiche hanno riguardato, in particolare, l'istituzione di un Centro di valutazione (CEVA) presso il Ministero dell'interno e i conseguenti adeguamenti nel testo, compresa la copertura finanziaria per la realizzazione, l'allestimento e il funzionamento del Centro.

È stato altresì specificato che l'istituendo Centro di valutazione del Ministero dell'interno, così come quello del Ministero della difesa, siano accreditati presso il Centro di Valutazione e certificazione nazionale (CVCN) e sono tenuti ad impiegare metodologie di verifica e test quali definiti dal medesimo CVCN. Con DPCM saranno inoltre definiti gli obblighi di informativa di tali Centri con il CVCN.

Ulteriori modifiche hanno riguardato specifiche previsioni del testo.

Il perimetro di sicurezza nazionale cibernetica

Il decreto-legge n. 105 del 2019 è finalizzato ad 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.

Nel corso dell'esame in prima lettura alla Camera, oltre alle modifiche apportate al testo del decreto-legge, sono state previste nuove disposizioni per l'esercizio dei poteri speciali del Governo.

Più nel dettaglio, l'istituzione del perimetro di sicurezza nazionale cibernetica, 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, è demandata ad un **DPCM**, da adottare su proposta del CISR (Comitato interministeriale per la sicurezza della Repubblica), previo parere delle competenti Commissioni parlamentari, **entro 4 mesi** dall'entrata in vigore della legge di conversione.

Entro 10 mesi dall'entrata in vigore della legge di conversione spetta ad un DPCM - da adottare su proposta del CISR, previo parere delle competenti Commissioni parlamentari - la determinazione delle **procedure di notifica** degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica e le **misure di sicurezza**.

I suddetti DPCM sono aggiornati – con cadenza almeno biennale – con la medesima proceduta prevista per la loro adozione.

È infine rimessa 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 - 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.

Si tratta, in particolare, dei beni appartenenti a categorie individuate da un decreto del Presidente del Consiglio dei ministri sulla base di criteri tecnici che dovrà essere emanato **entro 10 mesi** dall'entrata in vigore della norma di conversione del decreto.

Sono poi individuati 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 (ICT) e associate infrastrutture - qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica.

Al contempo sono determinati 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, inclusi nel perimetro di sicurezza nazionale cibernetica.

È altresì previsto 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 interessati. Entro 30 giorni il Presidente del Consiglio è tenuto a informare il Comitato parlamentare per la sicurezza della Repubblica (Copasir) delle misure disposte.

Al Presidente del Consiglio dei ministri è affidato inoltre il coordinamento della coerente attuazione delle disposizioni del decreto-legge che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del DIS che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni e con i soggetti coinvolti. Il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte dopo l'adozione degli atti normativi secondari previsti dall'art. 1 per l'attuazione delle misure ivi stabilite.

E' disposta l'istituzione di un Centro di valutazione (CEVA) presso il Ministero dell'interno il quale, come quello del Ministero della difesa, sono accreditati presso il Centro di Valutazione e certificazione nazionale (CVCN) e sono tenuti ad impiegare metodologie di verifica e test quali definiti dal medesimo CVCN. Con DPCM saranno inoltre definiti gli obblighi di informativa di tali Centri con il CVCN.

Il provvedimento reca quindi un articolato **sistema sanzionatorio** per i casi di violazione degli obblighi ivi previsti ed individua le **autorità competenti** all'accertamento delle violazioni e all'irrogazione delle **sanzioni.** Le autorità titolari delle attribuzioni quali configurate dal decreto-legge, sono chiamate inoltre ad assicurare "gli opportuni raccordi" con il Dipartimento delle informazioni per la sicurezza (DIS) e con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Parallelamente è autorizzata l'assunzione a **tempo indeterminato** di un contingente massimo di **77 unità di personale**, di cui 67 di area terza e 10 di area seconda, tenuto conto dell'esigenza di disporre di personale in possesso della professionalità necessaria per lo svolgimento delle funzioni del Centro di valutazione e certificazione nazionale (CVCN). A sua volta, la Presidenza del Consiglio è autorizzata ad assumere fino a **10 unità** di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione. Il suddetto reclutamento del personale avviene attraverso l'espletamento di uno o più **concorsi pubblici**.

Alcune disposizioni sono dettate per assicurare il raccordo tra il decreto-legge e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla **tecnologia 5G**.

È inoltre esteso l'ambito operativo delle norme in tema di poteri speciali esercitabili dal Governo nei settori ad alta intensità tecnologica (cd. ***golden power***).

Nuove norme sono, al contempo, dettate in materia di esercizio di poteri speciali da parte del Governo. Il nuovo articolo 4-bis infatti, riprendendo ed integrando le previsioni del decreto-legge n. 64 del 2019, non convertito in legge, modifica il decreto legge n. 21 del 2012 in tema di **poteri speciali del Governo** nei settori della difesa e della sicurezza nazionale, nonché per le **attività di rilevanza strategica** nei settori dell'energia, dei trasporti e delle comunicazioni (cd. ***golden power***).

Sono in particolare previste le seguenti modifiche:

- viene in generale allungato il termine per l'esercizio dei poteri speciali da parte del Governo, con contestuale arricchimento dell'informativa resa dalle imprese detentrici degli *asset* strategici;
- si amplia l'oggetto di alcuni poteri speciali;
- sono modificati e integrati gli obblighi di notifica finalizzati all'esercizio dei poteri speciali;

- viene modificata la disciplina dei poteri speciali in tema di tecnologie 5G, per rendere il procedimento sostanzialmente simmetrico rispetto a quello per l'esercizio dei poteri speciali nei settori della difesa e della sicurezza nazionale;
- viene ridefinito il concetto di "soggetto esterno all'Unione europea" e sono precisati i criteri per determinare se un investimento estero è suscettibile di incidere sulla sicurezza o sull'ordine pubblico.

Dossier

Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
https://temi.camera.it/dossier/OCD18-12945/disposizioni-urgenti-materia-perimetro-sicurezza-nazionale-cibernetica-13.html