dossier

30 settembre 2019

Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

D.L. 105/2019 – A.C. 2100

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

SERVIZIO STUDI
Ufficio ricerche su questioni istituzionali, giustizia e cultura
TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier n. 166

Camera dei deputati

SERVIZIO STUDI
Dipartimento istituzioni
Tel. 066760-3855 st_istituzioni@camera.it - @CD_istituzioni

Dipartimento trasporti
Tel. 066760-2614 st_trasporti@camera.it - @CD_trasporti

Progetti di legge n. 203

D19105.docx

INDICE

SCHEDE DI LETTURA

Schede di lettura

Articolo 1, commi 1 e 2
(Istituzione del perimetro di sicurezza nazionale cibernetica)

L'**articolo 1**, **comma 1**, istituisce il **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.

Il **comma 2** demanda ad un **DPCM** l'individuazione dei **soggetti inclusi nel perimetro** di sicurezza nazionale cibernetica. Il DPCM fa parte del novero di atti, tre DPCM e un regolamento governativo, complessivamente, previsti per l'attuazione del decreto-legge in esame.

In particolare, il **comma 1** fa riferimento ad **amministrazioni pubbliche**, nonché ad **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**;
- sono necessari per l'assolvimento di un **servizio essenziale** per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
- il cui malfunzionamento, interruzione – anche parziali - 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 in esame.

Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è un organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza. In particolare il Comitato: delibera sulla ripartizione delle risorse finanziarie e sui bilanci preventivi e consuntivi di DIS (Dipartimento delle informazioni per la sicurezza), AISE (Agenzia informazioni e sicurezza esterna) e AISI (Agenzia informazioni e sicurezza interna); indica il fabbisogno informativo necessario ai ministri per svolgere l'attività di governo. Sono membri del CISR: il Presidente del Consiglio dei ministri; l'Autorità delegata; il Ministro degli affari esteri; il Ministro dell'interno; il Ministro della difesa; il Ministro della giustizia; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico.

Al Direttore generale del DIS sono assegnate le funzioni di segretario del Comitato.

Il decreto legislativo 18 maggio 2018, n. 65, pone le 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 (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. In particolare, al **Presidente del Consiglio dei ministri** compete l'adozione - sentito il **Comitato interministeriale per la sicurezza della Repubblica (CISR) -** della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

Il decreto legislativo n. 65 del 2018, tra l'altro, definisce la "sicurezza della rete e dei sistemi informativi", in corrispondenza con la direttiva europea, quale capacità "di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi" (art. 3, comma 1, lett. *f)*). È altresì definita la nozione di **autorità competente NIS**, quale autorità competente per settore in materia di sicurezza delle reti e dei sistemi informativi. L'articolo 7, comma l, del decreto legislativo attribuisce ai **singoli ministeri** in base agli ambiti di competenza (Ministero dello sviluppo economico, Ministero delle infrastrutture e dei trasporti, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio) e, per taluni ambiti, alle **regioni e province autonome**.

Gli **operatori di servizi essenziali**, ai fini del decreto legislativo n. 65, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS. E' prescritto che, le autorità competenti NIS (quindi i ministeri competenti) identifichino con propri provvedimenti, per ciascun settore e sotto-settore, gli operatori con sede nel territorio nazionale, secondo i seguenti criteri e tenuto conto dei documenti prodotti al riguardo dal Gruppo di cooperazione: un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o o economiche fondamentali; la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Il decreto del Presidente del Consiglio dei ministri **individua i soggetti inclusi nel perimetro** secondo i seguenti criteri (**comma 2, lettera *a)*** dell'articolo in esame):

- il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività

civili, sociali o economiche fondamentali per gli interessi dello Stato;

- l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici il cui malfunzionamento, interruzione o esercizio improprio può costituire un pericolo per la sicurezza nazionale.

Resta ferma, per gli **organismi di informazione e sicurezza**, la specifica disciplina di cui alla legge 3 agosto 2007, n. 124 (recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto").

La legge n. 124 del 2007 stabilisce che il Sistema di informazione per la sicurezza della Repubblica è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità delegata (Ministro senza portafoglio o Sottosegretario di Stato) ove istituita, dal Dipartimento delle informazioni per la sicurezza (DIS), dall'Agenzia informazioni e sicurezza esterna (AISE) e dall'Agenzia informazioni e sicurezza interna (AISI).

Il decreto legislativo n. 65 del 2018 (art. 3, comma 1, lett. *e*) definisce la nozione “rete e sistema informativo”, in corrispondenza con la direttiva europea, nel modo seguente:

1) una rete di comunicazione elettronica riconducibile a "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 (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), 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 trasportato" (la disposizione rinvia all'articolo 1, comma 1, lettera *dd),* del decreto legislativo n. 259 del 2003);

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;

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.

Il medesimo DPCM (**lettera *b***) dovrà fissare i criteri che i soggetti inclusi nel perimetro dovranno seguire nel compilare **l'elenco delle reti, dei sistemi e dei servizi** (comprensivo dell'architettura e della componentistica) rilevanti ai fini della presente disciplina. Tale elenco dovrà essere aggiornato con cadenza almeno annuale.

L'organismo tecnico di supporto al CISR, integrato da un rappresentante della Presidenza del Consiglio dei ministri, collabora nella predisposizione di tali criteri, adottando "opportuni moduli organizzativi".

Il "**CISR Tecnico**" (disciplinato dall'art. 5 del DPCM 17 febbraio 2017) opera, a supporto del CISR, quale organismo collegiale permanente di coordinamento, presieduto dal Direttore Generale del DIS e composto dai Direttori di AISE ed AISI, oltre che dai Dirigenti di Vertice dei "ministeri CISR" (Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico).

Entro sei mesi dall'entrata in vigore del DPCM di cui qui si tratta, gli **elenchi così predisposti sono inviati**:

- alla Presidenza del Consiglio dei ministri dai soggetti pubblici;
- sempre alla Presidenza del Consiglio dei ministri 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, rispettivamente qualificati ovvero accreditati dall'AgID (si tratta dei soggetti individuati dall'art. 29 del Codice dell'amministrazione digitale, di cui al decreto legislativo n. 82 del 2005);
- 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 **DIS**, Dipartimento delle informazioni per la sicurezza, organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea e designato, dall'art. 7 del decreto legislativo n. 65 del 2018, quale **punto di contatto unico** per tali questioni, anche per le attività di prevenzione, preparazione e gestioni delle crisi svolte dal Nucleo per la sicurezza cibernetica;
- all'**organo per la regolarità e sicurezza dei servizi di telecomunicazione presso il Ministero dell'interno** il quale assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno 9 gennaio 2008, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate (art. 7-

bis del decreto-legge n. 144 del 2005, recante " Misure urgenti per il contrasto del terrorismo internazionale").

Il **Nucleo per la sicurezza cibernetica** (NSC) è stato introdotto dal DPCM 24 gennaio 2013 a supporto del Presidente del Consiglio dei ministri, per gli aspetti relativi alla prevenzione e all'approntamento rispetto a situazioni di crisi. Il DPCM 17 febbraio 2017, art. 7, ha previsto la sua collocazione istituzionale presso il DIS in via permanente. Ai sensi del medesimo articolo 7, il Nucleo è presieduto da un vice direttore generale del DIS, designato dal direttore generale, ed è composto dal Consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Per gli aspetti relativi alla trattazione di informazioni classificate, il Nucleo è integrato da un rappresentante dell'ufficio centrale per la segretezza di cui all'art. 9, della legge n. 124 del 2007.

Ai sensi del **comma 5** dell'articolo 1 del decreto-legge in esame, si procede ad un **aggiornamento almeno biennale** di quanto previsto dal decreto di cui al comma 2, con ulteriori decreti adottati con le stesse modalità qui previste.

Per ulteriori approfondimenti sull'evoluzione della normativa nazionale e dell'Unione europea in materia sicurezza cibernetica si veda il *dossier* del Servizio studi, Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber, 24 settembre 2019.

A livello di **Unione europea** la direttiva (UE) 2016/1148 del 6 luglio 2016 reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. **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 18 maggio 2018, n. 65**. Esso detta 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 2016/1148.

In particolare, al **Presidente del Consiglio dei ministri** compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (**CISR**), della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la

medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

La qualifica di "**autorità competente NIS**" viene attribuita ai singoli ministeri in base ai settori di competenza (Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio) e, per taluni ambiti, alle regioni e alle province autonome di Trento e di Bolzano. Tali autorità sono i soggetti competenti per settore (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) in materia di sicurezza delle reti e dei sistemi informativi; verificano, in particolare, l'applicazione della direttiva a livello nazionale ed individuano gli operatori di servizi essenziali nell'ambito dei criteri ivi definiti.

Presso la Presidenza del Consiglio dei ministri è istituito il **CSIRT**-*Computer Emergency Response Team* italiano, al quale sono attribuite le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

Viene designato il Dipartimento delle informazioni per la sicurezza (DIS) quale **punto di contatto unico**, organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea.

L'**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione al quale è attualmente attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Gli **operatori di servizi essenziali**, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS. Entro il 9 novembre 2018 le autorità competenti sono tenute ad identificare tali soggetti, ai fini del rispetto degli obblighi della direttiva.

Il decreto definisce inoltre gli obblighi in capo agli **operatori dei servizi essenziali e ai fornitori dei servizi digitali** con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III. È posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e, sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano

un impatto rilevante sui servizi forniti individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi.

Sono poi individuati i **poteri di controllo** delle autorità NIS sia nei confronti degli operatori di servizi essenziali, che dei fornitori di servizi digitali anche prevedendo poteri di verifica e di ispezione oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti.

Nel mese di luglio 2019 **le linee guida** sulla gestione dei rischi e la prevenzione, mitigazione e notifica degli incidenti, elaborate dalle Autorità NIS, sono state adottate e condivise con i 465 operatori di servizi essenziali (OSE) già individuati nel dicembre 2018 (si veda, al riguardo, il comunicato stampa del 3 luglio 2019 del Dipartimento delle informazioni per la sicurezza - DIS e la scheda sul sito "Agenda digitale").

Il decreto del Ministro dello sviluppo economico 12 dicembre 2018, in attuazione degli articoli 16-*bis* e 16-*ter* del decreto legislativo n. 259 del 2003, ha dettato misure di natura tecnico-organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza adeguato al rischio esistente e ha definito **i casi in cui la violazione delle reti o la perdita dell'integrità sono da considerarsi significative**, ai fini della notifica alle Autorità competenti da parte dei fornitori di reti e servizi.

Il decreto del Ministro dello sviluppo economico 15 febbraio 2019, in attuazione del DPCM 12 febbraio 2017, ha istituito il **Centro di Valutazione e Certificazione nazionale (CVCN)**, presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

Può valere ricordare altresì come il decreto legge 25 marzo 2019, n. 22 (in materia di *'Brexit'*) abbia recato (all'art. 1, comma 1) modifiche alla disciplina sui **poteri speciali** inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G, di cui al decreto-legge 15 marzo 2012, n. 21.

Sulla materia dei poteri speciali esercitabili dal Governo per la salvaguardia degli assetti proprietari delle società operanti in settori reputati strategici e di interesse nazionale è successivamente intervenuto il decreto-legge 11 luglio 2019, n. 64, non convertito in legge.

Si rammenta inoltre che il Regolamento (CE) n. 2019/452/UE istitutivo di un quadro per il controllo degli investimenti esteri diretti nell'Unione, stabilisce (art. 4) che gli Stati membri dell'UE, nel determinare se un investimento estero diretto possa incidere sulla sicurezza o sull'ordine

pubblico, devono prendere in considerazione, tra l'altro, fattori quali le infrastrutture critiche (fisiche e visuali) e le tecnologie critiche, (tra cui l'intelligenza artificiale, la robotica, la cibersicurezza ecc.).

Si veda anche la scheda sull'articolo 4 del decreto-legge in esame.

Il 1° agosto 2019, il Governo allora in carica ha presentato al Senato il disegno di legge recante "Disposizioni in materia di perimetro di sicurezza nazionale cibernetica" (A.S. n. 1448), assegnato alla 1ª Commissione permanente (Affari Costituzionali) in sede redigente il 7 agosto 2019. L'esame del disegno di legge non è stato avviato. Il decreto-legge in conversione qui in esame ne riprende, in parte mutati tuttavia, i contenuti.

Articolo 1, commi 3-5
(Procedure di segnalazione degli incidenti e misure di sicurezza)

L'**articolo 1**, **comma 3** demanda ad un DPCM la determinazione di un duplice profilo: le procedure di notifica degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica; le misure di sicurezza.

Il **comma 4** determina i soggetti ministeriali preposti all'elaborazione delle misure di sicurezza.

Il **comma 5** prevede l'aggiornamento - almeno biennale - di quanto previsto dal menzionato DPCM.

In particolare, il **comma 3** demanda ad un DPCM - da adottare **entro dieci mesi** dalla conversione del decreto legge - la definizione di un duplice profilo:

- le **procedure** secondo cui i soggetti del perimetro di sicurezza nazionale cibernetica segnalino gli **incidenti** aventi impatto su reti, sistemi informativi e sistemi informatici (**lett. *a***);
- le **misure** volte a garantirne elevati livelli di **sicurezza** (**lett. *b***).

Per quanto riguarda le **procedure di segnalazione** - di cui alla **lettera *a)*** - **degli incidenti su reti, sistemi informativi e sistemi informatici** rientranti nel perimetro di sicurezza nazionale cibernetica, i relativi soggetti (amministrazioni pubbliche, nonché enti oppure operatori nazionali, pubblici e privati) devono notificare l'incidente al **Gruppo di intervento per la sicurezza informatica in caso di incidente** (CSIRT) italiano.

Il CSIRT procede poi a inoltrare tempestivamente tali notifiche al **Dipartimento delle informazioni della sicurezza (DIS)**.

La trasmissione è prevista anche qualora siano interessate attività demandate al Nucleo per la sicurezza cibernetica.

Il medesimo DIS assicura indi una duplice ulteriore trasmissione:

- all'organo del Ministero dell'interno preposto alla sicurezza e regolarità dei servizi di telecomunicazioni;
- alla Presidenza del Consiglio dei ministri (se le notifiche degli incidenti giungano da un soggetto pubblico - o da un soggetto fornitore di servizi fiduciari qualificati o svolgente l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, ai sensi dell'art. 29 del Codice dell'amministrazione digitale, decreto legislativo n. 82 del 2005) ovvero al Ministero

dello sviluppo economico (se le notifiche giungano da un soggetto privato del perimetro di sicurezza nazionale cibernetica).

Per quanto riguarda le **misure di sicurezza** - di cui alla **lettera *b)*** - 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 sì da agire su più versanti:

- politiche di sicurezza, struttura organizzativa e gestione del rischio;
- mitigazione e gestione degli incidenti e loro prevenzione (anche attraverso la sostituzione di apparati o prodotti che risultino "gravemente inadeguati" sul piano della sicurezza);
- protezione fisica e logica e dei dati informativi;
- integrità delle reti e dei sistemi informativi;
- gestione operativa (compresa la continuità del servizio);
- monitoraggio, test e controllo;
- formazione e consapevolezza;
- affidamento di forniture, sistemi e servizi di tecnologie dell'informazione e della comunicazione (ICT nell'acronimo inglese: *Information and Communication Technology*).

L'**elaborazione delle misure** di sicurezza sopra menzionate è realizzata, secondo l'ambito di propria competenza, dal Ministero per lo sviluppo economico e dalla Presidenza del Consiglio. È prevista l'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e finanze, il Dipartimento delle informazioni per la sicurezza **(comma 4**).

Il **comma 5** prevede un **aggiornamento almeno biennale** delle previsioni del DPCM di cui qui si tratta - dunque di determinazione (ai sensi del comma 3) delle misure di sicurezza nonché delle procedure di segnalazione degli incidenti.

Medesimo aggiornamento almeno biennale è del pari previsto per l'altro DPCM, di determinazione (ai sensi del comma 2) dei soggetti, reti e sistemi facenti parte del perimetro di sicurezza nazionale cibernetica.

Il comma 3 sopra ricordato menziona alcuni soggetti istituzionali in ambito di sicurezza.

Il **Gruppo di intervento per la sicurezza informatica in caso di incidente** (CSIRT: acronimo per *Computer Security Incident Response Team*) è stato definito dalla direttiva dell'Unione europea n. 1148 del 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

Secondo quella direttiva (art. 9), ogni Stato membro è chiamato a designare un "Gruppo di intervento per la sicurezza informatica in caso di incidente", con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

Attuazione alla direttiva è stata data con il decreto legislativo n. 65 del 2018.

Il suo articolo 8 istituisce, a tal fine, presso la **Presidenza del Consiglio dei ministri** un nuovo organismo, il **CSIRT italiano**, al quale sono attribuite funzioni innanzi spettanti al CERT nazionale (acronimo per *Computer Emergency Response Team*, presso il Ministero per lo sviluppo economico) e del CERT-PA (presso l'Agenzia per l'Italia digitale-AGID), con altresì specificatamente attribuite 30 unità di personale.

Le funzioni attribuite al CSIRT italiano sono definite rinviando in gran parte ai requisiti indicati all'Allegato I del medesimo decreto legislativo n. 65.

Tale Allegato individua infatti i requisiti per il CSIRT (punto 1) e i relativi compiti (punto 2), riprendendo testualmente l'Allegato I della direttiva (UE) 2016/1148, che detta i requisiti e i compiti dei CSIRT.

I *requisiti*, di cui il CSIRT è chiamato ad assicurare la conformità, prevedono:

- che sia garantito un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione devono essere chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano;
- i locali del CSIRT e i sistemi informativi di supporto devono essere ubicati in siti sicuri;
- ai fini della continuità operativa, il CSIRT deve essere dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi; dispone di personale sufficiente per garantirne l'operatività 24 ore su 24; opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili "sistemi ridondanti e spazi di lavoro di *backup*".
- il CSIRT ha la possibilità, se lo ritiene, di partecipare a reti di cooperazione internazionale.

I *compiti* del CSIRT sono così definiti:

- monitoraggio degli incidenti a livello nazionale;
- emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- intervento in caso di incidente;
- analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;
- partecipazione alla rete dei CSIRT.

Il CSIRT è chiamato inoltre a stabilire relazioni di cooperazione con il settore privato.

Per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nelle procedure di trattamento degli incidenti e dei rischi e nei sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Il **Dipartimento delle informazioni della sicurezza** è stato istituito presso la Presidenza del Consiglio dei ministri dall'articolo 4 della legge n. 124 del 2007, per il coordinamento della programmazione e delle attività operative di Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni e sicurezza esterna (AISI).

La legge del 2007 è stata novellata dalla legge n. 133 del 2013, che ha inteso rafforzare, del Dipartimento, le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali.

Ulteriori previsioni concernenti il Dipartimento sono sopraggiunte con il DPCM 17 febbraio 2017, recante "**Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali"** (pubblicato nella G.U. del 13 aprile 2017)**.**

Il Nucleo per la sicurezza cibernetica è stato oggetto di disposizioni contenute nel citato DPCM 17 febbraio 2017 (artt. 8-10). Esso è stato traslato (dall'ufficio del Consigliere militare presso la Presidenza del Consiglio, com'era secondo il DPCM 24 gennaio 2013) presso il Dipartimento delle informazioni per la sicurezza, nella materia della sicurezza dello spazio cibernetico per gli aspetti relativi alla prevenzione, preparazione ad eventuali situazioni di crisi, attivazione delle procedure di allertamento.

Tra i suoi compiti figura quello di promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale.

Costituisce (ferme restando le competenze ministeriali) punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE, altre organizzazioni internazionali ed altri Stati.

Il Nucleo è presieduto da un vice direttore generale del Dipartimento delle informazioni per la sicurezza, designato dal direttore generale, ed è composto dal Consigliere militare e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9, della legge n. 124 del 2007.

Per la gestione delle crisi di natura cibernetica, la composizione del Nucleo è integrata, in ragione delle necessità, con un rappresentante del Ministero della salute, del Ministero delle infrastrutture e dei trasporti, del Dipartimento dei

Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile (CITDC), dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, degli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica, di altri soggetti eventualmente interessati.

Articolo 1, comma 6
(Procedure per l'acquisizione di sistemi ICT nel perimetro di sicurezza nazionale cibernetica)

L'**articolo 1**, **comma 6**, rimette ad un **regolamento** da emanarsi, con decreto del Presidente del Consiglio dei ministri, **entro 10 mesi** dalla data di entrata in vigore del decreto-legge**,** la definizione delle **procedure, delle modalità e dei termini** alle quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, ai sensi del decreto del Presidente del Consiglio dei ministri di cui al comma 2, 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** secondo quanto previsto dalla lettera *b)* del comma 2, diversi da quelli necessari per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati.

Secondo quanto previsto dall'ultimo periodo del comma 6, lettera a), per lo svolgimento delle attività di prevenzione, accertamento e di repressione dei reati e nei casi di deroga, sono utilizzati reti, sistemi informativi e servizi informatici conformi ai livelli di sicurezza di cui al comma 3, lettera *b)* dell'articolo 1, qualora non incompatibili con gli specifici impieghi cui essi sono destinati.

In particolare il **comma 6, lettera a**), stabilisce che i soggetti sopra indicati danno comunicazione al **Centro di valutazione e certificazione nazionale (CVCN)**, istituito presso l'ISCTI (Istituto Superiore della Comunicazioni e delle Tecnologie dell'Informazione) dal Ministro dello sviluppo economico, dell'**intendimento di provvedere all'affidamento di tali forniture**.

Il CVCN sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, **può**, entro trenta giorni, **imporre condizioni e test di *hardware* e *software***.

In tale ipotesi, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

Il citato decreto del Presidente del Consiglio dei ministri definisce inoltre i casi di deroga con riguardo alle forniture di beni e di servizi ICT per l'acquisto dei quali sia indispensabile procedere in sede estera.

Per le forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, sopra ricordati, il predetto Ministero procede, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal decreto-legge all'esame, attraverso un proprio Centro di valutazione in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza.

Il **comma 6, lettera *b)*** prevede che i fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici individuati **nell'elenco** che deve essere **trasmesso alla Presidenza del Consiglio dei ministri** e al **Ministero dello sviluppo economico** (secondo quanto previsto dalla lettera b) del comma 2), **assicurano** al CVCN e, limitatamente agli ambiti di specifica competenza, al Centro di valutazione operante presso il Ministero della difesa, **la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri**.

La mancata collaborazione da parte di tali soggetti è segnalata dal CVCN:

- al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati;
- alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero ai soggetti che forniscono servizi fiduciari qualificati o svolgono l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale (ai sensi dell'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82);

Il **comma 6, lettera *c),*** prevede che la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, secondo la ripartizione di competenza indicata nelle precedenti disposizioni, svolgano **attività di ispezione e verifica** in relazione a quanto previsto dal comma 2, lettera b), dal comma 3 e dalla lettera *a)* del comma 6 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 di cui al comma 2, lettera *b),* connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica 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, 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.

Tale attività è svolta, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica.

Il **comma 19** prevede l'autorizzazione di spesa per la copertura finanziaria relativa alla realizzazione, all'allestimento e al funzionamento del CVCN, di cui ai commi 6 e 7 (v. *infra*).

Articolo 1, commi 7 e 19
(Compiti del Centro di valutazione e certificazione nazionale)

L'**articolo 1, 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 (ICT) e associate infrastrutture - qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica.

Il Centro di valutazione e certificazione nazionale è stato istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019. Il centro è stato istituito presso l'Istituto Superiore delle comunicazioni e tecnologie dell'informazione. Il 19 aprile 2019 è stato firmato il decreto direttoriale che descrive il modello di funzionamento, l'organizzazione e il piano di sviluppo del CVCN, così come previsto dal richiamato decreto del Ministro dello sviluppo economico.
Per le assunzioni di personale si veda l'art. 2, commi 1 e 2.

In base al comma 7 il CVCN:

- contribuisce all'elaborazione delle misure di sicurezza, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT (lett. *a*);
- svolge attività di valutazione del rischio e di verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, dettando, se del caso, prescrizioni di utilizzo al committente (lett. *b*);
- elabora e adotta (previo conforme avviso dell'organismo tecnico di supporto al Comitato interministeriale per la sicurezza della Repubblica - CISR) schemi di certificazione cibernetica, qualora gli schemi di certificazione esistenti non siano ritenuti, per ragioni di sicurezza nazionale, adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica (lett. *c*).

Ai fini delle attività di cui alla lettera *b)*, il CVCN si avvale anche di laboratori che esso accredita.

I criteri per tale accreditamento sono da stabilirsi con DPCM entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto-legge.

Tale DPCM è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR).

Per le esigenze delle amministrazioni centrali dello Stato, sono impiegati i laboratori eventualmente istituiti presso le medesime amministrazioni, senza nuovi o maggiori oneri a carico della finanza pubblica.

Il **comma 19** prevede l'autorizzazione di spesa per la copertura finanziaria relativa alla realizzazione, all'allestimento e al funzionamento del CVCN di cui ai commi 6 e 7 (v. anche *supra*).

A tal fine, è autorizzata la spesa di **euro 3.200.000** per l'anno 2019 e di **euro 2.850.000** per ciascuno degli anni dal 2020 al 2023 e di euro **750.000** annui a decorrere dall'anno 2024.

A sua volta, l'art. 6 reca le norme di copertura finanziaria degli oneri di cui agli articoli 1, comma 19, e 2, commi 1 e 3, per complessivi euro 3.200.000 per l'anno 2019, euro 6.495.000 per ciascuno degli anni dal 2020 al 2023.

Per l'art. 2, il comma 1 (spesa previsto per le assunzioni di personale per lo svolgimento delle funzioni del CVCN) prevede che il limite di spesa è pari a 3.005.000 euro annui e il comma 3 (assunzioni presso la Presidenza del Consiglio) il limite di spesa è pari a 640.000 euro annui.

Articolo 1, comma 8
(Obblighi per alcuni specifici operatori)

L'**articolo 1, 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, inclusi nel perimetro di sicurezza nazionale cibernetica.

Per quanto riguarda la sicurezza, già le disposizioni vigenti pongono alcuni obblighi - di comunicazione; di adozione di misure tecniche ed organizzative - in capo a:

- gli operatori dei servizi essenziali (art. 12 del decreto legislativo n. 65 del 2018);
- i fornitori di servizi digitali (art. 14 del medesimo decreto legislativo n. 65 del 2018);
- le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (artt. 16-*bis* e 16-*ter*, comma 2, del decreto legislativo n. 259 del 2003, recante il codice delle comunicazioni elettroniche).

La disposizione qui in commento prevede - alla **lettera *a)*** - che tali soggetti - se inclusi nel perimetro di sicurezza nazionale cibernetica - osservino **le misure di sicurezza** quali previste dai predetti decreti legislativi, allorché esse siano "di livello almeno equivalente" a quelle adottate con l'apposito DPCM (v. *supra*, comma 3, lett. *b*) attuativo del presente decreto-legge.

Se tuttavia non vi sia equivalenza nel livello di sicurezza, le eventuali misure **aggiuntive** necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto-legge sono da definirsi:

- dalla Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli che forniscano servizi fiduciari qualificati o attività di gestore di posta elettronica certificata o di gestore dell'identità digitale o di conservatore di documenti informatici (di cui all'articolo 29 del decreto legislativo n. 82 del 2005, codice dell'amministrazione digitale,);
- dal Ministero dello sviluppo economico (che si avvale anche del Centro di valutazione e di certificazione nazionale - CVCN) per i soggetti privati.

La Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico (il quale è autorità NIS per il settore energia, sotto-settori

energia elettrica, gas e petrolio, e per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD[1], nonché per i servizi digitali) si raccordano, ove necessario, con le autorità NIS competenti.

Le autorità NIS competenti, di cui all'articolo 7 del decreto legislativo n. 65 del 2018 sono il Ministero delle infrastrutture e dei trasporti, per il settore trasporti, sotto-settori aereo, ferroviario, per vie d'acqua e su strada; il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob; il Ministero della salute per l'attività di assistenza sanitaria prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza; il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

La **lettera *b)*** del pari dispone in merito ad alcuni obblighi in capo ai soggetti sopra ricordati.

In particolare, dispone che essi assolvano l'obbligo di **notifica degli incidenti** aventi impatto su reti, sistemi informativi e sistemi informatici del perimetro di sicurezza nazionale cibernetica.

Con l'adempimento a tale obbligo si intende ottemperato l'obbligo di notifica già previsto dalle norme vigenti sopra ricordate (artt. 12 e 14 del decreto legislativo n. 65 del 2018; art. *16-ter* n. 259 del 2003).

La notifica degli incidenti è già soggetta ad una 'catena' di trasmissione tra autorità competenti in materia di sicurezza cibernetica, scandita dall'articolo 1, comma 3, lett. *a)* del presente decreto-legge. Quale ulteriore passaggio è previsto - per le notifiche provenienti dai soggetti oggetto del comma ora in commento (si è detto: operatori dei servizi essenziali; fornitori di servizi digitali; imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico) - che siffatte notifiche siano inoltrate dal Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT: v. *supra*, la scheda riferita all'articolo 1, comma 3 del decreto-legge) all'autorità NIS competente (oggetto del richiamato articolo 7 del decreto legislativo n. 65 del 2018: l'acronimo sta per *Network and Information Security*).

[1] Gli acronimi, rispettivamente, stanno per: *Internet Exchange Point*; *Domain Name Systems, Top-Level Domain*.

Articolo 1, commi 9-11
(Disposizioni sanzionatorie)

I commi da 9 a 11 recano un articolato **sistema sanzionatorio** per i casi di violazione degli obblighi previsti dal decreto-legge.

Più nel dettaglio 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 cui al comma 2 lett. b) (procedimento di compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici) e di cui al comma 6, lett. a) (procedimenti relativi all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi**)** o delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico, di cui al comma 6, lett. c):

- **forniscono informazioni**, dati o fatti **non rispondenti al vero** rilevanti per l'aggiornamento degli elenchi su ricordati o ai fini delle comunicazioni previste nei casi di affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, o per lo svolgimento delle attività ispettive e di vigilanza;
- **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**.

In proposito, si segnala l'opportunità di inserire tale reato nell'ampio catalogo di reati presupposto già contemplato dal decreto legislativo n. 231 del 2001.

Il **comma 9** disciplina una serie di **illeciti amministrativi**. Le sanzioni amministrative pecuniarie irrogate sono scaglionate in relazione alla gravità della condotta.

Più dettagliatamente è punito con la sanzione amministrativa pecuniaria:

- da 200.000 a 1.200.000 euro il mancato adempimento degli obblighi di predisposizione e di aggiornamento degli elenchi

delle reti, dei sistemi informativi e dei servizi informativi (**comma 9, lett. a**);

- da 250.000 a 1.500.000 euro:
  - il mancato adempimento dell'obbligo di notifica degli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici (**comma 9, lett. b)**);
  - 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 (**comma 9, lett. c**);
  - 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 (**comma 9, lett. f**);
  - 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 (**comma 9, lett. g**);
  - il mancato rispetto delle prescrizioni di utilizzo dettate dal CVCN (**comma 9, lett. h**);
- da 300.000 a 1.800.000 euro:
  - 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 (**comma 9, lett. d);**
  - 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* (**comma 9, lett. e**);

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.

Articolo 1, commi 12-14
(Accertamento delle violazioni e irrogazione delle sanzioni)

Il **comma 12** individua le **autorità competenti** all'accertamento delle violazioni e all'irrogazione delle **sanzioni** previste dai commi precedenti.

Si valuti l'opportunità di specificare che si fa riferimento alle sole sanzioni amministrative posto che evidentemente l'accertamento del delitto di cui al comma 11 compete all'autorità giudiziaria.

La autorità competenti vengono individuate:

- nella **Presidenza del Consiglio dei Ministri**, per le amministrazioni pubbliche, gli enti e gli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale (in base al comma 2, lett. *a)*, 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 (in base all'art. 29 del D.Lgs. n. 82 del 2005);
- nel **Ministero dello Sviluppo economico**, per gli operatori nazionali privati inclusi nel perimetro di sicurezza nazionale (in base al comma 2, lett. *a)*.

La Presidenza del Consiglio e il MISE sono dunque le autorità chiamate a vigilare sul rispetto degli obblighi previsti dai commi 2, 3, 6 e 7 della disposizione in commento e ad **irrogare le sanzioni amministrative pecuniarie.**

Per l'accertamento delle violazioni e l'irrogazione delle sanzioni si applica il **procedimento** disciplinato dalla **legge n. 689 del 1981** *(Modifiche al sistema penale).*

In base alla legge del 1981, l'applicazione della sanzione amministrativa pecuniaria avviene secondo il seguente procedimento: accertamento, contestazione-notifica al trasgressore; pagamento in misura ridotta o inoltro di memoria difensiva all'autorità amministrativa (con conseguente archiviazione o emanazione di ordinanza ingiunzione di pagamento); eventuale opposizione all'ordinanza ingiunzione davanti all'autorità giudiziaria ordinaria (giudice di pace o tribunale); accoglimento dell'opposizione, anche parziale, o rigetto (con sentenza ricorribile per cassazione); eventuale esecuzione forzata per la riscossione delle somme.

Allo stato attuale non è possibile circoscrivere il campo delle amministrazioni pubbliche che potranno essere sanzionate dalla

Presidenza del Consiglio e chiamate al pagamento di **sanzioni amministrative pecuniarie**: a ciò provvederà infatti il DPCM che delineerà il perimetro dei soggetti tenuti al rispetto della disciplina sulla sicurezza nazionale cibernetica; tra tali soggetti potrebbero ad esempio essere ricompresi i **ministeri** o le **regioni** e province autonome. Le amministrazioni pubbliche sanzionate potranno opporsi quindi all'ordinanza-ingiunzione di pagamento davanti al **giudice ordinario**.

Di norma, infatti, non è prevista l'attribuzione alla Presidenza del Consiglio di funzioni di accertamento ed irrogazione delle sanzioni amministrative pecuniarie verso le amministrazioni pubbliche.

Nella normativa vigente si riscontrano, peraltro, casi di poteri sanzionatori in relazione alle funzioni svolte dall'Ufficio nazionale per il servizio civile istituito presso la Presidenza del Consiglio. Si tratta del potere di applicare sanzioni amministrative agli **enti gestori del servizio civile** in caso di violazione dei doveri di cooperare per l'efficiente gestione del servizio civile e la corretta realizzazione dei progetti, previa contestazione degli addebiti e fissazione di un termine per controdedurre (art. 3-bis della legge 6 marzo 2001 n. 64).

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 (in base al comma 2, lett. *a)* possono incorrere in **responsabilità disciplinare e amministrativo-contabile**. Si tratta di violazioni che determinano infatti a carico del datore di lavoro una responsabilità amministrativa per il pagamento di una sanzione pecuniaria.

Come già ricordato, le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati **inclusi nel perimetro di sicurezza nazionale cibernetica** e tenuti al rispetto delle misure e degli obblighi previsti dall'art. 1 del decreto-legge in esame sono individuati - entro 4 mesi - con DPCM, su proposta del CISR (ai sensi del comma 2 lettera a).

La **responsabilità amministrativo-contabile** si configura qualora il dipendente pubblico (o soggetto legato alla p.a. da rapporto di servizio), per inosservanza dolosa o (gravemente) colposa dei propri obblighi di servizio, provochi un danno alla propria amministrazione o ad altro ente pubblico.

In particolare, l'istituto della responsabilità amministrativa ricorre in tutte le ipotesi nelle quali il funzionario o l'impiegato, agendo in violazione di obblighi di servizio o doveri di ufficio, produca all'amministrazione un danno, sia direttamente, sia indirettamente. Pertanto tale forma di responsabilità serve a tutelare la pubblica amministrazione, obbligando il funzionario a risarcire il danno arrecato all'ente a causa della sua condotta: si tratta, dunque, di una responsabilità a carattere risarcitorio (come la responsabilità civile) in quanto, di norma, è diretta alla riparazione di un danno patrimoniale. Si tratta, infine, di una

responsabilità speciale, governata da un giudice speciale, in quanto le funzioni giurisdizionali spettano alla Corte dei Conti.

L'istituto è stato interessato, a partire dagli anni '90, da un rilevante processo di riforma che ha profondamente inciso la sua disciplina normativa (L. 20/1994, modificata dal D.L. 546/1996), che presenta i seguenti caratteri fondamentali:

- il giudizio non è introdotto dall'amministrazione che subisce il danno, ma, d'ufficio, dalla Procura della Corte dei conti, eventualmente in base ad una denuncia;
- affinché un soggetto possa essere chiamato a rispondere in sede di responsabilità amministrativa occorre che lo stesso, con una condotta dolosa o gravemente colposa collegata o inerente al rapporto esistente con l'amministrazione, abbia causato un danno pubblico risarcibile che si ponga come conseguenza diretta e immediata di detta condotta. La gravità della colpa va valutata in relazione alla diversa natura delle funzioni, o mansioni, svolte dal dipendente pubblico e alla specificità del contesto organizzativo. La colpa è grave quando si discosta notevolmente dallo standard normale richiesto dal tipo di prestazione svolta;
- l'accertamento della responsabilità comporta la condanna al risarcimento del danno a favore dell'amministrazione danneggiata. Nel quantificare il danno il giudice deve valutare se dalla condotta illecita del funzionario sia derivata anche un'utilità per la pubblica amministrazione e tenere conto di questo elemento. Il responsabile deve risarcire solo la parte di danno che può essergli attribuita sulla base di un giudizio effettuato dal giudice in merito all'effettivo apporto causale del responsabile stesso (c.d. «potere riduttivo» del giudice); quindi, nel caso in cui vi siano più responsabili, ciascuno risponde solo della propria quota di danno.

Con l'espressione responsabilità contabile, ci si riferisce alla responsabilità di quei soggetti (agenti contabili) che avendo avuto in consegna (a vario titolo) denaro, beni o altri valori pubblici, o comunque avendone avuto la disponibilità materiale, non adempiano all'obbligo di restituzione che a loro incombe. Pertanto, tale responsabilità si basa sul mancato adempimento di un obbligo di restituzione di un bene (compreso il denaro) dell'amministrazione.

La **responsabilità disciplinare** si concretizza in una violazione del codice disciplinare rinvenibile nel contratto collettivo richiamato dal contratto individuale o nella violazione dei precetti fissati dagli artt. 55 e seguenti del D.Lgs. n. 165 del 2001 o dal codice di comportamento. La titolarità ad accertare la responsabilità disciplinare risiede in capo al dirigente di struttura o all'Ufficio per i procedimenti disciplinari.

Articolo 1, commi 15 e 16
(Raccordi organizzativi e compiti dell'AGID)

Il **comma 15** prevede che le autorità titolari delle attribuzioni quali configurate dal decreto-legge assicurino "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.

Il decreto-legge n. 144 del 2005 ("Misure per il contrasto del terrorismo internazionale") reca un articolo 7-*bis* ("Sicurezza telematica") secondo cui (ferme restando le competenze dei Servizi informativi e di sicurezza), l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale (individuate con decreto del Ministro dell'interno: cfr. il D.M. 9 gennaio 2008), operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture.

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**).

L'Agenzia per l'Italia digitale (AGID) è l'organismo tecnico del Governo che ha il compito di garantire, sulla base degli indirizzi del Presidente del Consiglio o del Ministro delegato, la realizzazione gli obiettivi dell'Agenda Digitale Italiana. Più in generale l'AGID promuove sia l'innovazione digitale del sistema Paese, sia la digitalizzazione delle pubbliche amministrazioni anche nel rapporto con cittadini e imprese. L'Agenzia "opera sulla base di principi di autonomia organizzativa, tecnico-operativa, gestionale, di trasparenza e di economicità e persegue gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e partecipazione dei cittadini e delle imprese".

L'Agenzia per l'Italia digitale è stata istituita dal D.L. 83/2012 (artt. 19-22). Successivamente, sono intervenuti prima il D.Lgs. 179/2016 e poi il D.Lgs. 217/2017 (entrambi di attuazione della legge 124/2015 di riforma della pubblica amministrazione) che hanno apportato diverse modifiche alla disciplina dell'AGID. Tra queste l'inserimento nel Codice dell'amministrazione digitale CAD (D.Lgs. 82/2005) di diverse disposizioni relative dell'Agenzia (in particolare viene abrogato l'art. 20 del D.L. 83 che confluisce nell'art. 14-*bis* del CAD ed è modificato l'art. 21 del medesimo D.L. 83).

Nel corso della XVII legislatura è stato approvato lo Statuto dell'AGID (DPCM 8 gennaio 2014) e il Regolamento di organizzazione (DPCM 27 marzo 2017). Inoltre, con il D.P.C.M. 9 gennaio 2015 sono state determinate le dotazioni delle risorse umane, finanziarie e strumentali dell'Agenzia.

Con la creazione dell'Agenzia per l'Italia digitale, ad opera del D.L. 83/2012, è stata realizzata una razionalizzazione delle funzioni pubbliche in materia di innovazione tecnologica e di digitalizzazione della pubblica amministrazione.

Alla nuova Agenzia sono state attribuite le funzioni precedentemente espletate dall'Agenzia per la diffusione delle tecnologie per l'innovazione, parte di quelle della DigitPA (enti che vengono contestualmente soppressi), nonché quelle facenti capo al Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri. All'Agenzia sono trasferite anche le funzioni in materia di sicurezza delle reti svolte dall'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione.

L'Agenzia ha tra gli altri i seguenti compiti:

- emanazione di **linee guida** contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme del CAD;
- **programmazione** e **coordinamento** delle attività delle amministrazioni per l'uso delle tecnologie dell'informazione e della comunicazione, mediante il **Piano triennale per l'informatica nella pubblica amministrazione**;
- **monitoraggio** delle attività svolte dalle amministrazioni in relazione alla loro coerenza con il Piano triennale;
- predisposizione, realizzazione e gestione di **interventi** e **progetti di innovazione**;
- promozione della cultura digitale;
- rilascio di **pareri tecnici**, obbligatori e non vincolanti, sugli schemi di contratti e accordi quadro di particolare valore da parte delle pubbliche amministrazioni centrali concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati per quanto riguarda la congruità tecnico-economica;
- rilascio di **pareri tecnici**, obbligatori e vincolanti sugli elementi essenziali delle procedure di gara bandite da Consip concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e definiti di carattere strategico nel piano triennale;
- **vigilanza** sui servizi fiduciari (quali quelli relativi alle transazioni elettroniche, sui gestori di posta elettronica certificata, sui soggetti che partecipano a SPID.

Sono **organi** dell'Agenzia:

- il Direttore generale, nominato dal Presidente del Consiglio o dal Ministro delegato tramite procedura di selezione ad evidenza pubblica, tra persone di particolare e comprovata qualificazione professionale in materia di innovazione tecnologica e in possesso di

una documentata esperienza di elevato livello nella gestione di processi di innovazione;
- il Comitato di indirizzo;
- il Collegio dei revisori dei conti.

Nel marzo 2019 è stato adottato dal governo il Piano triennale per l'informatica nella pubblica amministrazione 2019-2021, redatto a cura dell'AGID.

Il Piano triennale affronta in modo sistematico il problema della **sicurezza informatica** individuando alcuni interventi per aumentare il livello di sicurezza complessivo dell'amministrazione. Tra questi, in primo luogo, la razionalizzazione delle risorse ICT.

Per un approfondimento dei contenuti del Piano triennale e, più in generale, del ruolo delle pubbliche amministrazioni nella sicurezza informatica si veda il *dossier* del Servizio studi, Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber, 24 settembre 2019 (pag. 80 e seguenti).

Articolo 1, commi 17 e 18
(Novelle al decreto legislativo n. 65 del 2018 e invarianza degli oneri finanziari)

L'**articolo 1**, **comma 17** reca due novelle al decreto legislativo n. 65 del 2018 (il quale 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 novella - recata dalla **lettera *a)*** - attiene alla identificazione degli operatori di servizi essenziali (la quale è oggetto dell'articolo 4 del decreto legislativo n. 65).
Più esattamente, la novella concerne l'**elenco nazionale degli operatori di servizi essenziali**, che l'articolo 4, comma 5, del decreto legislativo n. 65 ha istituito presso il Ministero dello sviluppo economico.
Si viene ora a prevedere che quel Ministero trasmetta l'elenco nazionale di servizi essenziali al punto di contatto unico nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Il punto di contatto unico - ossia l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea - è (ai sensi dell'art. 7, comma 3 del decreto legislativo n. 65 del 2018) il Dipartimento delle informazioni per la sicurezza (DIS).
L'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione è - ai sensi dell'art. 7-*bis* ("Sicurezza telematica") del decreto-legge n. 144 del 2005 - preposto ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale.

La seconda novella - **lettera *b)*** - 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 (composto dalle autorità competenti NIS, dal punto di contatto unico e dal CSIRT italiano, ai sensi dell'art. 9 del medesimo decreto legislativo n. 65).

L'**articolo 1, comma 18** dispone, a sua volta, 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**.

Articolo 2, commi 1 e 2
(Personale per esigenze di funzionamento del CVCN)

Il **comma 1** autorizza il MISE 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**, di cui 67 di area terza e 10 di area seconda, nel limite di spesa di euro 3.005.000 annui a decorrere dal 2020, 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**), di cui all'articolo 1, commi 6 e 7 (alla cui scheda di lettura si rinvia).

Il Centro di valutazione e certificazione nazionale è stato istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019. Il centro è stato istituito presso l'Istituto Superiore delle comunicazioni e tecnologie dell'informazione. Il 19 aprile 2019 è stato firmato il decreto direttoriale che descrive il modello di funzionamento, l'organizzazione e il piano di sviluppo del CVCN, così come previsto dal richiamato decreto del Ministro dello sviluppo economico.

Per un approfondimento si veda il resoconto stenografico della seduta della Commissione Trasporti del 7 maggio 2019, audizione di rappresentanti dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) del Ministero dello sviluppo economico nell'ambito dell'indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5g ed alla gestione dei big data.

In particolare, nel documento depositato presso la IX Commissione, si osserva che [i]"n questa prospettiva va letta, infatti, la recente istituzione del Centro di valutazione e certificazione nazionale (CVCN) presso il Ministero dello Sviluppo Economico, che si aggiunge ai già attivi OCSI (Organismo di certificazione della sicurezza informatica) per prodotti e sistemi ICT commerciali – attivato nel 2004 - e CE.VA. (Centro di Valutazione) della sicurezza informatica di prodotti e sistemi destinati a gestire dati coperti dal segreto di Stato o di vietata divulgazione), anch'essi operativi presso l'ISCTI del Ministero dello Sviluppo Economico.

Sul piano normativo, il DPCM 17 febbraio 2017 aveva definito l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica.

In questo contesto, è stato all'epoca previsto che il Ministero dello sviluppo economico promuovesse "*l'istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere*

utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale".

Successivamente, il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica, varato dalla Presidenza del Consiglio dei Ministri nel marzo 2017, ha precisato che tale Centro sarebbe stato realizzato presso il Ministero dello sviluppo economico.

In tale contesto, il Centro di valutazione e certificazione nazionale, istituito con decreto del Ministro dello sviluppo economico del 15 febbraio 2019, costituisce, soprattutto in prospettiva, un importante tassello ai fini della sicurezza cibernetica del Paese.

Il Centro è stato istituito presso l'Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione (ISCTI) del Mise per la competenza acquisita negli anni nel settore della certificazione informatica. La fase di progettazione del Centro è stata ultimata ed è in corso di completamento anche la definizione delle procedure per il suo funzionamento, perseguendo l'obiettivo generale di contemperare gli aspetti di sicurezza e le esigenze di mercato delle imprese coinvolte.

Il 19 aprile 2019 il Direttore dell'ISCTI ha firmato il Decreto che descrive il modello di funzionamento, l'organizzazione ed il piano di sviluppo del CVCN.

La sua operatività si svilupperà secondo un approccio graduale sulla base delle risorse umane e finanziarie disponibili.

Al di là degli aspetti tecnici di realizzazione del Centro l'impatto delle sue attività dipenderà da una serie di fattori, in particolare la definizione di un quadro normativo che individui le infrastrutture critiche e strategiche - problematica comunque già all'attenzione del Governo - e stabilisca specifici obblighi per l'acquisizione di prodotti e sistemi destinati alle predette infrastrutture. Tale quadro dovrà tenere anche conto delle disposizioni sulla realizzazione del "framework" di certificazione europea, contenute in un regolamento di prossima pubblicazione nell'Unione Europea, comunemente denominato "Cyber Act".

Tale regolamento, che fra l'altro prevede il rafforzamento del mandato dell'ENISA, istituisce un perimetro normativo comune per la certificazione della sicurezza informatica. Il nuovo quadro di certificazione mira a rafforzare il mercato unico digitale dell'Unione, accrescendo l'affidabilità dei prodotti e la consapevolezza degli utenti.

In questo nuovo contesto, che prevede la costituzione di sistemi europei di certificazione di prodotti e servizi ICT, il nostro Paese, per il tramite del Ministero dello sviluppo economico, si trova assolutamente in linea con l'azione europea".

Il **comma 2** prevede che, fino al completamento delle procedure di assunzione, il MISE, fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale anche nell'ambito del Trattato dell'Atlantico del Nord, può avvalersi, per le esigenze del CVCN di un contingente di **personale non dirigenziale** appartenente alle pubbliche amministrazioni di cui all'art. 1, co. 2, d.lgs. 165/2001, con esclusione del **personale docente educativo e**

amministrativo tecnico ausiliario delle istituzioni scolastiche, in posizione di **fuori ruolo** o di **comando** o altro analogo istituto previsto dai rispettivi ordinamenti ai sensi dell'art. 17, co. 14, L. 127/1997, e dell'art. 70, co. 12, d.lgs. 165/2001, per un **massimo del 40 per cento** delle unità di personale da assumere in base al comma 1.

In base all'art. 17, co. 14, L. 127/1997, nel caso in cui disposizioni di legge o regolamentari dispongano l'utilizzazione presso le amministrazioni pubbliche di un contingente di personale in posizione di fuori ruolo o di comando, le amministrazioni di appartenenza sono tenute ad adottare il provvedimento di fuori ruolo o di comando entro quindici giorni dalla richiesta.

L'art. 70, co. 12, d.lgs. 165/2001, prevede che in tutti i casi, anche se previsti da normative speciali, nei quali enti pubblici territoriali, enti pubblici non economici o altre amministrazioni pubbliche, dotate di autonomia finanziaria sono tenute ad autorizzare l'utilizzazione da parte di altre pubbliche amministrazioni di proprio personale, in posizione di comando, di fuori ruolo, o in altra analoga posizione, l'amministrazione che utilizza il personale rimborsa all'amministrazione di appartenenza l'onere relativo al trattamento fondamentale.

Nei limiti complessivi della stessa quota il MISE può avvalersi, in posizione di **comando**, di personale che non risulti impiegato in **compiti operativi o specialistici** con qualifiche o gradi **non dirigenziali** del **comparto sicurezza-difesa** fino a **un massimo di 20 unità**, conservando lo stato giuridico e il trattamento economico fisso, continuativo ed accessorio, secondo quanto previsto dai rispettivi ordinamenti, con oneri a carico del MISE, ai sensi dell'art. 1777 del codice dell'ordinamento militare (d.lgs. 66/2010) e dell'art. 2, co. 91, L. 244/2007.

L'art. 1777 del codice dell'ordinamento militare prevede che, ferma restando, in quanto compatibile, la disciplina generale in materia di trattamento economico e di assegno per il nucleo familiare dei dipendenti pubblici prevista dalle disposizioni vigenti, al personale dell'Esercito italiano, della Marina militare e dell'Aeronautica militare si applicano le disposizioni emanate a seguito delle procedure di concertazione previste dal d.lgs. 195/1995, nonché le norme del libro VI (Trattamento economico, assistenza e benessere) che hanno efficacia ai soli fini del trattamento economico. Al medesimo personale si applicano le disposizioni di cui all'articolo 2, comma 91, della legge 24 dicembre 2007, n. 244, che pongono a carico delle amministrazioni utilizzatrici gli oneri del trattamento economico fondamentale e accessorio del personale in posizione di comando appartenente alle Forze di polizia e al Corpo nazionale dei vigili del fuoco.

In base all'art. 2, co. 91, L. 244/2007, a decorrere dal 1º febbraio 2008, il trattamento economico fondamentale ed accessorio attinente alla posizione di comando del personale appartenente alle Forze di polizia e al Corpo nazionale

dei vigili del fuoco è posto a carico delle amministrazioni utilizzatrici dello stesso.

Articolo 2, commi 3 e 4
(Assunzioni presso la Presidenza del Consiglio)

L'**articolo 2, comma 3** autorizza la Presidenza del Consiglio ad assumere fino a dieci 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.

In particolare, il **comma 3** autorizza la Presidenza del Consiglio dei ministri ad assumere - **a tempo indeterminato** - un **contingente massimo di dieci unità di personale non dirigenziale** (da inquadrare nella categoria funzionale A, parametro retributivo F1) per le funzioni in materia di digitalizzazione.

Le nuove assunzioni sono in aggiunta alle ordinarie facoltà assunzionali. Pertanto si ha un corrispondente incremento della dotazione organica.

L'autorizzazione di spesa è nel limite di **640.000 euro** annui, a decorrere dall'anno 2020.

Il **comma 4** reca una duplice concorrente autorizzazione alla Presidenza del Consiglio, fino al completamento delle procedure per le assunzioni a tempo indeterminato sopra ricordate.

Fatte salve le unità dedicate all'assolvimento delle esigenze connesse alle operazioni condotte dalle Forze armate per la difesa nazionale (anche nell'ambito dell'Alleanza atlantica), l'autorizzazione è, più in dettaglio, ad avvalersi di:

- personale non dirigenziale appartenente alle pubbliche amministrazioni;
- esperti o consulenti.

Una prima autorizzazione è ad avvalersi di **personale non dirigenziale appartenente ad altre pubbliche amministrazioni**.

Rimane escluso il personale docente educativo ed amministrativo tecnico ausiliario delle istituzioni scolastiche.

L'autorizzazione è ad avvalersi nel limite del 40 per cento delle unità previste dal comma 3 (ossia fino a **quattro**), di personale di altre pubbliche amministrazioni.

Le unità prescelte sono collocate in posizione di fuori ruolo, di comando o di altro analogo istituto.

La disposizione recata dal comma 3 fa richiamo alle seguenti altre norme.

L'articolo 17, comma 14, della legge n. 127 del 1997 prevede che, ove disposizioni di legge o regolamentari dispongano l'utilizzazione presso le amministrazioni pubbliche di un contingente di personale in posizione di fuori ruolo o di comando, le amministrazioni di appartenenza siano tenute ad adottare il provvedimento di fuori ruolo o di comando entro quindici giorni dalla richiesta.

L'articolo 9, comma *5-ter*, del decreto legislativo n. 303 del 1999 prevede che il personale dipendente di ogni ordine, grado e qualifica del comparto Ministeri chiamato a prestare servizio in posizione di comando o di fuori ruolo presso la Presidenza del Consiglio, mantenga il trattamento economico fondamentale delle amministrazioni di appartenenza, compresa l'indennità di amministrazione, ed i relativi oneri rimangano a carico delle stesse. Per il personale appartenente ad altre amministrazioni pubbliche, chiamato a prestare servizio in analoga posizione, la Presidenza del Consiglio provvede, d'intesa con l'amministrazione di appartenenza del dipendente, alla ripartizione dei relativi oneri, senza pregiudizio per il trattamento economico fondamentale spettante al dipendente medesimo.

Una seconda, concorrente autorizzazione è ad avvalersi di **esperti e consulenti**.

Essi debbono essere in possesso di particolare e comprovata specializzazione in materia informatica.

Parrebbe suscettibile di approfondimento se il numero massimo degli esperti e consulenti che possono essere nominati in base al comma 4 sia ricompreso nel limite del 40 per cento (quindi nel limite di quattro) ovvero se sia inteso come corrispondente al numero di unità determinate dal precedente comma 3 (massimo dieci) detratte *le unità (massimo quattro) di personale appartenente ad altre amministrazioni pubbliche.*

Gli esperti e consulenti sono nominati ai sensi dell'articolo 7, comma 6, del decreto legislativo n. 165 del 2001.

Quest'ultimo (fermo restando il divieto per le amministrazioni pubbliche di stipulare contratti di collaborazione che si concretino in prestazioni di lavoro esclusivamente personali e continuative) prevede che per specifiche esigenze non fronteggiabili con proprio personale in servizio, le amministrazioni pubbliche possano conferire esclusivamente incarichi individuali, con contratti di lavoro autonomo, ad esperti di particolare e comprovata specializzazione anche universitaria, in presenza dei seguenti presupposti di legittimità: *a)* l'oggetto della prestazione deve corrispondere alle competenze attribuite dall'ordinamento

all'amministrazione conferente, ad obiettivi e progetti specifici e determinati e deve risultare coerente con le esigenze di funzionalità dell'amministrazione conferente; *b)* l'amministrazione deve avere preliminarmente accertato l'impossibilità oggettiva di utilizzare le risorse umane disponibili al suo interno; *c)* la prestazione deve essere di natura temporanea e altamente qualificata; non è ammesso il rinnovo; l'eventuale proroga dell'incarico originario è consentita, in via eccezionale, al solo fine di completare il progetto e per ritardi non imputabili al collaboratore, ferma restando la misura del compenso pattuito in sede di affidamento dell'incarico; *d)* devono essere preventivamente determinati durata, oggetto e compenso della collaborazione.

Nell'ambito delle politiche di innovazione del settore pubblico un ruolo fondamentale è svolto dalla digitalizzazione delle amministrazioni pubbliche.

Per amministrazione digitale - o *eGovernment* – "si intende l'uso delle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche" (Commissione delle Comunità europee, Il ruolo dell'*eGovernment* per il futuro dell'Europa, 26 settembre 2003, p. 8). L'informatizzazione delle amministrazioni pubbliche è tra i temi centrali del dibattito pubblico negli ultimi anni, soprattutto al fine di dare piena attuazione all'Agenda digitale europea.

Il Presidente del Consiglio dei ministri è la figura di coordinamento delle politiche di digitalizzazione della pubblica amministrazione. Nell'attuale Governo è stato nominato il Ministro senza portafoglio per l'innovazione tecnologica e la digitalizzazione (D.P.R 4 settembre 2019). Presso la Presidenza del Consiglio è stato istituito il Dipartimento per la trasformazione digitale, struttura di supporto al Presidente del Consiglio per la promozione ed il coordinamento delle azioni di Governo finalizzate alla definizione di una strategia unitaria in materia di trasformazione digitale e di modernizzazione del Paese attraverso le tecnologie digitali (D.P.C.M. 19 giugno 2019).

L'Agenzia per l'Italia digitale (AGID) è l'organismo tecnico del Governo che ha il compito di garantire, sulla base degli indirizzi del Presidente del Consiglio, la realizzazione gli obiettivi dell'Agenda Digitale Italiana. Più in generale l'AGID promuove sia l'innovazione digitale del sistema Paese, sia la digitalizzazione delle pubbliche amministrazioni anche nel rapporto con cittadini e imprese.

Nel marzo 2019 è stato approvato il Piano triennale per l'informatica nella pubblica amministrazione 2019-2021 che definisce le linee operative di sviluppo dell'informatica pubblica nei prossimi anni. Tra i requisiti strategici da soddisfare, viene considerato prioritario il principio del *digital by default*, ovvero "digitale per definizione": le pubbliche amministrazioni devono fornire servizi digitali come opzione predefinita.

Articolo 2, comma 5
(Reclutamento del personale del CVCN e della Presidenza del consiglio dei ministri)

L'**articolo 1, comma 5,** dispone che il **reclutamento del personale** necessario al funzionamento del CVCN (di cui al comma 1) e allo svolgimento delle funzioni di digitalizzazione della Presidenza del Consiglio (di cui al comma 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** per le amministrazioni dello Stato, anche ad ordinamento autonomo, le agenzie e gli enti pubblici non economici (*ex* art. 4, c. 3-*quinquies* e 3-*sexies*, del D.L. 101/2013);
- il **ricorso alla Commissione** per l'attuazione del Progetto di Riqualificazione delle Pubbliche Amministrazioni (**RIPAM**) per lo svolgimento delle procedure selettive delle restanti amministrazioni (*ex* art. 35, c. 5, del D.Lgs. 165/2001).

Il comma in esame fa comunque salva la **facoltà per le amministrazioni di avvalersi delle modalità semplificate** e delle misure di riduzione dei tempi di accesso al pubblico impiego previste dall'articolo 3 della L. 56/2019.

In particolare, il comma 4 del richiamato articolo 3, con riferimento al triennio 2019-2021, reca norme transitorie volte a ridurre i tempi di accesso al pubblico impiego, fatta salva la previsione di cui all'art. 1, c. 399, della legge di bilancio per il 2019, secondo cui determinate amministrazioni non possono effettuare assunzioni di personale a tempo indeterminato con decorrenza giuridica ed economica anteriore al 15 novembre 2019.

Il suddetto comma consente di procedere, in deroga alla procedura di autorizzazione richiamata dal medesimo articolo 3 della L. 56 ed alle norme sulla mobilità volontaria:

a) all'assunzione a tempo indeterminato di vincitori o allo scorrimento delle graduatorie vigenti, nel limite massimo dell'80 per cento delle facoltà di assunzione previste per ciascun anno;
b) all'avvio di procedure concorsuali, nel limite massimo dell'80 per cento delle facoltà di assunzione previste per il corrispondente triennio, al netto delle risorse di cui alla lettera *a)*, solo successivamente alla maturazione della corrispondente facoltà di assunzione, secondo le modalità previste dalla normativa vigente (*ex* art. 4, c. 3-*quinquies* e 3-*sexies*, del D.L. 101/2013 e art. 35, c. 5, del D.Lgs. 165/2001). Per tali assunzioni, le amministrazioni tengono conto degli eventuali specifici titoli di preferenza previsti dalle disposizioni vigenti.

Resta fermo - con riferimento alle suddette facoltà assunzionali - il rispetto delle norme richiamate dal medesimo comma 4, tra cui il principio della previa verifica della sussistenza di situazioni di soprannumero o di eccedenze di personale nella medesima amministrazione.

Articolo 3
(Disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5G)

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.

Il **comma 1** stabilisce che le disposizioni del decreto in esame 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 sulla tecnologia 5G, rispetto ai quali è prevista dall'articolo 1-*bis* del decreto-legge in materia di poter 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) che dispone la previsione di un obbligo di comunicazione al CVCN con riferimento 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 indicati nell'elenco da predisporre ai sensi dell'articolo 1, comma 2, lettera b) del decreto-legge all'esame.

Il **comma 2** detta norme in materia di esercizio dei poteri speciali. Esso 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 dei centri di valutazione di cui all'articolo 1, comma 6, lettera a), (ossia il CVCN e il Centro di valutazione del Ministero della difesa) sulla base della disciplina prevista in attuazione del predetto regolamento.

Il **comma 3** stabilisce una disciplina transitoria, prevedendo 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 in esame, anche con prescrizioni di **sostituzione** di apparati o prodotti che risultino **gravemente inadeguati** sul piano della sicurezza.

In dettaglio il **comma 1** stabilisce che - fatta eccezione per quanto previsto dall'articolo 1, comma 6, lettera a) in materia di *procurement* - le disposizioni del decreto in esame si applicano ai **soggetti** indicati dall'articolo 1, comma 2, lettera a) inclusi nel **perimetro di sicurezza nazionale cibernetica**, anche nei casi in cui questi siano tenuti alla **notifica** al Governo delle operazioni di cui all'articolo 1-bis del decreto-legge n. 21 del 2012, in materia di poteri speciali.

Tale articolo 1-*bis* qualifica i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G quali **attività di rilevanza strategica** per il sistema di **difesa e sicurezza nazionale**, ai fini dell'esercizio dei **poteri speciali**; esso stabilisce l'assoggettamento a **notifica** (di cui all'articolo 1, comma 4 del decreto legge n. 21 del 2012) per i contratti o gli accordi ivi indicati - ove conclusi con soggetti esterni all'Unione europea - al fine dell'eventuale **esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni**.

Si tratta dei contratti o accordi che abbiano ad oggetto:

- l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di tecnologia 5G
- ovvero l'acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione.

A tal fine, la norma specifica che sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano.

Ai fini dell'inquadramento della normativa in materia di **poter speciali**, si ricorda che il D.L. n. 21 del 2012, come convertito in legge, reca norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.

L'articolo 1-bis di tale D.L. è stato inserito dall'art. 1, comma 1, del D.L. 25 marzo 2019, n. 22, convertito, con modificazioni, dalla L. 20 maggio 2019, n. 41 e disciplina la materia dei **poteri speciali** inerenti le reti di telecomunicazione elettronica a banda larga con **tecnologia 5G**. Si ricorda che sull'articolo 1-bis in parola era intervenuto, con novelle, il D.L. 11 luglio 2019, n. 64 (in particolare si veda l'art. 1, comma 3, dello stesso), successivamente però non convertito in legge (Comunicato 10 settembre 2019, pubblicato nella G.U. 10 settembre 2019, n. 212).

Nel dettaglio, l'articolo 1-bis indicato stabilisce l'assoggettamento a **notifica** (di cui all'articolo 1, comma 4 del decreto legge n. 21 del 2012) per i contratti o gli accordi, qualora siano conclusi con soggetti esterni all'Unione europea, che abbiano ad oggetto l'acquisto di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di

comunicazione elettronica a banda larga basati sulla tecnologia 5G; altresì soggette a notifica sono le acquisizioni di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione. La previsione come detto è finalizzata all'eventuale esercizio del potere di veto o all'imposizione di specifiche prescrizioni o condizioni.

A tal fine, si specifica altresì che sono oggetto di valutazione anche gli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza sia delle reti sia dei dati che vi transitano.

Un soggetto si intende esterno all'Unione europea qualora rientri nelle seguenti categorie:

1) persona fisica o persona giuridica, che non abbia la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che non sia comunque ivi stabilito;

2) persona giuridica che abbia stabilito la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, e che risulti controllato direttamente o indirettamente da una persona fisica o da una persona giuridica di cui al n. 1) precedente;

3) persona fisica o persona giuridica che abbia stabilito la residenza, la dimora abituale, la sede legale o dell'amministrazione o il centro di attività principale in uno Stato membro dell'Unione europea o dello Spazio economico europeo o che sia comunque ivi stabilito, al fine di eludere l'applicazione della disciplina della nuova norma introdotta.

Si demanda ad un D.P.C.M., sentito il Gruppo di coordinamento (costituito col citato decreto del Presidente del Consiglio dei ministri del 6 agosto 2014) la facoltà di individuare misure di semplificazione in ordine a modalità di notifica, termini, procedure relativi all'istruttoria, ai fini dell'eventuale esercizio dei poteri di veto ovvero di imposizione di specifiche prescrizioni.

In ordine all'ambito applicativo della disposizione, i **soggetti** di cui all'articolo 1, comma 2, lettera a), indicati in disposizione, sono quelli individuati (entro quattro mesi dalla data di entrata in vigore della legge di conversione del decreto-legge in esame) con D.P.C.M. adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR); in particolare, ai sensi della lettera menzionata a), sono individuate le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati **inclusi nel perimetro di sicurezza nazionale cibernetica** e tenuti al rispetto delle misure e degli obblighi previsti dall'articolo 1 del decreto-legge in esame.

Alla predetta individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base degli indicati criteri:

1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

Si ricorda che il decreto-legge in esame stabilisce, al comma 1 dell'articolo 1, l'istituzione del **perimetro di sicurezza nazionale cibernetica**, con la finalità di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero 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, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

La norma in esame precisa, come detto, che è fatta **eccezione per quanto previsto dall'articolo 1, comma 6, lettera a**), il quale demanda ad un D.P.C.M., da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge in esame, la disciplina di **procedure, modalità e termini** cui 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 di *information and communication technology* - ICT indicati dalla normativa in esame.**

Per approfondimenti si rinvia alla relativa scheda riferita all'articolo 1, comma 6.

Il **comma 2** detta norme in materia di **esercizio dei poteri speciali.** Esso stabilisce che, dalla data di entrata in vigore del citato regolamento su procedure, modalità e termini per l'affidamento di forniture di beni e servizi ICT (previsto dall'articolo 1, comma 6), i **poteri speciali inerenti le reti 5G** (di cui all'articolo 1-*bis* del D.L. n. 21 del 2012 già richiamato), 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 dei centri di valutazione** di cui all'articolo 1, comma 6, lettera a), sulla base della disciplina prevista in attuazione del predetto regolamento.

Dalla formulazione letterale della norma, che fa riferimento ai "centri di valutazione" sembra desumersi che tale attività sia svolta dal Centro di

valutazione nazionale istituito presso il MISE e da quello proprio del Ministero della difesa, entrambi citati dal richiamato comma 6, lettera a) dell'articolo 1.

Il **comma 3** stabilisce una disciplina transitoria, prevedendo la possibilità di ridefinire, nel **termine di sessanta giorni dalla data di entrata in vigore del regolamento** di cui all'articolo 1, comma 6, le condizioni o le prescrizioni relative ai beni e servizi acquistati con contratti già autorizzati.

Al riguardo si ricorda che il termine ultimo per l'emanazione del regolamento in questione è di 10 mesi dalla data di entrata in vigore del disegno di legge di conversione del decreto-legge e che pertanto gli interventi concernenti i contratti **già autorizzati** potrebbero intervenire in un periodo di oltre 10 mesi e 60 giorni (**ossia quasi un anno**) dalla data di pubblicazione della legge di conversione del decreto-legge. Considerato che l'esercizio dei poteri speciali con riferimento alle reti di telecomunicazione elettronica a banda larga con tecnologia 5G è stato introdotto dal decreto-legge n. 22 del 2019, si deve ritenere che tale possibilità di intervento si estenda a tutti i contratti conclusi dalla data nella quale le disposizioni del citato decreto-legge sono entrate in vigore e per i quali vi sia stata un'autorizzazione ai sensi dell'articolo 1-bis del decreto-legge n. 21 del 2012.

In particolare, possono essere modificate o integrate con **misure aggiuntive necessarie ad assicurare livelli di sicurezza** equivalenti a quelli previsti dal decreto-legge in esame le condizioni e le prescrizioni relative ai beni e servizi acquistati con **contratti già autorizzati** con **decreti del Presidente del Consiglio dei ministri -** e adottati sulla base della normativa sui poteri speciali in data anteriore alla data di entrata in vigore del medesimo regolamento -, qualora attinenti:

- alle reti
- ai sistemi informativi
- e ai servizi informatici

inseriti negli elenchi dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

Si indica a tal fine la **procedura** di cui al comma 2 della disposizione in commento, che prevede la previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità, da parte dei centri di valutazione, sulla base della disciplina prevista in attuazione del predetto regolamento.

Le modifiche o integrazioni contrattuali possono anche consistere in prescrizioni, ove necessario, di **sostituzione di apparati o prodotti** che risultino 'gravemente inadeguati' sul piano della sicurezza.

Si ricorda che, nella seduta del 5 settembre 2019 il Consiglio dei Ministri, su proposta del Ministro dello sviluppo economico, a norma dell'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21, ha deliberato:

- l'esercizio dei poteri speciali in relazione alla informativa notificata dalla società LINKEM S.p.a. relativa a contratti o accordi aventi ad oggetto l'acquisto di beni e servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga su tecnologia 5G e acquisizione di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione;
- l'esercizio di poteri speciali, con condizioni e prescrizioni, in relazione all'operazione notificata dalla società Vodafone S.p.a. consistente in accordi aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G;
- l'esercizio dei poteri speciali in relazione all'informativa notificata dalla società TIM S.p.a. relativa agli accordi conclusi prima del 26 marzo relativi ad apparati e sistemi di comunicazione rispetto ai quali la tecnologia 5G può essere considerata una naturale evoluzione;
- l'esercizio dei poteri speciali, con prescrizioni, in relazione all'informativa notificata dalla società Wind Tre S.p.a. circa gli accordi stipulati con la società Huawei, aventi ad oggetto l'acquisto di beni e servizi per la realizzazione e la gestione di reti di comunicazione elettronica basate sulla tecnologia 5G;
- l'esercizio dei poteri speciali in relazione all'informativa notificata dalla società FASTWEB S.p.a. relativa all'acquisto dalla società ZTE Corporation degli apparati relativi alle componenti radio per la realizzazione dell'ultima tratta della rete 5G FWA.

Tali poteri sono stati esercitati con decreti del Presidente del Consiglio dei ministri del 5 settembre 2019, trasmessi alle Camere ai sensi dell'articolo 1 e 1-bis del decreto-legge n. 21 del 2012.

Inoltre, con il decreto del Presidente del Consiglio dei ministri del 26 giugno 2019, sono stati esercitati i poteri speciali a norma dell'articolo 1-bis del decreto-legge n. 21 del 2012 in relazione all'accordo tra Fastweb e Samsung per la progettazione, fornitura, configurazione e manutenzione di apparati software relativi alle componenti radio e core network necessari alla realizzazione della rete 5G Fixed Wireless Access nelle città pilota di Bolzano e Biella.

Il 5G è il nuovo standard per la comunicazione mobile che presenta caratteristiche tali da costituire non una semplice evoluzione delle precedenti generazioni ma una vera e propria tecnologia abilitante idonea a costruire un ecosistema che potrà adattarsi ad un'ampia gamma di applicazioni: tra le sue caratteristiche fondamentali, oltre ad assicurare una velocità di download e upload molto elevata, sono da annoverare: la bassa latenza (ossia distanza temporale tra il momento in cui un evento succede e viene raccolto come dato e quello in cui un'azione consegue che risulta pari o addirittura inferiore ai tempi

di reazione umana), la capacità di connettere un numero assai più elevato di oggetti (si passa da 10-15.000 sensori per chilometro quadrato ad un milione), la maggiore economicità della trasmissione e la direzionalità del segnale (che "seguirà" l'oggetto da raggiungere con la connessione assicurando un uso più efficiente dello spettro e minori emissioni) e il cosiddetto *slicing* ossia la capacità di offrire sulla stessa infrastruttura connessioni specializzate per applicazioni critiche (ad esempio per la connessione delle auto a guida autonoma, o per la telemedicina) per le quali sono richieste caratteristiche specifiche in termini di latenza, affidabilità, sicurezza ecc.

Con la decisione n. 243/2012/UE del 14 marzo 2012, è stato definito un **programma pluriennale europeo in materia di spettro radio** ("Radio Spectrum Policy Programme"- RSPP), che prevede che gli Stati membri e la Commissione europea cooperino per sostenere e conseguire una serie di obiettivi strategici, in particolare che adottino tutte le misure necessarie per garantire la disponibilità di spettro radio sufficiente (almeno 1.200 Mhz) per copertura e capacità all'interno dell'Unione, al fine di consentire di disporre della banda larga più veloce e fare in modo che le applicazioni senza fili ed il ruolo guida europeo nei nuovi servizi possano contribuire efficacemente alla crescita economica e alla realizzazione dell'obiettivo dell'accesso ad una velocità della banda larga di almeno 30 Mbps entro il 2020 per tutti cittadini (Risoluzione del Parlamento europeo del 19 gennaio 2016). La comunicazione della Commissione del 6 maggio 2015 "A Digital Single Market Strategy for Europe" e la successiva la comunicazione, c.d "Gigabit Society" del 14 settembre 2016, hanno evidenziato che disponibilità di un idoneo quantitativo di spettro radio rappresenta uno dei presupposti essenziali per la fornitura e diffusione dei servizi wireless a banda larga e ultra-larga, insieme ad adeguati standard a garanzia di una comunicazione efficiente tra i vari componenti digitali (quali dispositivi, reti e archivi di dati), sottolineando l'importanza delle reti di telecomunicazione ad alta capacità, ritenute un asset fondamentale affinché l'Unione europea possa competere nel mercato globale.

Le **politiche europee per lo sviluppo del 5G** sono esposte nel "Piano di azione per il 5G" della Commissione europea, di cui alla comunicazione della Commissione europea del 14 settembre 2016, COM(2016) 588 final. La Comunicazione prevede una serie di azioni mirate al **dispiegamento tempestivo e coordinato in Europa delle reti 5G**. In particolare obiettivo della Comunicazione è quello di assicurare l'allineamento delle tabelle di marcia e delle priorità per il dispiegamento coordinato delle reti 5G per una loro rapida introduzione **entro il 2018** e per una progressiva introduzione su larga scala entro il 2020. E' inoltre in preparazione il nuovo **Codice europeo delle comunicazioni elettroniche** (Proposta di direttiva 2016/0288/COD), che ha la finalità di consentire ai consumatori di beneficiare di un maggiore livello di protezione uniforme in tutta l'UE e nel cui ambito si prevede la promozione degli **investimenti** nel **5G**, disponendo che gli Stati membri dovranno garantire agli operatori, in linea generale, la prevedibilità normativa per un periodo di almeno 20 anni per quanto riguarda la concessione di licenze relative allo spettro per la banda larga senza fili. Dopo aver raggiunto un accordo provvisorio con il

Parlamento europeo sulla riforma di tale **codice,** nonché su un aggiornamento del mandato dell'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), il 29 giugno 2018 gli ambasciatori dei paesi dell'UE hanno **approvato**, a nome del Consiglio, un **testo,** che dovrà essere approvato dal Parlamento europeo e dal Consiglio.

I lavori per la standardizzazione e lo sviluppo dei sistemi 5G, iniziati nel 2013 (a partire dall'iniziativa della Commissione UE: " 5G Public Private Partnership" e del gruppo di lavoro " 5G Architecture Working Group"), sono tuttora in corso, con impiego di risorse europee che stanno finanziando numerosi progetti di ricerca (19 progetti).

Per ulteriori approfondimenti, anche in relazione agli interventi per lo sviluppo del 5G, si vedano i temi web della Camera, dove è attualmente in corso, presso la Commissione Trasporti, poste e telecomunicazioni (IX), l'Indagine conoscitiva sulle nuove tecnologie delle telecomunicazioni, con particolare riguardo alla transizione verso il 5G ed alla gestione dei big data.

Articolo 4
(Disposizioni in materia di infrastrutture e tecnologie critiche)

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.

Più in dettaglio:

- viene **ampliato** (comma 1) **il perimetro** dei **beni** che possono essere **inclusi nell'ambito di applicazione di tale 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 ri**compreso** il possibile **pregiudizio alla sicurezza e al funzionamento delle reti e degli impianti** e alla **continuità degli approvvigionamenti**;
- 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**. 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 (comma 2);
- 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 (medesimo comma 2).

Si ricorda in questa sede che, per salvaguardare gli assetti proprietari delle **società operanti in settori reputati strategici e di interesse nazionale**, il legislatore ha organicamente disciplinato, con il **decreto-legge 15 marzo 2012, n. 21 – come successivamente modificato nel tempo** – la materia dei **poteri speciali esercitabili dal Governo** anche per aderire alle indicazioni e alle censure sollevate in sede europea. Sono stati in particolare definiti, anche mediante il rinvio ad atti di normazione secondaria (DPCM), l'ambito oggettivo e soggettivo, la tipologia, le condizioni e le procedure di esercizio da parte dello Stato (in particolare, del Governo) dei suddetti poteri speciali. Si tratta di poteri esercitabili nei settori della difesa e della sicurezza nazionale, nonché di taluni

ambiti di attività definiti di **rilevanza strategica** nei settori dell'energia, dei trasporti e delle **comunicazioni**.

Per ulteriori approfondimenti sulla disciplina, si rinvia alla ricostruzione contenuta nel *focus* pubblicato sul portale della documentazione della Camera dei deputati.

Per quanto rileva ai fini del presente lavoro, si rammenta che:

- il **decreto-legge n. 148 del 2017** ha modificato ed esteso la disciplina dell'esercizio dei poteri speciali del Governo in ordine alla *governance* di società considerate strategiche; ha inoltre ampliato l'esercizio dei poteri speciali, applicabili nei settori dell'energia, dei trasporti e delle comunicazioni, al settore della cd. **alta intensità tecnologica**;
- successivamente il **decreto-legge n. 22 del 2019** ha introdotto disposizioni specifiche in tema di poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con **tecnologia 5G**;
- il **decreto-legge n. 64 del 2019** ha modificato le norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni. Il Consiglio dei ministri, nella riunione del 5 settembre 2019, ha deliberato l'esercizio dei poteri speciali ai sensi di tale provvedimento, con riferimento ad alcune operazioni riguardanti le comunicazioni elettroniche basate su tecnologia 5G e l'acquisizione di componenti ad alta intensità tecnologica. Tuttavia, stante la **mancata conversione** in legge, il provvedimento è decaduto il 9 settembre 2019. Si segnala inoltre che, nel corso dell'esame parlamentare del disegno di legge di conversione del decreto legge n. 75 del 2019 (A.S. 1460), è stato approvato un emendamento al medesimo disegno di legge con il quale si prevede la **sanatoria degli effetti** del decreto legge n. 64 del 2019. Per approfondimenti sulle disposizioni di tale ultimo decreto si rinvia al *dossier* predisposto dai servizi di Camera e Senato.

Come anticipato, l'**articolo 4** del decreto in esame modifica l'articolo 2 del decreto legge n. 21 del 2012, che disciplina i **poteri speciali inerenti agli attivi strategici nei settori dell'energia, dei trasporti e delle comunicazioni, nonché nei settori ad alta intensità tecnologica**.

In particolare, occorre rammentare che ai sensi dell'articolo 2 del decreto legge n. 21 del 2012 il Governo può:

- esercitare il **potere di veto** alle delibere, atti e operazioni che abbiano per effetto modifiche della titolarità, del controllo, della disponibilità o della destinazione degli attivi strategici, dando luogo a una situazione eccezionale, non disciplinata dalla normativa nazionale ed europea di settore, di minaccia di grave pregiudizio per gli interessi pubblici relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti (articolo 2, comma 3). L'esercizio del potere è assistito dall'obbligo, per la società, di fornire

al Governo una **informativa completa** su delibera, atto o operazione (articolo 2, comma 4);

- imporre **condizioni e impegni** diretti a garantire la tutela degli interessi essenziali dello Stato, in caso di acquisto da parte di un soggetto esterno all'Unione europea di partecipazioni in società che detengono gli attivi strategici (articolo 2, comma 6, primo periodo). L'esercizio del potere è assistito da un obbligo di notifica dell'acquisto di rilevanza tale da determinare l'insediamento stabile dell'acquirente in ragione dell'assunzione del controllo della società la cui partecipazione è oggetto dell'acquisto (articolo 2, comma 5);
- opporsi **all'acquisto** da parte di un soggetto esterno all'Unione europea di partecipazioni in società che detengono gli attivi strategici in casi eccezionali di rischio per la tutela dei predetti interessi, non eliminabili attraverso l'assunzione degli impegni (articolo 2, comma 6, secondo periodo). L'esercizio del potere è assistito da un obbligo di notifica dell'acquisto (articolo 2, comma 5).

Tali poteri speciali sono esercitati esclusivamente sulla base di **criteri oggettivi e non discriminatori** (articolo 2, comma 7), tenendo conto, in particolare, di elementi quali:

- la sussistenza di legami fra l'acquirente e Paesi terzi che non riconoscono i principi di democrazia o dello Stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale, desunti dalla natura delle loro alleanze, o hanno rapporti con organizzazioni criminali o terroristiche o con soggetti ad esse comunque collegati;
- l'idoneità dell'assetto risultante dall'atto giuridico o dall'operazione, tenuto conto anche delle modalità di finanziamento dell'acquisizione e della capacità economica, finanziaria, tecnica e organizzativa dell'acquirente, a garantire la sicurezza e la continuità degli approvvigionamenti, nonché il mantenimento, la sicurezza e l'operatività delle reti e degli impianti. Per le operazioni di acquisto di partecipazioni è valutato anche il pericolo per la sicurezza o per l'ordine pubblico.

Il decreto legge n. 148 del 2017 ha ampliato l'esercizio dei poteri speciali applicabili nei settori dell'energia, dei trasporti e delle comunicazioni, al settore della cd. alta intensità tecnologica (**articolo 2, comma 1-*ter* del decreto legge n. 21 del 2012**) affidando a uno o più **regolamenti**, adottati ai sensi dell'articolo 17, comma 1, della legge n. 400 del 1988, il compito di individuare, ai fini della verifica in ordine alla sussistenza di un pericolo per la sicurezza e l'ordine pubblico, i **settori ad alta intensità tecnologica.**

Tra di essi la norma annovera:

a) le infrastrutture critiche o sensibili, tra cui immagazzinamento e gestione dati, infrastrutture finanziarie;

b) tecnologie critiche, compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con potenziali applicazioni a doppio uso, la sicurezza in rete, la tecnologia spaziale o nucleare;

c) sicurezza dell'approvvigionamento di input critici;

d) accesso a informazioni sensibili o capacità di controllare le informazioni sensibili.

Tali regolamenti sono adottati su proposta del Ministro dell'economia e delle finanze, del Ministro dello sviluppo economico e del Ministro delle infrastrutture e dei trasporti, di concerto con il Ministro dell'interno, con il Ministro della difesa e con il Ministro degli affari esteri, oltre che con i Ministri competenti per settore, previo parere delle Commissioni parlamentari competenti.

L'articolo 4, comma 1 del decreto in esame integra il disposto del comma 1-*ter* sotto un **duplice profilo**.

In primo luogo 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.**

Viene poi ampliato l'oggetto delle richiamate norme regolamentari, per chiarire che esse individuano i **beni** e i **rapporti di rilevanza strategica per l'interesse nazionale –** i quali si pongono come **ulteriori** rispetto a quelli individuati con riferimento al sistema di difesa e sicurezza nazionale, nonché con riferimento ai settori dell'energia, dei trasporti e delle comunicazioni – nei **settori** individuati come **rilevanti per l'ordine pubblico e per la sicurezza** dalle **norme europee**, in particolare ai sensi dell'articolo 4, **paragrafo 1, del regolamento (UE) n. 452 del 2019**, **inclusi** i **settori ad alta intensità tecnologica**.

Tali ultimi settori restano dunque inclusi nell'ambito di applicazione dei regolamenti il cui contenuto, contestualmente, viene ampliato mediante l'inclusione di ulteriori situazioni che possono recare pregiudizio alla sicurezza e all'ordine pubblico.

Rinviando all'articolo 4, paragrafo 1, del **regolamento (UE) n. 452 del 2019**, viene inclusa una lista che amplia (con alcune intersezioni) quella già contenuta nell'articolo 2, comma 1-*ter* del decreto legge n. 21 del 2012.

In base alla norma europea, **nel determinare se un investimento estero diretto possa incidere sulla sicurezza o sull'ordine pubblico**, gli Stati membri e la Commissione **possono prendere in considerazione** i suoi effetti potenziali, tra l'altro, a livello di:

a) **infrastrutture critiche**, siano esse **fisiche o virtuali**, tra cui l'energia, i trasporti, l'acqua, la salute, le comunicazioni, i media, il

trattamento o l'archiviazione di dati, le infrastrutture aerospaziali, di difesa, elettorali o finanziarie, e le strutture sensibili, nonché gli investimenti in terreni e immobili fondamentali per l'utilizzo di tali infrastrutture;

b) **tecnologie critiche** e **prodotti a duplice uso**, tra cui l'**intelligenza artificiale**, la robotica, i semiconduttori, la **cibersicurezza**, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie;

c) **sicurezza dell'approvvigionamento di fattori produttivi critici**, tra cui l'energia e le materie prime, nonché la sicurezza alimentare;

d) **accesso a informazioni sensibili**, compresi i dati personali, o la capacità di controllare tali informazioni; o

e) **libertà e pluralismo dei media**.

I "prodotti a duplice uso" vengono definiti dall'articolo 2, punto 1, del regolamento (CE) n. 428 del 2009 come i prodotti, inclusi il *software* e le tecnologie, che possono avere un utilizzo sia civile sia militare. Essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari.

Il comma 2 dell'a**rticolo** in esame stabilisce che, **fino all'entrata in vigore delle norme secondarie** (regolamento da adottare ai sensi dell'articolo 2, comma 1-*ter*, del decreto legge n. 21 del 2012), è soggetto a **notifica** (di cui al comma 5 del medesimo articolo 2) **l'acquisto a qualsiasi titolo, da parte di un soggetto esterno all'Unione europea,** di partecipazioni in società che detengono beni e rapporti nei settori delle infrastrutture e delle tecnologie critiche, come definiti dal richiamato articolo 4, paragrafo 1, lettere a) e b), del regolamento (UE) n. 452 del 2019, di **rilevanza** tale da determinare l'insediamento stabile dell'acquirente, in ragione dell'assunzione del **controllo** della società la cui partecipazione è oggetto dell'acquisto, ai sensi dell'articolo 2359 del codice civile e del Testo Unico Finanziario – TUF (decreto legislativo n. 58 del 1998).

Il comma 2 prevede altresì che, a seguito della notifica, **il Governo possa esercitare i poteri speciali** previsti dalla normativa **per garantire la sicurezza e l'ordine pubblico**, mediante **l'imposizione di condizioni e impegni diretti a garantire la tutela degli interessi essenziali dello Stato** (articolo 2, comma 6, primo periodo, del decreto legge n. 21 del 2012) nonché **l'opposizione all'acquisto della partecipazione** (articolo 2, comma 6, secondo periodo, del decreto legge n. 21 del 2012). Tali poteri speciali sono esercitati esclusivamente sulla **base di criteri oggettivi e**

non discriminatori, tenendo conto, in particolare, degli elementi identificati dall'articolo 2, comma 7, del decreto legge n. 21 del 2012 esposto in precedente.

Al riguardo, si fa presente che l'ultima Relazione al Parlamento sull'esercizio dei poteri speciali aggiornata a fine 2018, afferma che è in corso di predisposizione il regolamento attuativo delle novità introdotte con il decreto-legge n. 148 del 2017, per individuare i settori ad alta intensità tecnologica, nonché la tipologia di atti o operazioni oggetto dell'esercizio dei poteri speciali.

Articolo 5
(Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica)

L'**articolo 5** dispone circa alcune **attribuzioni emergenziali** in capo al **Presidente del Consiglio,** in caso di **rischio grave o crisi di natura cibernetica**.

In particolare, 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 7-*bis*, comma 5, del decreto-legge n. 174 del 2015 prevede che il Comitato interministeriale per la sicurezza della Repubblica possa essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale.

Tale intervento disattivatore 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.

Tale attribuzione del Presidente del Consiglio è prevista operare allorché 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**.

Situazione di crisi cibernetica è - secondo la definizione reca dall'articolo 2, comma 1, lettera *o)* del DPCM del 17 febbraio 2017 - una "situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale".

Articolo 6
(Copertura finanziaria)

L'**articolo 1**, **comma 1**, reca la **quantificazione degli oneri** associati alle disposizioni dell'articolo 1, comma 19, e dell'articolo 2, commi 1 e 3, pari a:

- 3.200.000 euro per l'anno 2019,
- 6.495.000 euro per ciascuno degli anni dal 2020 al 2023,
- 4.395.000 euro annui a decorrere dall'anno 2024.

Si tratta, in particolare, degli **oneri** connessi alla realizzazione, l'allestimento e il funzionamento del **Centro di valutazione e certificazione nazionale** (**CVCN**), istituito presso il Ministero dello sviluppo economico ai sensi dell'articolo 1, comma 19, e delle spese per il relativo personale, alla cui assunzione il Ministero medesimo è autorizzato ai sensi dell'articolo 2, commi 1 e 3, del provvedimento.

Il comma 1 indica quindi le seguenti **coperture**:

a) quanto a 4.395.000 euro annui a decorrere dall'anno 2020, si dispone la corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2019-2021, nell'ambito del programma «**Fondi di riserva e speciali**» della missione «Fondi da ripartire» dello stato di previsione del MEF per l'anno 2019, allo scopo parzialmente utilizzando:
   - l'accantonamento relativo al Ministero dello sviluppo economico (Mise) quanto a euro 350.000 annui a decorrere dall'anno 2020
   - e l'accantonamento relativo al MEF quanto a euro 4.045.000 a decorrere dall'anno 2020;
b) quanto a euro 3.200.000 per l'anno 2019 e a euro 2.100.000 per ciascuno degli anni dal 2020 al 2023, mediante corrispondente utilizzo delle risorse del **Fondo** per il rilancio degli **investimenti delle Amministrazioni centrali dello Stato**, istituito dalla legge di bilancio per il 2019 (legge n. 145 del 2018), da imputare sulla quota parte del fondo attribuita al **Ministero dello sviluppo economico**.

   Si tratta del **Fondo finalizzato agli investimenti delle Amministrazioni centrali**, istituito e disciplinato dall'articolo 1, commi 95, 96, 98 e 105 della legge di bilancio 2019, con una dotazione complessiva di circa **43,6 miliardi** di euro per gli anni **dal 2019 al 2033**. In particolare, ai sensi del comma 95, il Fondo dispone di una dotazione iniziale di 740 milioni di euro per l'anno 2019, di 1.260 milioni di euro per l'anno 2020, di 1.600

milioni di euro per l'anno 2021, di 3.250 milioni di euro per ciascuno degli anni 2022 e 2023, di 3.300 milioni di euro per ciascuno degli anni dal 2024 al 2028 e di 3.400 milioni di euro per ciascuno degli anni dal 2029 al 2033. Le risorse sono genericamente finalizzate al rilancio degli investimenti delle Amministrazioni centrali dello Stato e allo sviluppo del Paese, tranne una quota parte – peraltro non quantificata – da destinare alla realizzazione, allo sviluppo e alla sicurezza di sistemi di trasporto pubblico di massa su sede propria (comma 96).
Per il **riparto** di tale fondo è stato presentato alle Commissioni parlamentari competenti, per il prescritto parere, l'A.G. n. 81. Tale decreto, che ha ottenuto parere favorevole con osservazioni il 29 maggio alla Camera e il 6 giugno al Senato, è ancora in attesa di pubblicazione in Gazzetta Ufficiale. Per approfondimenti, si veda il relativo dossier.
Nello schema di decreto citato, al **MISE** risultano **assegnati**, per gli anni che qui interessano, 111 milioni di euro per il 2019, 220 milioni di euro per il 2020, 269 milioni di euro per il 2021, 500 milioni di euro per il 2022 e 410 milioni di euro per il 2023.
Nella Relazione tecnica del provvedimento in esame si precisa, inoltre, che la quota parte del MISE che viene utilizzata a copertura è **quella che è stata assegnata all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione** con decreto del Ministero dell'economia e delle finanze in corso di definizione.

Si ricorda, infine, che il comma 105 della legge di bilancio 2019 prevede che, sulla base dei dati di monitoraggio, nonché delle risultanze dell'ultimo Rendiconto generale dello Stato, ciascun Ministero, entro il 15 settembre di ogni anno, illustri lo stato dei rispettivi investimenti e lo stato di utilizzo dei finanziamenti, con indicazione delle principali criticità riscontrate nell'attuazione degli interventi, nell'ambito della Relazione annuale sullo stato di avanzamento degli interventi finanziati con le risorse del Fondo per il finanziamento degli investimenti e lo sviluppo infrastrutturale del Paese (art. 1, comma 1075, legge n. 205 del 2017).

Il **comma 2** autorizza il Ministro dell'economia e delle finanze ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Articolo 7
(Entrata in vigore)

L'articolo dispone che il decreto-legge entri in vigore il giorno successivo a quello della sua pubblicazione in Gazzetta Ufficiale.

Il decreto-legge è dunque vigente dal 22 settembre 2019.