deputati PD

Ufficio Documentazione e Studi

Dossier n. 33

14 Novembre 2019

Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica

CYBERSICUREZZA

*Lo **"spazio cibernetico"** rappresenta un nuovo dominio operativo di natura artificiale – **di importanza strategica per lo sviluppo economico, sociale e culturale** – trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale), nel quale gli esseri umani agiscono. In questa prospettiva, il dispiegamento della **tecnologia di rete 5G** di quinta generazione costituirà un fattore qualificante per lo sviluppo di molti servizi digitali e le relative reti 5G saranno l'infrastruttura portante non solo di nuovi servizi di comunicazione elettronica, ma anche di una vasta gamma di servizi essenziali, quali l'energia, i trasporti, i servizi bancari e sanitari, i sistemi di controllo industriale[1].*

*Il decreto-legge n. 105 del 2019, in materia di **perimetro di sicurezza nazionale cibernetica**, persegue diversi obiettivi, il principale è quello di **garantire, per le finalità di sicurezza nazionale, l'integrità e la sicurezza delle reti**, in particolare quelli inerenti ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e dei dati che vi transitano. Inoltre configura **un sistema di organi, procedure e misure**, al fine di consentire una efficace valutazione sotto il profilo tecnico della sicurezza degli apparati e dei prodotti, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.*

*Ulteriore obiettivo dell'intervento legislativo è quello di disporre di più **idonei strumenti d'immediato intervento** che consentano di affrontare con la massima efficacia e tempestività eventuali **situazioni di emergenza in ambito cibernetico**.*

[1] "Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa *cyber*", dossier n. 83, Servizio Studi della Camera dei deputati, 24 settembre 2019, XVIII legislatura.

PREMESSA

Il decreto-legge 21 settembre 2019, n. 105 è stato esaminato dalla Camera dei deputati in prima lettura e poi trasmesso al Senato della Repubblica, con modificazioni, il 24 ottobre 2019. Nel corso del successivo esame al Senato sono state apportate ulteriori modificazioni rispetto al testo approvato dalla Camera[2].

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

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

Ulteriori modifiche hanno riguardato specifiche previsioni del testo, per i quali si rinvia ai dossier del Servizio Studi del Senato e della Camera.

*Per maggiori approfondimenti si rinvia ai lavori parlamentari del disegno di legge "*Conversione in legge del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*" AC 2100-B (relatori Emanuele Fiano del PD per la I Commissione Affari Costituzionali e Emanuele Scagliusi del M5S per la IX Commissione Trasporti) e ai relativi dossier dei Servizi Studi della Camera e del Senato.*

ISTITUZIONE DEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Si istituisce il **perimetro di sicurezza nazionale cibernetica**, al fine di garantire 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**.

In particolare, si fa riferimento **ad amministrazioni pubbliche**, nonché ad **enti e operatori nazionali, pubblici e privati aventi una sede nel territorio nazionale** 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**.

L'individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica è rimandata ad un decreto del Presidente del Consiglio dei ministri (**DPCM**), adottato su

[2] In particolare, sono state oggetto di modifica le disposizioni di cui all'articolo 1, commi 6, 7, 9 e 19 e di cui all'articolo 6, comma 1 del decreto-legge.

proposta del **Comitato interministeriale per la sicurezza della Repubblica (CISR)**[3], entro quattro mesi dalla data di entrata in vigore della legge di conversione del decreto-legge in esame.

L'individuazione avviene **sulla base di un criterio di gradualità**, tenendo conto **dell'entità del pregiudizio per la sicurezza nazionale.**

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

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

Tali elenchi vengono trasmessi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico, che li inoltrano al **Dipartimento delle informazioni per la sicurezza** (DIS), anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica[4]; all'organo per la regolarità e sicurezza dei servizi di telecomunicazione presso il Ministero dell'interno.

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")[5].

Per ulteriori approfondimenti sull'evoluzione della normativa nazionale e dell'Unione europea in materia sicurezza cibernetica si veda il dossier n. 83 del Servizio studi della Camera del 24 settembre 2019 Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber.

PROCEDURE DI SEGNALAZIONE DEGLI INCIDENTI E MISURE DI SICUREZZA

Ad un altro DPCM è demandata la determinazione sia delle procedure di notifica degli **incidenti** prodottisi **su reti, sistemi informativi e sistemi informatici** inclusi nel perimetro di sicurezza nazionale cibernetica, sia **le misure** volte a garantirne elevati livelli **di**

[3] 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.

[4] il **Nucleo per la sicurezza cibernetica**, che opera all'interno del Dipartimento delle informazioni per la sicurezza (DIS) con il compito di promuovere 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 il punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'Unione europea, altre organizzazioni internazionali ed altri Stati.

[5] 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**).

sicurezza, tenendo conto degli **standard definiti a livello internazionale e dell'Unione europea.**

Le amministrazioni pubbliche, nonché gli enti oppure gli operatori nazionali, pubblici e privati devono **notificare l'incidente al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT italiano)**[6]. Il CSIRT procede poi a inoltrare tempestivamente tali notifiche **al Dipartimento delle informazioni della sicurezza (DIS).**

Per quanto riguarda **le misure di sicurezza esse devono assicurare elevati livelli di sicurezza** delle reti, sistemi informativi e sistemi informatici rientranti nel perimetro di sicurezza nazionale cibernetica, tenendo conto degli **standard definiti a livello internazionale** e **dell'Unione europea**. 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 interventi su 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).

Il provvedimento determina i **soggetti ministeriali preposti all'elaborazione delle misure di sicurezza**, e stabilisce **l'aggiornamento almeno biennale** di quanto previsto dai DPCM.

Gli schemi dei decreti, previsti dal provvedimento, sono trasmessi alle Camere per l'espressione del **parere delle Commissioni parlamentari** competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il provvedimento può essere comunque adottato.

Riassumendo l'elaborazione delle misure di sicurezza sopramenzionate è realizzata, secondo l'ambito di competenza, dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio. È prevista l'intesa con il Ministero della Difesa, il Ministero dell'Interno, il Ministero dell'Economia e delle finanze, il DIS.

[6] 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 UE n. 1148 del 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione. Secondo questa direttiva, ogni Stato membro è chiamato a designare un "Gruppo di intervento per la sicurezza informatica in caso di incidente". Il CSIRT italiano ha compiti di natura tecnica finalizzati a supportare la p.a., i cittadini e le imprese attraverso azioni di sensibilizzazione, prevenzione e coordinamento della risposta ad eventi cibernetici su vasta scala.

DETERMINAZIONI DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI IN CASO DI CRISI DI NATURA CIBERNETICA

Alcune **attribuzioni emergenziali** sono assegnate alla Presidenza del Consiglio, in caso di rischio grave o crisi di natura cibernetica. In particolare, si prevede che **il Presidente del Consiglio** – su deliberazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) – possa **disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati** nelle reti, nei sistemi o per l'espletamento dei servizi posti nel perimetro di sicurezza nazionale cibernetica. Siffatto intervento **"disattivatore"** deve risultare indispensabile in caso di grave e imminente rischio per la sicurezza nazionale e realizzarsi per il tempo strettamente necessario all'eliminazione dello specifico fattore di rischio o alla sua mitigazione, **secondo un criterio di proporzionalità**. Il Presidente del Consiglio è tenuto a informare il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) delle misure disposte.

ACQUISIZIONE DI SISTEMI ICT (*INFORMATION, AND COMMUNICATION TECHNOLOGY*)

Si rimette ad **un regolamento di esecuzione la definizione delle procedure, delle modalità e dei termini** alle quali si attengono i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica ovvero le centrali di committenza alle quali essi fanno ricorso[7] quando intendano procedere all'**affidamento di forniture di beni, sistemi e servizi ICT**, destinati a essere impiegati sulle reti e sui sistemi informativi e per l'espletamento dei servizi informatici di pertinenza[8]

In particolare sono tenuti a dare **comunicazione al Centro di valutazione e certificazione nazionale (CVCN)[9] 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, **impone condizioni e test di hardware e software**, da compiere anche in collaborazione con i soggetti rientranti nel perimetro. In tale ipotesi, i relativi bandi di gara e contratti sono **integrati con clausole** che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.

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 può procedere nell'ambito delle risorse umane e finanziarie disponibili, senza nuovi o maggiori oneri a carico della finanza pubblica, **attraverso un proprio Centro di valutazione**. Una modifica approvata dal Senato introduce **analoga previsione per il Ministero dell'interno**, che così può avvalersi anch'esso di **un proprio Centro di valutazione**.

---

[7] Ai sensi dell'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208.

[8] A seguito di una modifica introdotta nel corso dell'esame in sede referente **non si tratterà di tutti i beni**, sistemi e servizi ICT potenzialmente oggetto di acquisto, ma solo dei beni **appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri.** Il decreto dovrà essere emanato entro 10 mesi dall'entrata in vigore della norma di conversione del decreto.

[9] Il **Centro di valutazione e certificazione nazionale (CVCN)** 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 (ISCTI)**.

Altra modifica approvata dal Senato specifica che il **Centro di valutazione del Ministero della difesa e quello del Ministero dell'interno** devo anch'essi essere **accreditati presso il CVCN** e sono tenuti a impiegare metodologie di verifica e test quali definite del CVCN.

Per effetto di alcuni emendamenti, introdotto un **obbligo di informativa** di quei Centri di valutazione con il CVCN, le ipotesi di esenzione dall'obbligo di comunicazione e i **casi di deroga** stabiliti con riguardo alle **forniture per le quali sia indispensabile procedere in sede estera**.

Per le reti, i sistemi informativi e i servizi informatici connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, **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, dalle 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.

COMPITI DEL CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE (CVCN)

Il decreto-legge individua alcuni **compiti del Centro di valutazione e certificazione nazionale (CVCN)**, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, **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 CVCN può **effettuare verifiche** preliminari ed **imporre condizioni e test** [10]di hardware e software secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Per le proprie attività il CVCN si avvale anche di laboratori che provvede ad accreditare. Un DPCM fisserà i criteri per l'accreditamento[11]. Una modifica approvata dal Senato aggiunge la previsione che con il medesimo atto siano altresì stabiliti i **"raccordi"**, ivi compresi i contenuti, le modalità e i termini delle comunicazioni **tra il CVCN e i predetti laboratori**, nonché tra il medesimo **CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa**. Questo, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la **convergenza e la non duplicazione delle valutazioni** (in presenza di medesimi condizioni e livelli di rischio)

Con una modifica approvata nel corso dell'esame in sede referente, alla Camera, è stato raggiunto **un buon compromesso** tra le esigenze di sicurezza e di verifica da parte degli organi dello Stato e gli operatori che devono rispondere a queste richieste entro i termini di legge (45 giorni, prorogabili una sola volta di 15 giorni) e sostanzialmente con il **silenzio-assenso**. Decorso il predetto termine senza che il CVCN si sia pronunciato, i soggetti interessati possono proseguire nella procedura di affidamento.

[10] Una modifica **introdotta dal Senato** inserisce, tra i compiti, anche **la definizione di metodologie di verifica e di test.**

[11] Tale DPCM, da emanare entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto-legge, è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR).

OBBLIGHI PER ALCUNI SPECIFICI OPERATORI

Previsti una serie **di obblighi riguardanti l'osservanza delle misure di sicurezza e la notifica degli incidenti** aventi impatto su reti, sistemi informativi e sistemi informatici del perimetro di sicurezza nazionale cibernetica, per gli **operatori dei servizi essenziali**, i **fornitori di servizi digitali** e le **imprese** che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica.

In particolare, la disposizione prevede che tali soggetti osservino le misure di sicurezza previste dalle disposizioni vigenti[12], allorché esse siano **"di livello almeno equivalente"** a quelle adottate con l'apposito DPCM attuativo del 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, devono essere definite:

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[13];

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[14]** per il settore energia, sotto-settori energia elettrica, gas e petrolio, e per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD[15], nonché per i servizi digitali) si raccordano, ove necessario, con le autorità NIS competenti[16].

La notifica degli incidenti è soggetta ad una "catena" di trasmissione tra le autorità competenti in materia di sicurezza cibernetica.

DISPOSIZIONI SANZIONATORIE

Il decreto-legge prevede **un articolato sistema sanzionatorio**. Più nel dettaglio, punisce con la pena della **reclusione da uno a tre anni** coloro che, allo scopo di ostacolare o

---

[12] D.lgs. n. 65 del 2018 e d.lgs. n. 259 del 2003.

[13] Di cui all'articolo 29 del D.lgs. n. 82 del 2005 (codice dell'amministrazione digitale).

[14] L'acronimo sta per *Network and Information Security*.

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

[16] Le autorità NIS competenti, di cui all'articolo 7 del D.lgs. n. 65 del 2018 (adottato in attuazione della direttiva UE 2016/1148, c.d. direttiva NIS *Network and Information Security*) 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.

condizionare l'espletamento dei procedimenti di compilazione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici e quelli relativi all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti e sui sistemi informativi o delle attività ispettive e di vigilanza da parte della Presidenza del Consiglio dei ministri e del Mise: **forniscono informazioni, dati o fatti non rispondenti al vero**; **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.**

Sono disciplinati inoltre una serie di illeciti amministrativi (per i dettagli si rinvia al comma 9 dell'articolo 9 del disegno di legge di conversione del decreto-legge).

Vengono **individuate le autorità competenti all'accertamento delle violazioni e all'irrogazione delle sanzioni previste**. Si tratta: della **Presidenza del Consiglio dei ministri,** per le amministrazioni pubbliche, gli enti e gli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale nonché per i soggetti qualificati o accreditati per fornire servizi fiduciari o attività di gestore di posta elettronica certificata o di gestore dell'identità digitale[17]; del **Ministero dello Sviluppo economico**, per gli operatori nazionali privati inclusi nel perimetro di sicurezza nazionale.

Per l'accertamento delle violazioni e l'irrogazione delle sanzioni **si applica il procedimento disciplinato dalla legge 24 novembre 1981, n. 689.**

Per la violazione delle disposizioni**, i dipendenti** delle amministrazioni pubbliche, degli enti e degli operatori nazionali pubblici inclusi nel perimetro di sicurezza nazionale **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.

COORDINAMENTO E RACCORDI ORGANIZZATIVI

Si affida al **Presidente del Consiglio** dei ministri il **coordinamento** della "coerente attuazione" delle disposizioni del decreto-legge che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del **DIS** che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni e con i soggetti coinvolti. Il Presidente del Consiglio dei ministri è altresì tenuto a trasmettere **alle Camere una relazione sulle attività** svolte.

La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni attinenti al perimetro di sicurezza cibernetica, può **avvalersi dell'Agenzia per l'Italia Digitale (AGID)**, che 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.

Si 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.

[17] In base all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, recante il codice dell'amministrazione digitale.

ASSUNZIONI DEL PERSONALE DEL CVCN

Il Ministero dello sviluppo economico (MISE) è autorizzato ad assumere a tempo indeterminato, con incremento della vigente dotazione organica nel limite delle unità eccedenti, in aggiunta alle ordinarie facoltà assunzionali, un contingente massimo di 77 unità di personale per lo svolgimento delle funzioni del Centro di valutazione e certificazione nazionale (CVCN), prevedendo che fino al completamento delle procedure di assunzione, possa avvalersi, a tale scopo, con alcune eccezioni, di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni.

ASSUNZIONI PRESSO LA PRESIDENZA DEL CONSIGLIO

La Presidenza del Consiglio è autorizzata ad assumere fino a dieci unità di personale non dirigenziale, per lo svolgimento delle funzioni in materia di digitalizzazione, avvalendosi, nelle more di tali assunzioni, di esperti, consulenti o di personale non dirigenziale di altre amministrazioni pubbliche. Essi debbono essere in possesso di particolare e comprovata specializzazione in materia informatica.

RETI DI TELECOMUNICAZIONE ELETTRONICA A BANDA LARGA CON TECNOLOGIA 5G

La legge 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.** Si stabilisce, pertanto, che **le disposizioni del decreto-legge 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 poteri speciali n. 21 del 2012, 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**.

Con un nuovo regolamento viene deciso che **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 ossia il CVCN e il Centro di valutazione del Ministero della difesa.

Fissata anche 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**, al fine di risolvere le vulnerabilità accertate.

ESERCIZIO DEI POTERI SPECIALI DEL GOVERNO (*GOLDEN POWER*)

Con un emendamento presentato dal Governo, durante l'esame in Commissione alla Camera, sono state inserite una serie di disposizioni[18] in materia di esercizio dei **poteri speciali del Governo** nei settori della **difesa** e della **sicurezza nazionale**, nonché per le attività di rilevanza strategica nei settori dell'**energia**, dei **trasporti** e delle **comunicazioni** (cd. ***golden power***).[19]

Si 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** nonché **l'opposizione all'acquisto della partecipazione.** Tali poteri speciali sono esercitati esclusivamente sulla **base di criteri oggettivi e non discriminatori.**

In sintesi:

- viene in generale allungato il termine **per l'esercizio dei poteri speciali** da parte del Governo, con contestuale **arricchimento** dell'informativa resa dalle imprese detentrici degli *asset* strategici;
- si amplia l'oggetto di alcuni **poteri speciali**;
- sono modificati e integrati gli **obblighi di notifica** finalizzati all'esercizio dei poteri speciali;
- viene modificata la **disciplina dei poteri speciali in tema di tecnologie 5G**, per rendere il procedimento sostanzialmente simmetrico rispetto a quello per l'esercizio dei poteri speciali nei settori della difesa e della sicurezza nazionale;
- viene ridefinito il concetto di "**soggetto esterno all'Unione europea**" e sono precisati i criteri per determinare se un **investimento estero** è suscettibile di incidere sulla sicurezza o sull'ordine pubblico.

In particolare, a differenza del decreto-legge n. 64, l'emendamento:

- introduce **ulteriori circostanze** che il **Governo può tenere in considerazione,** per l'esercizio dei **poteri speciali**, nel caso in cui l'acquirente di partecipazioni rilevanti sia un **soggetto esterno all'Unione europea**;
- sottopone all'obbligo di notifica anche l'**acquisizione, a qualsiasi titolo** – **in luogo del solo acquisto** – **di beni o servizi** relativi alle reti 5G, quando posti in essere con **soggetti esterni all'Unione europea**;

[18] Si tratta in parte di norme analoghe a quelle contenute nel decreto-legge n. 64 del 2019, successivamente decaduto, con una serie significativa di modifiche ed integrazioni. L'articolo aggiuntivo è stato valutato ammissibile dalle Presidenze delle Commissioni riunite I e IX, nella seduta del 16 ottobre 2019, in quanto riconducibile alle materie trattate dal decreto-legge in esame, ed in particolare dagli articoli 3 e 4.

[19] Si rinvia per approfondire il tema della *golden power* al dossier "Elementi per l'esame in Assemblea" del provvedimento.

- consente di aggiornare i **regolamenti che individuano gli attivi di rilevanza strategica** tramite **decreti del Presidente del Consiglio dei ministri**, in luogo di decreti del Presidente della Repubblica anche in deroga alle procedure richieste dalla legge n. 400 del 1988;
- viene **semplificata** la procedura per l'espressione del **parere delle Commissioni parlamentari competenti**;
- disciplina la **notifica** riguardante delibere, atti e operazioni relativi **a specifici *asset* di rilevanza strategica per l'interesse nazionale** nei settori dei trasporti, dell'energia e delle comunicazioni, in presenza di condizioni particolari relative alla **provenienza dell'acquirente** ovvero agli **effetti delle operazioni** compiute.

Una norma **impone alle autorità amministrative di settore di collaborare fra loro**, anche attraverso lo scambio di informazioni, al fine di agevolare l'esercizio dei poteri speciali. Si tratta di: Banca d'Italia, Commissione nazionale per le società e la borsa (CONSOB), Commissione di vigilanza sui fondi pensione (COVIP), Istituto per la vigilanza sulle assicurazioni (IVASS), Autorità di regolazione dei trasporti (ART), Autorità garante della concorrenza e del mercato (AGCM), Autorità per le garanzie nelle comunicazioni (Agcom), Autorità di regolazione per energia reti e ambiente (ARERA) e il **Gruppo di coordinamento** costituito ai sensi dell'articolo 3 del decreto del Presidente del Consiglio dei ministri del 6 agosto 2014; a tale Gruppo le altre autorità non possano opporre il segreto d'ufficio, esclusivamente per le finalità di agevolare l'esercizio dei poteri speciali. Il **Gruppo di coordinamento** è presieduto dal Segretario generale della Presidenza del Consiglio dei ministri o dal Vicesegretario delegato ed è composto dai responsabili di specifici uffici dei ministeri o da altri designati dai rispettivi ministri interessati.

Con un'altra disposizione si coordina l'esercizio dei **poteri speciali** con i **procedimenti** disciplinati dalle **norme europee** (**Reg. 2019/452/UE**) sul **controllo degli investimenti esteri diretti nell'Unione**, disciplinando il dialogo tra autorità nazionali e Commissione europea.È fatta salva la **possibilità di esercitare i poteri speciali** anche prima del ricevimento del parere della Commissione o delle osservazioni degli Stati membri, nei casi in cui la tutela della sicurezza nazionale o dell'ordine pubblico richiedano l'adozione di una **decisione immediata** ai sensi del medesimo regolamento.

Viene infine stabilito che presso la **Presidenza del Consiglio dei Ministri** sia istituito il **punto di contatto per l'attuazione del regolamento sugli investimenti esteri diretti.**