concernente l'attività che si intende svolgere nel territorio della Repubblica. L'autorizzazione è rilasciata dalla Consob, sentita la Banca d'Italia.

7. La Consob, sentita la Banca d'Italia, può indicare, in via generale, i servizi e le attività che, ai sensi del comma 6, le imprese di paesi terzi diverse dalle banche non possono prestare nel territorio della Repubblica senza stabilimento di succursali.»

«Art. 29-*ter* (*Banche di paesi terzi*). — 1. Nel caso in cui sia previsto lo svolgimento di servizi o attività di investimento, con o senza servizi accessori, lo stabilimento in Italia di succursali da parte di banche di paesi terzi è autorizzato dalla Banca d'Italia, sentita la Consob, al ricorrere delle condizioni di cui all'articolo 28, comma 1. Resta ferma l'applicazione degli articoli 13, 14, comma 4, e 15, comma 4, del T.U. bancario.

2. L'autorizzazione è negata se non risulta garantita la capacità della succursale della banca di paesi terzi di rispettare gli obblighi alla stessa applicabili ai sensi del presente decreto o contenuti in atti dell'Unione europea direttamente applicabili.

3. Le banche di paesi terzi possono prestare servizi e attività di investimento, con o senza servizi accessori, a clienti al dettaglio o a clienti professionali su richiesta come individuati ai sensi dell'articolo 6, comma 2-*quinquies*, lettera *b)*, e comma 2-*sexies*, lettera *b)*, esclusivamente mediante stabilimento di succursali nel territorio della Repubblica.

4. La Banca d'Italia, sentita la Consob, può disciplinare le condizioni per il rilascio dell'autorizzazione allo svolgimento dei servizi e delle attività di cui ai commi 1 e 6.

5. Alla prestazione in Italia di servizi e attività di investimento, con o senza servizi accessori, in regime di libera prestazione di servizi nei confronti di controparti qualificate o di clienti professionali come individuati ai sensi dell'articolo 6, comma 2-*quinquies*, lettera *a)*, e comma 2-*sexies*, lettera *a)*, del presente decreto da parte di banche di paesi terzi si applicano le disposizioni del Titolo VIII del regolamento (UE) n. 600/2014.

6. Le banche di paesi terzi possono prestare servizi e attività di investimento, con o senza servizi accessori, a controparti qualificate o a clienti professionali come individuati ai sensi dell'articolo 6, comma 2-*quinquies*, lettera *a)*, e comma 2-*sexies*, lettera *a)*, del presente decreto anche senza stabilimento di succursali nel territorio della Repubblica, in mancanza di una decisione della Commissione europea a norma dell'articolo 47, paragrafo 1, del regolamento (UE) n. 600/2014, oppure ove tale decisione non sia più vigente, sempreché ricorrano le condizioni previste dall'articolo 28, comma 1, lettere *b)*, *c)*, *d)* ed *e)*, e venga presentato un programma concernente l'attività che si intende svolgere nel territorio della Repubblica. L'autorizzazione è rilasciata dalla Banca d'Italia, sentita la Consob.

7. La Banca d'Italia, sentita la Consob, può indicare, in via generale, i servizi e le attività che le banche di paesi terzi, ai sensi del comma 6, non possono prestare nel territorio della Repubblica senza stabilimento di succursali.».

— Per i riferimenti del regolamento (UE) n. 575/2013, si veda nelle note all'articolo 10.

— La direttiva 2013/36/UE del Parlamento europeo e del Consiglio, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE, è pubblicata nella G.U.U.E. 27 giugno 2013, n. L 176.

— Per i riferimenti della direttiva 2014/59/UE, si veda nelle note all'articolo 11.

— Il regolamento (UE) n. 1024/2013 del Consiglio, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi, è pubblicato nella G.U.U.E. 29 ottobre 2013, n. L 287.

— Il regolamento (UE) n. 806/2014 del Parlamento europeo e del Consiglio, che fissa norme e una procedura uniformi per la risoluzione degli enti creditizi e di talune imprese di investimento nel quadro del meccanismo di risoluzione unico e del Fondo di risoluzione unico e che modifica il regolamento (UE) n. 1093/2010, è pubblicato nella G.U.U.E. 30 luglio 2014, n. L 225.

— Per i riferimenti normativi del decreto legislativo 16 novembre 2015, n. 180, si veda nelle note all'articolo 11.

— La direttiva 2014/65/UE del Parlamento europeo e del Consiglio, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE (rifusione) (Testo rilevante ai fini del *SEE)*, è pubblicata nella G.U.U.E. 12 giugno 2014, n. L 173.

— Il regolamento (UE) 15 maggio 2014, n. 600/2014 del Parlamento europeo e del Consiglio, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 (Testo rilevante ai fini del *SEE)*, è pubblicato nella G.U.U.E. 12 giugno 2014, n. 173.

— Per i riferimenti del titolo VIII del citato decreto legislativo 1° gennaio 1993, n. 385, si veda nelle note all'articolo 10.

— Per i riferimenti del titolo II della parte V del citato decreto legislativo 24 febbraio 1998, n. 58, si veda nelle note all'articolo 26.

*Note all'art. 28:*

— La direttiva (UE) 2019/1159 del Parlamento europeo e del Consiglio, recante modifica della direttiva 2008/106/CE concernente i requisiti minimi di formazione per la gente di mare e che abroga la direttiva 2005/45/CE riguardante il reciproco riconoscimento dei certificati rilasciati dagli Stati membri alla gente di mare (Testo rilevante ai fini del *SEE)*, è pubblicata nella G.U.U.E. 12 luglio 2019, n. L 188.

— Per il testo dell'articolo 32 della citata legge 24 dicembre 2012, n. 234, si veda nelle note all'articolo 1.

— La direttiva 2018/106/CE del Parlamento europeo e del Consiglio, concernente i requisiti minimi di formazione per la gente di mare (rifusione) (Testo rilevante ai fini del *SEE)*, è pubblicata nella G.U.U.E. 3 dicembre 2008, n. L 323.

*Note all'art. 29:*

— La direttiva (UE) 2019/1151 del Parlamento europeo e del Consiglio, recante modifica della direttiva (UE) 2017/1132 per quanto concerne l'uso di strumenti e processi digitali nel diritto societario (Testo rilevante ai fini del *SEE)*, è pubblicata nella G.U.U.E. 17 luglio 2019, n. L 186.

— Per il testo dell'articolo 32 della citata legge 24 dicembre 2012, n. 234, si veda nelle note all'articolo 1.

**21G00063**

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 5 febbraio 2021, n. **54**.

**Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.**

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87, quinto comma, della Costituzione;

Visto l'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri;

Visto il decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e in particolare l'articolo 1, comma 6;

Visto il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

Visto il decreto del Ministro delle comunicazioni 15 febbraio 2006, recante individuazioni delle prestazioni, eseguite dal Ministero delle comunicazioni per conto terzi, ai sensi dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366, pubblicato nella *Gazzetta Ufficiale* n. 82 del 7 aprile 2006;

Visto l'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale;

Vista la legge 24 novembre 1981, n. 689, recante modifiche al sistema penale;

Vista la legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 7 agosto 2020;

Udito il parere del Consiglio di Stato n. 1664/2020 espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 20 ottobre 2020;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 29 gennaio 2021;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro dello sviluppo economico, di concerto con i Ministri dell'interno, della difesa, dell'economia e delle finanze e per l'innovazione tecnologica e la digitalizzazione;

EMANA
il seguente regolamento:

## *Capo I*
## DISPOSIZIONI GENERALI

### Art. 1.
### *Definizioni*

1. Ai fini del presente decreto si intende per:

*a)* decreto-legge: il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

*b)* perimetro: il perimetro di sicurezza nazionale cibernetica istituito ai sensi dell'articolo 1, comma 1, del decreto-legge;

*c)* DPCM: il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante il regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge;

*d)* soggetti inclusi nel perimetro: i soggetti di cui all'articolo 1, comma 2, lettera *a)*, del decreto-legge individuati sulla base dei criteri di cui all'articolo 4 del DPCM;

*e)* compromissione: la perdita di sicurezza o di efficacia dello svolgimento di una funzione essenziale dello Stato o di un servizio essenziale, connessa al malfunzionamento, all'interruzione, anche parziali, ovvero all'utilizzo improprio di reti, sistemi informativi e servizi informatici;

*f)* incidente: ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici;

*g)* analisi del rischio: un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità, sulla sicurezza o sulla efficacia della funzione essenziale o del servizio essenziale, e conseguentemente di trattare tale rischio individuando ed implementando idonee misure di sicurezza;

*h)* rete, sistema informativo:

1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera *dd)*, del decreto legislativo 1° agosto 2003, n. 259;

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, ivi inclusi i sistemi di controllo industriale;

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, compresi i programmi di cui al numero 2);

*i)* servizio informatico: un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di *cloud computing* di cui all'articolo 3, comma 1, lettera *aa)*, del decreto legislativo 18 maggio 2018, n. 65;

*l)* categorie: tipologie di beni, sistemi o servizi ICT destinati ad essere impiegati sui beni ICT di cui all'elenco dell'articolo 7 del DPCM, individuate sulla base di criteri tecnici, la cui acquisizione è subordinata alla valutazione del CVCN;

*m)* oggetto della fornitura: bene, sistema o servizio ICT, appartenente alle categorie, che il soggetto incluso nel perimetro intende acquisire;

*n)* CVCN: il Centro di Valutazione e Certificazione nazionale, istituito presso il Ministero dello sviluppo economico, di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge;

*o)* CV: i centri di valutazione del Ministero dell'interno e del Ministero della difesa di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge;

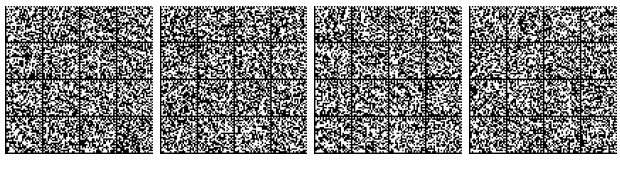
*p)* LAP: laboratorio accreditato di prova, indipendente dai soggetti inclusi nel perimetro e dai fornitori, che ha ottenuto l'accreditamento dal CVCN ai sensi dell'articolo 1, comma 7 del decreto-legge;

*q)* oggetto della valutazione: l'oggetto della fornitura di beni, sistemi o servizi ICT, sottoposto al procedimento di valutazione da parte del CVCN o dei CV;

*r)* centrali di committenza: Consip S.p.A. e i soggetti aggregatori ai fini della realizzazione degli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, nonché la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, nell'ambito individuato dall'articolo 31, comma 5, del decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120;

*s)* fornitore: persona fisica o giuridica che fornisce l'oggetto della fornitura di beni, sistemi o servizi ICT, destinato alle reti, ai sistemi informativi e ai servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge;





*t)* evidenze: documenti, registrazioni, dati, constatazioni, dichiarazioni di fatti, reportistica, attività, procedure, o altre informazioni utili ad attestare l'adempimento degli obblighi previsti dal decreto-legge;

*u)* verifica: attività di analisi e controllo documentale delle evidenze al fine di accertare l'adempimento degli obblighi previsti dal decreto-legge;

*v)* ispezione: attività di tipo ricognitivo e valutativo che si articola nell'analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto utili ad accertare l'adempimento degli obblighi previsti dal decreto-legge;

*z)* autorità competenti: le autorità che, ai sensi dell'articolo 1, comma 6, lettera *c)*, del decreto-legge, dispongono ed effettuano verifiche e ispezioni;

*aa)* personale incaricato: il personale incaricato dalle Autorità competenti dello svolgimento delle verifiche e delle ispezioni.

Art. 2.

*Oggetto*

1. Il presente decreto, in attuazione dell'articolo 1, comma 6, lettere *a)*, *b)* e *c)*, del decreto-legge, definisce:

*a)* le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del CVCN e dei CV, ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri di cui alla lettera *b)* del presente comma, fatti salvi i casi di deroga di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge;

*b)* i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione di cui alla lettera *a)*;

*c)* le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

*Capo II*

PROCEDURA DI VALUTAZIONE DEL CVCN E DEI CV

Art. 3.

*Comunicazione di affidamento*

1. I soggetti inclusi nel perimetro, prima dell'avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge, anche nel caso in cui tali procedure siano espletate attraverso le centrali di committenza, ne danno comunicazione al CVCN o ai CV.

2. La comunicazione è trasmessa in via telematica al CVCN o ai CV per le valutazioni di rispettiva competenza del CVCN o dei CV. I dati contenuti nelle comunicazioni sono raccolti in archivi informatici istituiti presso le Amministrazioni nelle quali operano il CVCN e i CV, con risorse disponibili a legislazione vigente.

3. La comunicazione di cui al comma 1, oltre ai dati identificativi del soggetto incluso nel perimetro, contiene i seguenti elementi:

*a)* la descrizione generale dell'oggetto della fornitura;

*b)* l'impiego, ovvero la destinazione d'uso dell'oggetto della fornitura nell'ambito dei beni ICT di cui all'articolo 7 del DPCM;

*c)* la categoria di appartenenza dell'oggetto della fornitura;

*d)* le informazioni e i servizi che l'oggetto della fornitura deve trattare e le relative modalità di gestione;

*e)* le informazioni relative all'eventuale acquisizione mediante gli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208.

4. In aggiunta agli elementi di cui al comma 3, la comunicazione include il documento di analisi del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. Il documento contiene la descrizione dei seguenti elementi:

*a)* l'ambiente operativo dell'ambito di impiego specificando:

1. i componenti con i quali l'oggetto della fornitura interagisce e le configurazioni di tali componenti;

2. le eventuali misure di sicurezza esistenti di tipo fisico, tecnico, procedurale, relative al personale con indicazione delle eventuali certificazioni o verifiche eseguite;

*b)* i requisiti di sicurezza che caratterizzano l'impiego dell'oggetto della fornitura, espressi in termini di capacità di proteggere la disponibilità, l'integrità e la riservatezza delle informazioni e i servizi di cui al comma 3, lettera *d)*.

5. Con successivo atto del CVCN, da adottarsi entro sessanta giorni dalla data di entrata in vigore del presente decreto, sono definite le metodologie per la predisposizione del documento di analisi del rischio e per l'individuazione dei livelli di severità dei *test* di cui all'articolo 5, comma 2.

6. Ai fini del comma 5, il CVCN, sulla base di *standard* tecnici di riferimento, tiene conto dell'impatto di violazioni intenzionali o accidentali sui requisiti di sicurezza, di cui alla lettera *b)* del comma 4, che determinano eventi di indisponibilità, malfunzionamento e compromissione della funzione essenziale o del servizio essenziale.

Art. 4.

*Procedimento di verifica e valutazione*

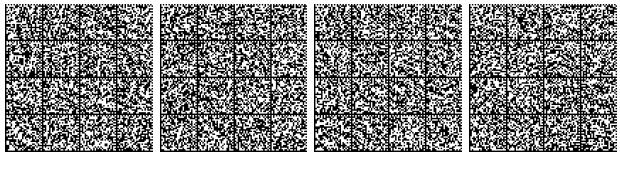
1. Il CVCN o i CV, secondo le rispettive competenze stabilite nell'articolo 1, comma 6, del decreto-legge, svolgono il procedimento di verifica e valutazione dell'analisi documentale contenuta nella comunicazione di cui all'articolo 3.

2. Il procedimento si articola in:

*a)* verifiche preliminari di cui all'articolo 5;

*b)* fase di preparazione all'esecuzione dei *test*, di cui all'articolo 6;





*c)* esecuzione dei *test* di *hardware* e di *software* di cui all'articolo 7.

3. All'esito delle verifiche e dei *test* di cui al comma 2, il CVCN o i CV, con apposito provvedimento, definiscono eventuali condizioni e *test* di *hardware* e di *software* da inserire nelle clausole del bando di gara o del contratto, di cui all'articolo 5, nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro, di cui all'articolo 8.

4. Le attività di cui alla lettera *a)* del comma 2 sono svolte entro il termine di quarantacinque giorni dalla comunicazione di cui all'articolo 3, prorogabile una sola volta di quindici giorni nei casi di particolare complessità, nell'ipotesi in cui l'oggetto di valutazione:

*a)* sia costituito da beni, sistemi e servizi ICT integrati tra di loro;

*b)* sia basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di *test* consolidate;

*c)* interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali.

5. Le attività di cui alla lettera *c)* del comma 2 si concludono entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i *test* al CVCN o ai CV secondo le condizioni individuate ai sensi dell'articolo 5, commi 5 e 6.

6. Decorsi i termini di cui al comma 4 senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento. Decorsi i termini di cui al comma 5, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire l'esecuzione del contratto.

7. Ai fini dello svolgimento delle attività di cui al comma 2, lettera *c)*, il CVCN può avvalersi di LAP e si coordina, ove previsto, con i centri di valutazione del Ministero dell'Interno e del Ministero della Difesa, ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge.

8. Il CVCN condivide con i CV e i LAP le metodologie per l'effettuazione dei *test* ai sensi del decreto del Presidente del Consiglio dei ministri adottato in attuazione dell'articolo 1, comma 7, lettera *b)*, del decreto-legge. Il CVCN, i CV e i LAP assicurano, anche con strumenti adeguati, la riservatezza di tali metodologie.

9. Gli atti del procedimento di verifica e valutazione sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'articolo 1, comma 1, del decreto-legge.

Art. 5.

*Verifiche preliminari, individuazione di condizioni e* test

1. A seguito della comunicazione di cui all'articolo 3, il CVCN o i CV effettuano verifiche preliminari ed eventualmente richiedono al soggetto incluso nel perimetro le informazioni necessarie per assicurare la collaborazione ai fini dell'individuazione delle condizioni per il fornitore e della tipologia di *test* di *hardware* e di *software* da eseguire. In caso di incompletezza o incongruenza delle informazioni fornite dal soggetto incluso nel perimetro i termini di conclusione del procedimento sono sospesi, per una sola volta, fino al ricevimento delle informazioni richieste ai sensi degli articoli 2, comma 7, e 6, comma 1, lettera *b)*, della legge 7 agosto 1990, n. 241.

2. Nell'individuazione dei *test* da eseguire, il CVCN e i CV tengono conto dell'analisi del rischio di cui all'articolo 3 e dei livelli di severità determinati sulla base della metodologia di cui al comma 5 del medesimo articolo 3.

3. Il CVCN e i CV possono richiedere l'esecuzione delle seguenti tipologie di *test*:

*a) test* di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto;

*b) test* di intrusione a supporto dell'analisi di vulnerabilità.

4. Con atto del CVCN, da adottarsi entro sessanta giorni dalla data di entrata in vigore del presente decreto e da aggiornarsi periodicamente, sono definiti i *test* corrispondenti ai livelli di severità derivanti dall'analisi del rischio di cui all'articolo 3.

5. Nel caso di imposizione di *test*, il fornitore è tenuto ad effettuare almeno le seguenti attività propedeutiche e indispensabili alla loro esecuzione:

*a)* fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza di cui all'articolo 3, comma 4, lettera *b)*;

*b)* provvedere all'allestimento di un ambiente di *test* adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il fornitore o presso il soggetto del perimetro;

*c)* fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni;

*d)* fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione;

*e)* fornire una descrizione dei *test* funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

6. Ai sensi dell'articolo 4, comma 3, il CVCN e i CV definiscono, con apposito provvedimento, da comunicarsi al soggetto incluso nel perimetro le eventuali ulteriori condizioni, i *test* da eseguire ed eventuali indicazioni per il supporto da parte del fornitore ai fini dell'integrazione nei bandi di gara o nei contratti con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei *test*.

7. Le centrali di committenza, ai fini della realizzazione degli strumenti di cui all'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, tengono conto, anche per le finalità di cui all'articolo 31, comma 5, del decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, delle previsioni di cui all'articolo 1, comma 6, del decreto-legge, e di cui al presente decreto, con riferimento alle acquisizioni di beni, sistemi e servizi ICT inclusi nelle categorie di cui all'articolo 1, lettera *l)*, e di cui al capo III del presente decreto. Al fine dell'effettuazione di tali acquisizioni mediante i detti strumenti, i soggetti pubblici inclusi nel perimetro specificano, secondo quanto previsto nella relativa documentazione di gara e tenendo conto delle caratteri-

stiche della specifica acquisizione, gli elementi relativi a condizioni e a *test* di cui al comma 6. Gli aggiudicatari assicurano il rispetto di dette previsioni.

8. Nei bandi di gara o nei contratti, i requisiti di sicurezza dell'oggetto di fornitura sono indicati dal soggetto incluso nel perimetro adottando se necessario le opportune cautele di riservatezza, anche nei casi in cui l'acquisizione avvenga attraverso le centrali di committenza.

9. Il soggetto incluso nel perimetro, successivamente all'aggiudicazione della gara o della stipula del contratto, comunica al CVCN o ai CV, in via telematica, i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto di fornitura.

Art. 6.

*Preparazione all'esecuzione dei* test

1. A seguito della comunicazione di cui al comma 9 dell'articolo 5, il CVCN e i CV verificano, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni, secondo le modalità dell'articolo 7. Nel caso in cui:

*a)* l'oggetto sia stato sottoposto a precedenti valutazioni o sia in corso di valutazione, sono effettuate le verifiche di cui al comma 2, finalizzate a evitare la duplicazione di *test* eventualmente già eseguiti;

*b)* l'oggetto non sia stato sottoposto a precedenti valutazioni e non sia in corso di valutazione, si procede come descritto al comma 3.

2. Nei casi di cui al comma 1, lettera *a)*, ferme restando le condizioni di cui all'articolo 5, sull'oggetto di valutazione non sono effettuati *test* nei casi in cui:

*a)* su tutte le funzioni di sicurezza necessarie per soddisfare i requisiti di sicurezza di interesse nella nuova valutazione siano stati eseguiti o siano in corso di esecuzione sia i *test* di corretta implementazione di cui all'articolo 5, comma 3, lettera *a)*, sia i *test* di intrusione di cui all'articolo 5, comma 3, lettera *b)*;

*b)* i *test* di intrusione siano stati eseguiti o siano in corso di esecuzione con riferimento a livelli di severità non inferiori a quelli selezionati per la valutazione in corso.

3. Nei casi di cui al comma 1, lettera *a)*, diversi dal comma 2, ferme restando le condizioni di cui all'articolo 5, il CVCN o i CV, se necessario in collaborazione con il soggetto incluso nel perimetro, identificano i *test* da eseguire escludendo quelli precedentemente eseguiti o in corso di esecuzione.

4. Nei casi di cui al comma 1, lettera *b)*, e di cui al comma 3:

*a)* il CVCN può affidare l'esecuzione dei *test* ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore;

*b)* il CVCN e i CV invitano il fornitore a predisporre le attività preliminari all'esecuzione dei *test* di cui all'articolo 5 e definiscono la sede in cui svolgere tali attività.

5. Nei casi di cui al comma 2, il CVCN o i CV, ferma restando la possibilità di prevedere le prescrizioni di utilizzo di cui all'articolo 8, comunicano al soggetto incluso nel perimetro, e per conoscenza al fornitore, la conclusione del procedimento.

6. Allo sviluppo e alla gestione della piattaforma di cui al comma 1 si fa fronte con le risorse disponibili a legislazione vigente.

Art. 7.

*Esecuzione dei* test

1. Concluse le attività preliminari di cui all'articolo 6, il CVCN o i CV comunicano l'avvio dei *test* al soggetto incluso nel perimetro e al fornitore. I *test* si concludono entro i termini individuati dall'articolo 4, comma 5.

2. Con la comunicazione di cui al comma 1 il CVCN o i CV specificano le modalità di collaborazione dei fornitori durante l'esecuzione delle prove.

3. I *test* sono eseguiti presso i laboratori del CVCN, dei CV e dei LAP. Se necessario, possono essere eseguiti da personale del CVCN, dei CV e dei LAP presso il fornitore o il soggetto incluso nel perimetro.

4. I *test* sono effettuati secondo le metodologie predisposte dal CVCN di cui dall'articolo 4, comma 8, assicurando il rispetto di quanto previsto all'articolo 4, comma 9. I CV e i LAP sono tenuti a non divulgare tali metodologie.

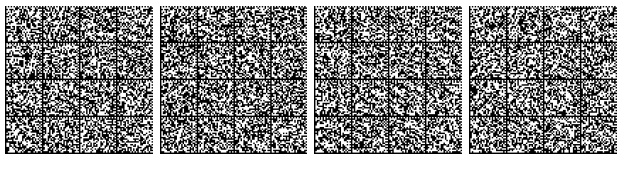
5. Ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241, nel caso in cui si verifichi un malfunzionamento dell'oggetto di valutazione o dell'ambiente di *test* predisposto dal fornitore che renda impossibile o difficoltosa l'esecuzione dei *test*, il CVCN o i CV comunicano tempestivamente al soggetto incluso nel perimetro, informando anche il fornitore, i motivi che ostano al proseguimento dei *test*. Entro il termine di dieci giorni dalla ricezione della comunicazione, il fornitore può provvedere a risolvere il malfunzionamento. La predetta comunicazione sospende i termini di cui all'articolo 4, comma 5, che iniziano nuovamente a decorrere dalla data di soluzione del malfunzionamento verificata dal CVCN o dai CV. In caso di eventuale mancata soluzione entro il termine, il CVCN o i CV comunicano al soggetto incluso nel perimetro e al fornitore l'impossibilità di proseguire l'esecuzione dei *test* e concludono il procedimento indicando la motivazione.

6. Il CVCN, i CV e i LAP redigono un rapporto di prova nel quale sono indicati in dettaglio l'ambiente di *test*, le prove eseguite ed i relativi esiti.

7. I LAP, eventualmente incaricati per l'esecuzione dei *test*, trasmettono il rapporto di prova al CVCN entro sette giorni lavorativi dalla scadenza dei termini per l'esecuzione dei *test*.

8. Nel caso in cui sia stato incaricato il LAP e si verifichi un malfunzionamento dell'oggetto di valutazione o dell'ambiente di *test* predisposto dal fornitore, lo stesso LAP informa tempestivamente il CVCN che procede ai sensi del comma 5.





Art. 8.

*Esito della valutazione e prescrizioni di utilizzo*

1. Sulla base del rapporto di prova di cui all'articolo 7, commi 6 e 7, il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei *test*. Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro i termini di cui all'articolo 4, comma 5.

2. In caso di esito negativo del rapporto di valutazione, il CVCN e i CV, previa comunicazione dei motivi ostativi all'accoglimento dell'istanza ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241, comunicano al soggetto incluso nel perimetro e al fornitore il provvedimento negativo motivato.

3. Nel caso in cui l'esito di cui al comma 1 sia positivo, il CVCN può imporre al soggetto incluso nel perimetro prescrizioni per l'utilizzo dell'oggetto dell'affidamento ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge.

4. Le prescrizioni di cui al comma 3 possono riguardare anche il mantenimento nel tempo del livello di sicurezza nell'ambiente di esercizio.

Art. 9.

*Oneri economici a carico del fornitore*

1. Le spese a carico del fornitore per le attività di valutazione svolte dal CVCN e dai CV e per le attività di *test* condotte dai LAP sono calcolate sulla base delle disposizioni di cui all'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366.

Art. 10.

*Casi di deroga*

1. Nel rispetto dell'articolo 1, comma 6, lettera *a)*, ultimo periodo, del decreto-legge, non sono tenute agli obblighi di comunicazione previsti dal presente decreto le Autorità di pubblica sicurezza e le forze di polizia di cui agli articoli 1, 13, 14, 15 e 16, della legge 1° aprile 1981, n. 121.

2. Ai sensi dell'articolo 1, comma 6, lettera *a)*, del decreto-legge, ai fini della deroga alla comunicazione di cui all'articolo 3, è considerato indispensabile procedere in sede estera, salvo motivate esigenze connesse a specifici impieghi, per le forniture dei seguenti beni, sistemi e servizi ICT, se acquisite e utilizzate nel Paese in cui i soggetti del perimetro operano, tramite uffici, sedi o filiali all'estero:

*a)* realizzazione e aggiornamento di reti informatiche e di telecomunicazioni;

*b)* servizi di connettività;

*c)* servizi di gestione, assistenza e manutenzione di apparati e sistemi informatici, di rete e di telecomunicazione, erogati in presenza presso la sede estera.

3. L'elenco e la documentazione relativa agli affidamenti effettuati ai sensi del comma 2 sono resi disponibili per le verifiche e le ispezioni di cui al capo IV del presente decreto.

4. Nei casi di cui al presente articolo è comunque garantito l'utilizzo di beni, sistemi e servizi ICT conformi alle misure di sicurezza di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge.

Art. 11.

*Periodo transitorio*

1. Il CVCN e i CV individuano i *test* da eseguire secondo un approccio gradualmente crescente nelle verifiche di sicurezza ai sensi dell'articolo 1, comma 6, del decreto-legge. Nei primi diciotto mesi dalla data di entrata in vigore del presente decreto, ferma restando la possibilità di imporre le condizioni di cui all'articolo 5 e le prescrizioni di utilizzo di cui all'articolo 8, nonché di effettuare l'analisi documentale di cui all'articolo 4, il CVCN e i CV possono effettuare *test* con livello di complessità crescente nel tempo, secondo un programma contenuto nell'atto di cui all'articolo 5, comma 4.

Art. 12.

*Casi particolari*

1. Ai sensi dell'articolo 3, comma 2, del decreto-legge, la 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, strumentale ai fini dell'esercizio dei poteri speciali di cui all'articolo 1-*bis* del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, è effettuata secondo le procedure, le modalità e i termini di cui all'articolo 1, comma 6, del decreto-legge, e di cui al presente decreto.

*Capo III*

CATEGORIE DI TIPOLOGIE DI BENI, SISTEMI E SERVIZI ICT

Art. 13.

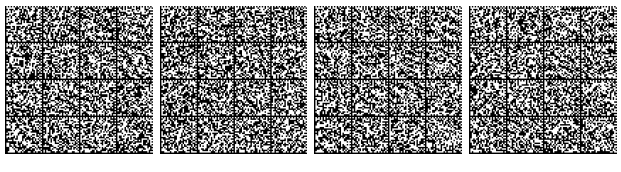
*Criteri tecnici per l'individuazione delle categorie*

1. Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate sulla base dell'esecuzione o svolgimento delle seguenti funzioni:

*a)* commutazione oppure protezione da intrusioni e rilevazione di minacce informatiche in una rete, ivi inclusa l'applicazione di politiche di sicurezza;

*b)* comando, controllo e attuazione in una rete di controllo industriale;





*c)* monitoraggio e controllo di configurazione di una rete di comunicazione elettronica;

*d)* sicurezza della rete riguardo alla disponibilità, autenticità, integrità o riservatezza dei servizi offerti o dei dati conservati, trasmessi o trattati;

*e)* autenticazione e allocazione delle risorse di una rete di comunicazione elettronica;

*f)* implementazione di un servizio informatico per mezzo della configurazione di un programma *software* esistente oppure dello sviluppo, parziale o totale, di un nuovo programma *software*, costituente la parte applicativa rilevante ai fini dell'erogazione del servizio informatico stesso.

2. Le categorie, sulla base dei criteri di cui al comma 1, sono individuate con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 1, comma 6, lettera *a)*, del decreto-legge.

## *Capo IV*

## ISPEZIONI E VERIFICHE

### Art. 14.

*Oggetto delle verifiche e delle ispezioni*

1. Le verifiche e le ispezioni hanno lo scopo di accertare, nell'ambito di quanto previsto dal presente decreto, l'adempimento da parte dei soggetti inclusi nel perimetro dei seguenti obblighi:

*a)* predisposizione, aggiornamento e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge;

*b)* notifica al CSIRT italiano (*Computer Security Incident Response Team*) degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici nei termini e con le modalità previste dal decreto del Presidente del Consiglio dei ministri di cui all'articolo 1, comma 3, lettera *a)*, del decreto-legge;

*c)* adozione delle misure di sicurezza di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge, nei termini e con le modalità previste dal relativo decreto attuativo;

*d)* comunicazione al CVCN di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge, nei termini e con le modalità previste dal presente decreto;

*e)* impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in conformità alle condizioni e con superamento dei *test* imposti dal CVCN ai sensi dell'articolo 1, comma 6, lettera *a)*, del decreto-legge;

*f)* collaborazione per l'effettuazione delle attività di *test* da parte dei soggetti ai sensi dell'articolo 1, comma 6, lettera *b)*, del decreto-legge;

*g)* osservanza delle prescrizioni formulate dalle autorità competenti ai sensi dell'articolo 1, comma 6, lettera *c)*, del decreto-legge, all'esito delle attività di ispezione e verifica;

*h)* osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge.

### Art. 15.

*Autorità competenti*

1. Ai sensi dell'articolo 1, comma 6, lettera *c)*, del decreto-legge, le verifiche e le ispezioni sono svolte:

*a)* dalla Presidenza del Consiglio dei Ministri, per i profili di pertinenza dei soggetti pubblici inclusi nel perimetro e di quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, rientranti tra i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge, ed in particolare dalla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione;

*b)* dal Ministero dello sviluppo economico per i soggetti privati inclusi nel perimetro e di cui al medesimo articolo 1, comma 2-*bis*, del decreto-legge, ed in particolare dalla struttura competente in materia di tecnologie delle comunicazioni e di sicurezza informatica;

*c)* dalle strutture specializzate di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge, secondo le rispettive competenze, limitatamente alle reti, ai sistemi informativi, ai servizi informatici, di cui all'articolo 1, comma 2, lettera *b)*, dello stesso decreto-legge, 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, che comunicano gli esiti alla Presidenza del Consiglio dei Ministri per i profili di competenza.

2. Le autorità competenti istituiscono e aggiornano un elenco del personale da incaricare per lo svolgimento delle attività di ispezione e verifica. L'eventuale accesso ad informazioni classificate di cui all'articolo 42 della legge 3 agosto 2007, n. 124, derivante dallo svolgimento delle predette attività, è effettuato, nel rispetto del principio di cui al comma 1 del medesimo articolo e, nel caso di informazioni con classifica superiore a «riservato», esclusivamente da personale in possesso del requisito di cui al comma 1-*bis* del predetto articolo 42.

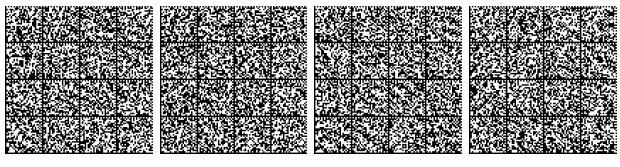
3. Ai fini dello svolgimento delle verifiche e delle ispezioni, le autorità competenti individuano il personale incaricato, nonché un responsabile del procedimento ai sensi dell'articolo 6 della legge 7 agosto 1990, n. 241.

4. Nell'attribuzione degli incarichi le autorità competenti si attengono a criteri di professionalità e di rotazione.

5. Al momento dell'accettazione dell'incarico, il personale incaricato dichiara di non trovarsi, per quanto a sua conoscenza, in una situazione di conflitto di interessi e si impegna a segnalare ogni sopravvenuta situazione di conflitto, anche potenziale.

6. Ai sensi dell'articolo 1, comma 8, lettera *a)*, del decreto-legge, le autorità competenti si raccordano, ove necessario per lo svolgimento delle verifiche e delle ispezioni, con le autorità di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65, anche al fine di avvalersi di personale dipendente esperto nei settori di cui al medesimo decreto legislativo.





Art. 16.

*Attività di verifica e ispezione*

1. Le autorità competenti dispongono verifiche e ispezioni sulla base degli atti di programmazione dalle medesime adottati, nonché in caso di esigenze derivanti da:

*a)* notifiche di incidenti ai sensi dell'articolo 1, comma 3, lettera *a)*, del decreto-legge;

*b)* rilevati inadempimenti rispetto agli obblighi imposti dal decreto-legge e dai relativi decreti attuativi;

*c)* segnalazioni provenienti da altre Autorità Pubbliche.

2. Le ispezioni sono svolte anche successivamente alle verifiche qualora si ritenga necessario riscontrare le evidenze acquisite, oppure qualora le predette verifiche presentino elementi tali da richiedere un approfondimento.

3. Il responsabile del procedimento di cui all'articolo 15, comma 3, comunica ai soggetti di cui all'articolo 7, comma 1, della legge 7 agosto 1990, n. 241, inclusi nel perimetro, l'avvio del procedimento di verifica o di ispezione con le modalità di cui all'articolo 8 della predetta legge, richiedendo le informazioni e la documentazione necessaria al fine dell'espletamento delle relative attività.

4. I soggetti destinatari della comunicazione di cui al comma 3 nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per lo svolgimento delle attività di cui al comma 1, comunicandone il nominativo al responsabile del procedimento.

5. Il procedimento di verifica si conclude entro il termine di centoventi giorni dalla data della comunicazione di cui al comma 3.

6. Il procedimento di ispezione si conclude entro il termine di novanta giorni dalla data della comunicazione di cui al comma 3.

7. All'esito dell'attività di cui al comma 1, le autorità competenti possono formulare specifiche prescrizioni a cui i soggetti inclusi nel perimetro devono attenersi. Il rispetto delle prescrizioni può essere oggetto di attività di verifica e ispezione.

Art. 17.

*Attività di verifica*

1. Le verifiche sono effettuate mediante analisi e controllo documentale delle evidenze e di ogni altro elemento di fatto e di diritto, al fine di accertare l'adempimento degli obblighi previsti dal decreto-legge e dai relativi decreti attuativi.

2. Il procedimento di cui al comma 1 è avviato secondo le modalità di cui all'articolo 16, comma 3. I soggetti destinatari della comunicazione di cui al medesimo articolo 16, comma 3, rendono disponibile la documentazione richiesta ai fini delle attività di verifica di cui al comma 1, entro quindici giorni dalla ricezione della comunicazione.

3. Fatta salva l'applicazione delle sanzioni di cui all'articolo 1, comma 9, del decreto-legge, durante l'esecuzione delle attività di cui al comma 1, il responsabile del procedimento, qualora le evidenze risultino incomplete o incongruenti, può richiedere chiarimenti e integrazioni che sono resi entro dieci giorni dalla ricezione della richiesta, secondo le modalità indicate dal richiedente.

4. Dell'attività svolta nel corso delle verifiche è redatto apposito verbale che il personale incaricato trasmette al responsabile del procedimento.

5. Qualora nel corso della verifica vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

Art. 18.

*Attività di ispezione*

1. Le ispezioni possono essere svolte mediante:

*a)* riscontro delle evidenze eventualmente acquisite in sede di verifica, qualora le stesse presentino elementi meritevoli di approfondimento;

*b)* analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari.

2. Per lo svolgimento delle attività di cui al comma 1, il personale incaricato può richiedere o eventualmente acquisire direttamente tutte le evidenze ritenute utili ai fini dell'accertamento.

3. Le ispezioni possono essere effettuate presso le sedi utilizzate dai soggetti inclusi nel perimetro nei casi di cui all'articolo 16, comma 1. Il procedimento di cui al comma 1 è avviato secondo le modalità di cui all'articolo 16, comma 3, con un preavviso non inferiore a quindici giorni. L'informativa riporta:

*a)* le date e i siti in cui sarà effettuata l'ispezione;

*b)* le persone da intervistare o i loro ruoli e responsabilità;

*c)* le reti, i sistemi informativi e i servizi informatici da sottoporre a ispezione;

*d)* i nominativi del personale incaricato;

*e)* eventuali altre informazioni utili ai fini dell'ispezione.

4. Entro cinque giorni dalla ricezione della comunicazione di cui al comma 3, il soggetto ricevente può proporre date alternative a quelle previste per l'ispezione, individuando un termine non superiore a dieci giorni per il differimento dell'ispezione. Qualora il soggetto proponga date alternative, l'autorità competente può:

*a)* accettare la proposta di modifica delle date, inviando una comunicazione almeno sette giorni prima della prima data prevista per l'ispezione;

*b)* proporre ulteriori date e comunicarle al soggetto con le modalità di cui alla precedente lettera *a)*; tali nuove date non possono essere soggette a richieste di modifica da parte del soggetto e si intendono confermate.

5. In mancanza della proposta di cui alla lettera *a)* del comma 4, le date delle ispezioni si intendono confermate.

6. Almeno cinque giorni prima dell'ispezione prevista, il soggetto sottoposto alla stessa comunica il nominativo dell'incaricato di cui all'articolo 16, comma 4.

7. Durante il corso dell'ispezione, i soggetti inclusi nel perimetro mettono a disposizione tutte le risorse umane richieste e necessarie per agevolare le relative attività, garantendo altresì l'accesso ai locali, ai dispositivi e alle informazioni rilevanti ai fini dell'ispezione, anche se non esplicitamente e preventivamente indicati nella comunicazione di cui all'articolo 16, comma 3.

8. Qualora durante il corso dell'ispezione emergano evidenze meritevoli di approfondimento, le stesse possono essere esaminate in una fase successiva.

9. Dell'attività svolta nel corso dell'ispezione è redatto apposito processo verbale da parte del personale incaricato che lo sottoscrive unitamente all'incaricato di cui all'articolo 16, comma 4. Qualora quest'ultimo si rifiuti di sottoscrivere il verbale, il personale incaricato ne dà evidenza nel verbale. Una copia del verbale è comunque rilasciata all'incaricato di cui all'articolo 16, comma 4, e una copia è trasmessa al responsabile del procedimento.

10. Qualora nel corso dell'ispezione vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

Art. 19.

*Esiti delle attività di verifica e di ispezione*

1. L'autorità competente, raccolti gli esiti delle attività di cui all'articolo 16, adotta il provvedimento di conclusione del procedimento, impartendo, se necessario, specifiche prescrizioni ai sensi dell'articolo 1, comma 6, lettera *c)*, del decreto-legge e dandone comunicazione all'interessato. Nei casi previsti, l'autorità competente avvia il procedimento per l'applicazione delle sanzioni di cui all'articolo 1, comma 9, del decreto-legge.

Art. 20.

*Invarianza finanziaria*

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri per la finanza pubblica e le amministrazioni pubbliche interessate vi provvedono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 5 febbraio 2021

MATTARELLA

CONTE, *Presidente del Consiglio dei ministri*

PATUANELLI, *Ministro dello sviluppo economico*

LAMORGESE, *Ministro dell'interno*

GUERINI, *Ministro della difesa*

GUALTIERI, *Ministro dell'economia e delle finanze*

PISANO, *Ministro per l'innovazione tecnologica e la digitalizzazione*

*Registrato alla Corte dei conti il 23 marzo 2021*
*Ufficio di controllo sugli atti della Presidenza del Consiglio, del Ministero della giustizia e del Ministero degli affari esteri, reg.ne n. 668*

---

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art. 10, comma 3, del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con D.P.R. 28 dicembre 1985, n. 1092, al solo fine di facilitare la lettura delle disposizioni di legge modificate o alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

*Note alle premesse:*

— L'art. 87 della Costituzione conferisce, tra l'altro, al Presidente della Repubblica il potere di promulgare le leggi e di emanare i decreti aventi valore di legge ed i regolamenti.

— Si riporta il testo dell'art. 17 della legge 23 agosto 1988, n. 400 «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri»:

«Art. 17 *(Regolamenti)*. — 1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il parere del Consiglio di Stato che deve pronunziarsi entro novanta giorni dalla richiesta, possono essere emanati regolamenti per disciplinare:

*a)* l'esecuzione delle leggi e dei decreti legislativi, nonché dei regolamenti comunitari;

*b)* l'attuazione e l'integrazione delle leggi e dei decreti legislativi recanti norme di principio, esclusi quelli relativi a materie riservate alla competenza regionale;

*c)* le materie in cui manchi la disciplina da parte di leggi o di atti aventi forza di legge, sempre che non si tratti di materie comunque riservate alla legge;

*d)* l'organizzazione ed il funzionamento delle amministrazioni pubbliche secondo le disposizioni dettate dalla legge;

*e)*.

2. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato e previo parere delle Commissioni parlamentari competenti in materia, che si

pronunciano entro trenta giorni dalla richiesta, sono emanati i regolamenti per la disciplina delle materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi della Repubblica, autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari.

3. Con decreto ministeriale possono essere adottati regolamenti nelle materie di competenza del ministro o di autorità sottordinate al ministro, quando la legge espressamente conferisca tale potere. Tali regolamenti, per materie di competenza di più ministri, possono essere adottati con decreti interministeriali, ferma restando la necessità di apposita autorizzazione da parte della legge. I regolamenti ministeriali ed interministeriali non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo. Essi debbono essere comunicati al Presidente del Consiglio dei ministri prima della loro emanazione.

4. I regolamenti di cui al comma 1 ed i regolamenti ministeriali ed interministeriali, che devono recare la denominazione di "regolamento", sono adottati previo parere del Consiglio di Stato, sottoposti al visto ed alla registrazione della Corte dei conti e pubblicati nella *Gazzetta Ufficiale*.

4-*bis*. L'organizzazione e la disciplina degli uffici dei Ministeri sono determinate, con regolamenti emanati ai sensi del comma 2, su proposta del Ministro competente d'intesa con il Presidente del Consiglio dei ministri e con il Ministro del tesoro, nel rispetto dei princìpi posti dal decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, con i contenuti e con l'osservanza dei criteri che seguono:

*a)* riordino degli uffici di diretta collaborazione con i Ministri ed i Sottosegretari di Stato, stabilendo che tali uffici hanno esclusive competenze di supporto dell'organo di direzione politica e di raccordo tra questo e l'amministrazione;

*b)* individuazione degli uffici di livello dirigenziale generale, centrali e periferici, mediante diversificazione tra strutture con funzioni finali e con funzioni strumentali e loro organizzazione per funzioni omogenee e secondo criteri di flessibilità eliminando le duplicazioni funzionali;

*c)* previsione di strumenti di verifica periodica dell'organizzazione e dei risultati;

*d)* indicazione e revisione periodica della consistenza delle piante organiche;

*e)* previsione di decreti ministeriali di natura non regolamentare per la definizione dei compiti delle unità dirigenziali nell'ambito degli uffici dirigenziali generali.

4-*ter*. Con regolamenti da emanare ai sensi del comma 1 del presente articolo, si provvede al periodico riordino delle disposizioni regolamentari vigenti, alla ricognizione di quelle che sono state oggetto di abrogazione implicita e all'espressa abrogazione di quelle che hanno esaurito la loro funzione o sono prive di effettivo contenuto normativo o sono comunque obsolete.».

— Si riporta il testo dell'art. 1, comma 6 del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.»:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, sono disciplinati le procedure, le modalità e i termini con cui:

*a)* i soggetti di cui al comma 2-*bis*, che intendano procedere, anche per il tramite delle centrali di committenza alle quali essi sono tenuti a fare ricorso ai sensi dell'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, 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 di cui al comma 2, lettera *b)*, appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con i soggetti di cui al comma 2-*bis*, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di hardware e software, 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. I test devono essere conclusi nel termine di sessanta giorni. Decorso il termine di cui al precedente periodo, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In relazione alla specificità delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, individuati ai sensi del comma 2, lettera *b)*, i predetti Ministeri, 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 presente decreto, possono procedere, con le medesime modalità e i medesimi termini previsti dai periodi precedenti, attraverso la comunicazione ai propri Centri di valutazione accreditati per le attività di cui al presente decreto, ai sensi del comma 7, lettera *b)*, che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi i predetti Centri informano il CVCN con le modalità stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera *b)*. Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera *b)*, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati;

*b)* i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera *b)*, assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa, di cui alla lettera *a)* del presente comma, la propria collaborazione per l'effettuazione delle attività di test di cui alla lettera *a)* del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresì alla Presidenza del Consiglio dei ministri le analoghe segnalazioni dei Centri di valutazione dei Ministeri dell'interno e della difesa, di cui alla lettera *a)*;

*c)* la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attività di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera *b)*, dal comma 3, dal presente comma e dal comma 7, lettera *b)*, impartendo, se necessario, specifiche prescrizioni; nello svolgimento delle predette attività di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi è effettuato in conformità a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera *b)*, 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, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, 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.».

— Il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 «Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133», è pubblicato nella *Gazzetta Ufficiale* n. 261 del 21 ottobre 2020.

— Il decreto del Ministro delle comunicazioni 15 febbraio 2006 «Individuazioni delle prestazioni, eseguite dal Ministero delle comunicazioni per conto terzi, ai sensi dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366», è pubblicato nella *Gazzetta Ufficiale* n. 82 del 7 aprile 2006.

— Si riporta il testo dell'art. 29 del decreto legislativo 7 marzo 2005, n. 82 «Codice dell'amministrazione digitale»:

«Art. 29 *(Qualificazione dei fornitori di servizi)*. — 1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida.

2. Ai fini della qualificazione, i soggetti di cui al comma 1 devono possedere i requisiti di cui all'articolo 24 del Regolamento (UE) 23 luglio 2014, n. 910/2014, disporre di requisiti di onorabilità, affidabilità, tecnologici e organizzativi compatibili con la disciplina europea, nonché di garanzie assicurative adeguate rispetto all'attività svolta. Con decreto del Presidente del Consiglio dei ministri, o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, sentita l'AgID, nel rispetto della disciplina europea, sono definiti i predetti requisiti in relazione alla specifica attività che i soggetti di cui al comma 1 intendono svolgere. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche.

3.

4. La domanda di qualificazione si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità di AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto da AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. - 8.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse di AgID, senza nuovi o maggiori oneri per la finanza pubblica.».

— La legge 24 novembre 1981, n. 689 «Modifiche al sistema penale», è pubblicata nella *Gazzetta Ufficiale* n. 329 del 30 novembre 1981, S.O.

— La legge 7 agosto 1990, n. 241 «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi», è pubblicata nella *Gazzetta Ufficiale* n. 192 del 18 agosto 1990.

*Note all'art. 1:*

— Per il riferimento al decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133, si veda nelle note alle premesse.

— Per il riferimento al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, si veda nelle note alle premesse.

— Si riporta il testo dell'art. 1, comma 2, lett. *a)*, del citato decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):

*a)* sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell'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 dei seguenti 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;

2-*bis*) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

(*Omissis*).».

— Si riporta il testo dell'art. 1, comma 1, lett. *dd)*, del decreto legislativo 1° agosto 2003, n. 259 «Codice delle comunicazioni elettroniche»:

«Art. 1 *(Definizioni)*. — 1. Ai fini del presente Codice si intende per:

(*Omissis*).

*dd)* reti di comunicazione elettronica: i 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;

(*Omissis*).».

— Si riporta il testo dell'art. 3, comma 1, lett. *aa)*, del decreto legislativo 18 maggio 2018, n. 65 «Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»:

«Art. 3 *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

(*Omissis*).

*aa)* servizio di cloud computing, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.».

— Si riporta il testo dell'art. 1, comma 7, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

7. Nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, il CVCN assume i seguenti compiti:

*a)* contribuisce all'elaborazione delle misure di sicurezza di cui al comma 3, lettera *b)*, per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;

*b)* ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attività di cui al comma 6, lettera *a)*, dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del CISR, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni. Con lo stesso decreto sono 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, di cui al comma 6,

lettera *a)*, anche la 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;

*c)* elabora e adotta, previo conforme avviso dell'organismo tecnico di supporto al CISR, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.».

— Si riporta il testo dell'art. 1, comma 512, della legge 28 dicembre 2015, n. 208 «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2016)»:

«Art. 1. - 512. Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti. Le regioni sono autorizzate ad assumere personale strettamente necessario ad assicurare la piena funzionalità dei soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, in deroga ai vincoli assunzionali previsti dalla normativa vigente, nei limiti del finanziamento derivante dal Fondo di cui al comma 9 del medesimo articolo 9 del decreto-legge n. 66 del 2014.

(*Omissis*).».

— Si riporta il testo dell'art. 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133 «Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria»:

«Art. 83 *(Efficienza dell'Amministrazione finanziaria)*. — (*Omissis*).

15. Al fine di garantire la continuità delle funzioni di controllo e monitoraggio dei dati fiscali e finanziari, i diritti dell'azionista della società di gestione del sistema informativo dell'amministrazione finanziaria ai sensi dell'articolo 22, comma 4, della legge 30 dicembre 1991, n. 413, sono esercitati dal Ministero dell'economia e delle finanze ai sensi dell'articolo 6, comma 7, del regolamento di cui al decreto del Presidente della Repubblica 30 gennaio 2008, n. 43, che provvede agli atti conseguenti in base alla legislazione vigente. Sono abrogate tutte le disposizioni incompatibili con il presente comma. Il consiglio di amministrazione, composto di cinque componenti, è conseguentemente rinnovato entro il 30 giugno 2008 senza applicazione dell'articolo 2383, terzo comma, del codice civile.

(*Omissis*).».

— Si riporta il testo dell'art. 31, comma 5, del decreto legge 16 luglio 2020, n. 76, convertito nella legge 11 settembre 2020, n. 120 «Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria»:

«Art. 31 *(Semplificazione dei sistemi informativi delle pubbliche amministrazioni e dell'attività di coordinamento nell'attuazione della strategia digitale e in materia di perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

5. Per assicurare la piena efficacia dei progetti di trasformazione digitale la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, nell'ambito dei progetti e delle attività da essa gestiti, provvede alla definizione e allo sviluppo di servizi e prodotti innovativi operando, anche in favore delle amministrazioni committenti, in qualità di innovation procurement broker. In tale ambito, per l'acquisizione dei beni e dei servizi funzionali alla realizzazione di progetti ad alto contenuto innovativo, la medesima società non si avvale di Consip S.p.A. nella sua qualità di centrale di committenza, in deroga all'ultimo periodo dell'articolo 4, comma 3-*ter*, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135.

(*Omissis*).».

— Si riporta il testo dell'art. 1, comma 2, lett. *b)*, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR):

(*Omissis*);

*b)* sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, l'organismo tecnico di supporto al CISR, integrato con un rappresentante della Presidenza del Consiglio dei ministri; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al comma 2-*bis* trasmettono tali elenchi, rispettivamente, alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico; la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico inoltrano gli elenchi di rispettiva pertinenza al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.».

*Note all'art. 4:*

— Si riporta il testo dell'art. 1, comma 1 del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, 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, è istituito il perimetro di sicurezza nazionale cibernetica.

(*Omissis*).».

*Note all'art. 5:*

— Si riporta il testo degli articoli 2, comma 7, e 6, comma 1, lettera *b)*, della legge 7 agosto 1990, n. 241 «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi»:

«Art. 2 *(Conclusione del procedimento)*. — (*Omissis*).

7. Fatto salvo quanto previsto dall'articolo 17, i termini di cui ai commi 2, 3, 4 e 5 del presente articolo possono essere sospesi, per una sola volta e per un periodo non superiore a trenta giorni, per l'acquisizione di informazioni o di certificazioni relative a fatti, stati o qualità non attestati in documenti già in possesso dell'amministrazione stessa o non direttamente acquisibili presso altre pubbliche amministrazioni. Si applicano le disposizioni dell'articolo 14, comma 2.

(*Omissis*).».

«Art. 6 *(Compiti del responsabile del procedimento).* — 1. Il responsabile del procedimento:

*a)* valuta, ai fini istruttori, le condizioni di ammissibilità, i requisiti di legittimazione ed i presupposti che siano rilevanti per l'emanazione di provvedimento;

*b)* accerta di ufficio i fatti, disponendo il compimento degli atti all'uopo necessari, e adotta ogni misura per l'adeguato e sollecito svolgimento dell'istruttoria. In particolare, può chiedere il rilascio di dichiarazioni e la rettifica di dichiarazioni o istanze erronee o incomplete e può esperire accertamenti tecnici ed ispezioni ed ordinare esibizioni documentali;

*c)* propone l'indizione o, avendone la competenza, indice le conferenze di servizi di cui all'articolo 14;

*d)* cura le comunicazioni, le pubblicazioni e le notificazioni previste dalle leggi e dai regolamenti;

*e)* adotta, ove ne abbia la competenza, il provvedimento finale, ovvero trasmette gli atti all'organo competente per l'adozione. L'organo competente per l'adozione del provvedimento finale, ove diverso dal responsabile del procedimento, non può discostarsi dalle risultanze dell'istruttoria condotta dal responsabile del procedimento se non indicandone la motivazione nel provvedimento finale.».

*Note all'art. 7:*

— Si riporta il testo dell'art. 10-*bis*, della citata legge 7 agosto 1990, n. 241:

«Art. 10-*bis (Comunicazione dei motivi ostativi all'accoglimento dell'istanza).* — 1. Nei procedimenti ad istanza di parte il responsabile del procedimento o l'autorità competente, prima della formale adozione di un provvedimento negativo, comunica tempestivamente agli istanti i motivi che ostano all'accoglimento della domanda. Entro il termine di dieci giorni dal ricevimento della comunicazione, gli istanti hanno il diritto di presentare per iscritto le loro osservazioni, eventualmente corredate da documenti. La comunicazione di cui al primo periodo sospende i termini di conclusione dei procedimenti, che ricominciano a decorrere dieci giorni dopo la presentazione delle osservazioni o, in mancanza delle stesse, dalla scadenza del termine di cui al secondo periodo. Qualora gli istanti abbiano presentato osservazioni, del loro eventuale mancato accoglimento il responsabile del procedimento o l'autorità competente sono tenuti a dare ragione nella motivazione del provvedimento finale di diniego indicando, se ve ne sono, i soli motivi ostativi ulteriori che sono conseguenza delle osservazioni. In caso di annullamento in giudizio del provvedimento così adottato, nell'esercitare nuovamente il suo potere l'amministrazione non può addurre per la prima volta motivi ostativi già emergenti dall'istruttoria del provvedimento annullato. Le disposizioni di cui al presente articolo non si applicano alle procedure concorsuali e ai procedimenti in materia previdenziale e assistenziale sorti a seguito di istanza di parte e gestiti dagli enti previdenziali. Non possono essere addotti tra i motivi che ostano all'accoglimento della domanda inadempienze o ritardi attribuibili all'amministrazione.».

*Note all'art. 9:*

— Si riporta il testo dell'art. 6 del decreto legislativo 30 dicembre 2003, n. 366 «Modifiche ed integrazioni al D.Lgs. 30 luglio 1999, n. 300, concernenti le funzioni e la struttura organizzativa del Ministero delle comunicazioni, a norma dell'articolo 1 della L. 6 luglio 2002, n. 137»:

«Art. 6 *(Individuazione delle prestazioni in conto terzi e produttività del personale).* — 1. Con decreto del Ministro delle comunicazioni, di concerto con il Ministro dell'economia e delle finanze, da emanare entro sessanta giorni dalla data di entrata in vigore del presente decreto legislativo, si provvede all'individuazione delle prestazioni eseguite dal Ministero delle comunicazioni per conto terzi e alla variazione in aumento delle tariffe previste dal D.M. 5 settembre 1995 del Ministro delle poste e delle telecomunicazioni, concernente tariffazione delle prestazioni scientifiche e sperimentali eseguite dall'Istituto superiore delle poste e delle telecomunicazioni per conto terzi, pubblicato nella *Gazzetta Ufficiale* n. 273 del 29 novembre 1995 e dal D.M. 24 settembre 2003 del Ministro delle comunicazioni, concernente determinazione delle quote di surrogazione del personale, dei costi di uso delle apparecchiature e degli automezzi e delle spese generali ai fini del rimborso degli oneri sostenuti dal Ministero delle comunicazioni per prestazioni rese a terzi, pubblicato nella *Gazzetta Ufficiale* n. 284 del 6 dicembre 2003.

2. In considerazione dell'accresciuta complessità delle funzioni e dei compiti assegnati al Ministero dall'articolo 32-*ter*, comma 1, lettere *h)*, *i)* ed *m)*, del decreto legislativo 30 luglio 1999, n. 300, come modificato dall'articolo 2, comma 1, del presente decreto legislativo, dall'articolo 2-*bis*, comma 10, del decreto-legge 23 gennaio 2001, n. 5, convertito, con modificazioni, dalla legge 20 marzo 2001, n. 66, come modificato dall'articolo 41, comma 8, della legge 16 gennaio 2003, n. 3, dal decreto legislativo 9 maggio 2001, n. 269, nonché dal decreto legislativo 1° agosto 2003, n. 259, una somma non superiore al 30 per cento delle entrate provenienti dalla riscossione dei compensi per prestazioni non rientranti tra i servizi pubblici essenziali o non espletate a garanzia di diritti fondamentali rese dal Ministero delle comunicazioni per conto terzi, certificate con decreto del Ministro delle comunicazioni, è destinata, d'intesa con le organizzazioni sindacali, all'incentivazione della produttività del personale in servizio presso il predetto Ministero, ai sensi della vigente normativa. Il Ministro dell'economia e delle finanze è autorizzato ad apportare con propri decreti le occorrenti variazioni di bilancio.».

*Note all'art. 10:*

— Si riporta il testo degli articoli 1, 13, 14, 15 e 16 della legge 1° aprile 1981, n. 121 «Nuovo ordinamento dell'Amministrazione della pubblica sicurezza»:

«Art. 1 *(Attribuzioni del Ministro dell'interno).* — Il Ministro dell'interno è responsabile della tutela dell'ordine e della sicurezza pubblica ed è autorità nazionale di pubblica sicurezza. Ha l'alta direzione dei servizi di ordine e sicurezza pubblica e coordina in materia i compiti e le attività delle forze di polizia.

Il Ministro dell'interno adotta i provvedimenti per la tutela dell'ordine e della sicurezza pubblica.

Restano ferme le competenze del Consiglio dei ministri previste dalle leggi vigenti.».

«Art. 13 *(Prefetto).* — Il prefetto è autorità provinciale di pubblica sicurezza.

Il prefetto ha la responsabilità generale dell'ordine e della sicurezza pubblica nella provincia e sovraintende all'attuazione delle direttive emanate in materia.

Assicura unità di indirizzo e coordinamento dei compiti e delle attività degli ufficiali ed agenti di pubblica sicurezza nella provincia, promuovendo le misure occorrenti.

A tali fini il prefetto deve essere tempestivamente informato dal questore e dai comandanti provinciali dell'Arma dei carabinieri e della Guardia di finanza su quanto comunque abbia attinenza con l'ordine e la sicurezza pubblica nella provincia.

Il prefetto dispone della forza pubblica e delle altre forze eventualmente poste a sua disposizione in base alle leggi vigenti e ne coordina le attività.

Il prefetto trasmette al Ministro dell'interno relazioni sull'attività delle forze di polizia in riferimento ai compiti di cui al presente articolo.

Il prefetto tiene informato il commissario del Governo nella regione sui provvedimenti che adotta nell'esercizio dei poteri ad esso attribuiti dalla presente legge.».

«Art. 14 *(Questore).* — Il questore è autorità provinciale di pubblica sicurezza.

Il questore ha la direzione, la responsabilità e il coordinamento, a livello tecnico operativo, dei servizi di ordine e di sicurezza pubblica e dell'impiego a tal fine della forza pubblica e delle altre forze eventualmente poste a sua disposizione.

A tale scopo il questore deve essere tempestivamente informato dai comandanti locali dell'Arma dei carabinieri e della Guardia di finanza su quanto comunque abbia attinenza con l'ordine e la sicurezza pubblica.».

«Art. 15 *(Autorità locali di pubblica sicurezza).* — Sono autorità locali di pubblica sicurezza il questore nel capoluogo di provincia e i funzionari preposti ai commissariati di polizia aventi competenza negli altri comuni.

Ove non siano istituiti commissariati di polizia, le attribuzioni di autorità locale di pubblica sicurezza sono esercitate dal sindaco quale ufficiale di Governo.

Quando eccezionali esigenze di servizio lo richiedono, il prefetto, o il questore su autorizzazione del prefetto, può inviare funzionari della Polizia di Stato, nei comuni di cui al comma precedente, per assumere temporaneamente la direzione dei servizi di pubblica sicurezza.

Resta in tale caso sospesa la competenza dell'autorità locale di pubblica sicurezza. Le autorità provinciali di pubblica sicurezza, ai fini dell'ordine e della sicurezza pubblica e della prevenzione e difesa dalla violenza eversiva, sollecitano la collaborazione delle amministrazioni locali e mantengono rapporti con i sindaci dei comuni.».

«Art. 16 *(Forze di polizia)*. — Ai fini della tutela dell'ordine e della sicurezza pubblica, oltre alla polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze:

*a)* l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza;

*b)* il Corpo della guardia di finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica.

Fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, sono altresì forze di polizia e possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica il Corpo degli agenti di custodia e il Corpo forestale dello Stato.

Le forze di polizia possono essere utilizzate anche per il servizio di pubblico soccorso.».

— Si riporta il testo dell'art. 1, comma 3, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133 «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica»:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

3. Entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative, adottato su proposta del CISR:

*a)* sono definite le procedure secondo cui i soggetti di cui al comma 2-*bis* notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera *b)*, al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato;

*b)* sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea relative:

1) alla struttura organizzativa preposta alla gestione della sicurezza;

1-*bis*) alle politiche di sicurezza e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti.».

*Note all'art. 12:*

— Si riporta il testo dell'art. 1-*bis* del decreto-legge 15 marzo 2021, n. 21, convertito con modificazioni dalla legge 11 maggio 2012, n. 56 «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»:

«Art. 1-*bis (Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G)*. — 1. Costituiscono, ai fini dell'esercizio dei poteri di cui al comma 2, attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

2. La stipula di contratti o accordi aventi ad oggetto l'acquisizione, a qualsiasi titolo, di beni o servizi relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di cui al comma 1, ovvero l'acquisizione, a qualsiasi titolo, di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'Unione europea, è soggetta alla notifica di cui al comma 3-*bis*, al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni. A tal fine, 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, compresi quelli individuati sulla base dei principi e delle linee guida elaborati a livello internazionale e dall'Unione europea.

2-*bis*. In sede di prima applicazione delle disposizioni di cui al comma 2, l'impresa notificante fornisce un'informativa completa sui contratti o accordi di cui al primo periodo del medesimo comma 2, conclusi prima del 26 marzo 2019 e che non sono in corso di esecuzione.

3. Per le finalità di cui ai commi 2 e 2-*bis*, per soggetto esterno all'Unione europea si intende il soggetto di cui all'articolo 2, comma 5-*bis*.

3-*bis*. Entro dieci giorni dalla conclusione di un contratto o accordo di cui al comma 2, l'impresa che ha acquisito, a qualsiasi titolo, i beni o i servizi di cui allo stesso comma notifica alla Presidenza del Consiglio dei ministri un'informativa completa, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni. Entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunica l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. Qualora sia necessario svolgere approfondimenti riguardanti aspetti tecnici relativi alla valutazione di possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, il termine di trenta giorni previsto dal presente comma può essere prorogato fino a venti giorni, prorogabili ulteriormente di venti giorni, per una sola volta, in casi di particolare complessità. I poteri speciali sono esercitati nella forma dell'imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. Decorsi i predetti termini, i poteri speciali si intendono non esercitati. Qualora si renda necessario richiedere informazioni all'acquirente, tale termine è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Qualora si renda necessario formulare richieste istruttorie a soggetti terzi, il predetto termine di trenta giorni è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di venti giorni. Le richieste di informazioni e le richieste istruttorie a soggetti terzi successive alla prima non sospendono i termini. In caso di incompletezza della notifica, il termine di trenta giorni previsto dal presente comma decorre dal ricevimento delle informazioni o degli elementi che la integrano. Fermo restando quanto previsto dall'undicesimo periodo del presente comma, nel caso in cui l'impresa notificante abbia iniziato l'esecuzione del contratto o dell'accordo oggetto della notifica prima che sia decorso il termine per l'esercizio dei poteri speciali, il Governo, nel provvedimento di esercizio dei predetti poteri, può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore all'esecuzione del predetto contratto o accordo. Salvo che il fatto costituisca reato, chiunque non osservi gli obblighi di notifica di cui al presente articolo ovvero le disposizioni contenute nel provvedimento di esercizio dei poteri speciali è soggetto alla sanzione amministrativa pecuniaria fino al 150 per cento del valore dell'operazione e comunque non inferiore al 25 per cento del medesimo valore. Nei casi di violazione degli obblighi di notifica di cui al presente articolo, anche in assenza della notifica, la Presidenza del Consiglio dei Ministri può avviare il procedimento ai fini dell'eventuale esercizio dei poteri speciali. A tale scopo, trovano applicazione i termini e le norme procedurali previsti dal presente comma. Il termine di trenta giorni di cui al presente comma decorre dalla conclusione del procedimento di accertamento della violazione dell'obbligo di notifica.

4. Con decreto del Presidente del Consiglio dei ministri, sentito il Gruppo di coordinamento costituito ai sensi dell'articolo 3 del decreto del Presidente del Consiglio dei ministri del 6 agosto 2014, possono

essere individuate misure di semplificazione delle modalità di notifica, dei termini e delle procedure relativi all'istruttoria ai fini dell'eventuale esercizio dei poteri di cui al comma 2.».

*Note all'art. 15:*

— Si riporta il testo dell'art. 29 del citato decreto legislativo 7 marzo 2005, n. 82:

«Art. 29 *(Qualificazione dei fornitori di servizi)*. — 1. I soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata presentano all'AgID domanda di qualificazione, secondo le modalità fissate dalle Linee guida.

2. Ai fini della qualificazione, i soggetti di cui al comma 1 devono possedere i requisiti di cui all'articolo 24 del Regolamento (UE) 23 luglio 2014, n. 910/2014, disporre di requisiti di onorabilità, affidabilità, tecnologici e organizzativi compatibili con la disciplina europea, nonché di garanzie assicurative adeguate rispetto all'attività svolta. Con decreto del Presidente del Consiglio dei ministri, o del Ministro delegato per l'innovazione tecnologica e la digitalizzazione, sentita l'AgID, nel rispetto della disciplina europea, sono definiti i predetti requisiti in relazione alla specifica attività che i soggetti di cui al comma 1 intendono svolgere. Il predetto decreto determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento delle predette attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche.

[3. Fatto salvo quanto previsto dall'articolo 44-*bis*, comma 3, del presente decreto e dall'articolo 14, comma 3, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, il richiedente deve inoltre possedere i requisiti individuati con decreto del Presidente del Consiglio dei ministri da fissare in base ai seguenti criteri:

*a)* per quanto riguarda il capitale sociale, graduazione entro il limite massimo di cinque milioni di euro, in proporzione al livello di servizio offerto;

*b)* per quanto riguarda le garanzie assicurative, graduazione in modo da assicurarne l'adeguatezza in proporzione al livello di servizio offerto.].

4. La domanda di qualificazione si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità di AgID o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto da AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. - 8.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse di AgID, senza nuovi o maggiori oneri per la finanza pubblica.».

— Si riporta il testo dell'art. 1, comma 2-*bis*, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

2-*bis*. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera *a)*, è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CISR, entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2. Il predetto atto amministrativo, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità di cui al presente comma.».

— Si riporta il testo dell'art. 42 della legge 3 agosto 2007, n. 124 «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»:

«Art. 42 *(Classifiche di segretezza)*. — 1. Le classifiche di segretezza sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali.

1-*bis*. Per la trattazione di informazioni classificate segretissimo, segreto e riservatissimo è necessario altresì il possesso del nulla osta di sicurezza (NOS).

2. La classifica di segretezza è apposta, e può essere elevata, dall'autorità che forma il documento, l'atto o acquisisce per prima la notizia, ovvero è responsabile della cosa, o acquisisce dall'estero documenti, atti, notizie o cose.

3. Le classifiche attribuibili sono: segretissimo, segreto, riservatissimo, riservato. Le classifiche sono attribuite sulla base dei criteri ordinariamente seguiti nelle relazioni internazionali.

4. Chi appone la classifica di segretezza individua, all'interno di ogni atto o documento, le parti che devono essere classificate e fissa specificamente il grado di classifica corrispondente ad ogni singola parte.

5. La classifica di segretezza è automaticamente declassificata a livello inferiore quando sono trascorsi cinque anni dalla data di apposizione; decorso un ulteriore periodo di cinque anni, cessa comunque ogni vincolo di classifica.

6. La declassificazione automatica non si applica quando, con provvedimento motivato, i termini di efficacia del vincolo sono prorogati dal soggetto che ha proceduto alla classifica o, nel caso di proroga oltre il termine di quindici anni, dal Presidente del Consiglio dei ministri.

7. Il Presidente del Consiglio dei ministri verifica il rispetto delle norme in materia di classifiche di segretezza. Con apposito regolamento sono determinati l'ambito dei singoli livelli di segretezza, i soggetti cui è conferito il potere di classifica e gli uffici che, nell'ambito della pubblica amministrazione, sono collegati all'esercizio delle funzioni di informazione per la sicurezza della Repubblica, nonché i criteri per l'individuazione delle materie oggetto di classifica e i modi di accesso nei luoghi militari o in quelli definiti di interesse per la sicurezza della Repubblica.

8. Qualora l'autorità giudiziaria ordini l'esibizione di documenti classificati per i quali non sia opposto il segreto di Stato, gli atti sono consegnati all'autorità giudiziaria richiedente, che ne cura la conservazione con modalità che ne tutelino la riservatezza, garantendo il diritto delle parti nel procedimento a prenderne visione senza estrarne copia.

9. Chiunque illegittimamente distrugge documenti del DIS o dei servizi di informazione per la sicurezza, in ogni stadio della declassificazione, nonché quelli privi di ogni vincolo per decorso dei termini, è punito con la reclusione da uno a cinque anni.».

— Si riporta il testo dell'art. 1, comma 8, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

8. I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-*ter*, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:

*a)* osservano le misure di sicurezza previste, rispettivamente, dai predetti decreti legislativi, ove di livello almeno equivalente a quelle adottate ai sensi del comma 3, lettera *b)*, del presente articolo; le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto sono definite dalla Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-*bis*, e dal Ministero dello sviluppo economico per i soggetti privati di cui al medesimo comma, avvalendosi anche del CVCN; il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri si raccordano, ove necessario, con le autorità competenti di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65;

*b)* assolvono l'obbligo di notifica di cui al comma 3, lettera *a)*, che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, e delle correlate disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera *a)*, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice di cui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT

italiano inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera *a)*, all'autorità competente di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.».

— Si riporta il testo dell'art. 7 del citato decreto legislativo 18 maggio 2018, n. 65:

«Art. 7 *(Autorità nazionali competenti e punto di contatto unico)*. — 1. Sono designate quali Autorità competenti NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III:

*a)* il Ministero dello sviluppo economico per il settore energia, sottosettori energia elettrica, gas e petrolio e per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;

*b)* il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;

*c)* 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, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;

*d)* il Ministero della salute per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera *a)*, del decreto legislativo 4 marzo 2014, n. 38, 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;

*e)* 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.

2. Le Autorità competenti NIS sono responsabili dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigilano sull'applicazione del presente decreto a livello nazionale esercitando altresì le relative potestà ispettive e sanzionatorie.

3. Il Dipartimento delle informazioni per la sicurezza (DIS) è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.

4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.

5. Il punto di contatto unico collabora nel gruppo di cooperazione in modo effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.

6. Le autorità competenti NIS e il punto di contatto unico consultano, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella delle autorità competenti NIS, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicità.

8. Agli oneri derivanti dal presente articolo pari a 1.300.000 euro a decorrere dal 2018, si provvede ai sensi dell'articolo 22.».

*Note all'art. 16:*

— Si riporta il testo degli articoli 7 e 8 della citata legge 7 agosto 1990, n. 241:

«Art. 7 *(Comunicazione di avvio del procedimento)*. — 1. Ove non sussistano ragioni di impedimento derivanti da particolari esigenze di celerità del procedimento, l'avvio del procedimento stesso è comunicato, con le modalità previste dall'articolo 8, ai soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti ed a quelli che per legge debbono intervenirvi. Ove parimenti non sussistano le ragioni di impedimento predette, qualora da un provvedimento possa derivare un pregiudizio a soggetti individuati o facilmente individuabili, diversi dai suoi diretti destinatari, l'amministrazione è tenuta a fornire loro, con le stesse modalità, notizia dell'inizio del procedimento.

2. Nelle ipotesi di cui al comma 1 resta salva la facoltà dell'amministrazione di adottare, anche prima della effettuazione delle comunicazioni di cui al medesimo comma 1, provvedimenti cautelari.».

«Art. 8 *(Modalità e contenuti della comunicazione di avvio del procedimento)*. — 1. L'amministrazione provvede a dare notizia dell'avvio del procedimento mediante comunicazione personale.

2. Nella comunicazione debbono essere indicati:

*a)* l'amministrazione competente;

*b)* l'oggetto del procedimento promosso;

*c)* l'ufficio, il domicilio digitale dell'amministrazione e la persona responsabile del procedimento;

c-*bis*) la data entro la quale, secondo i termini previsti dall'articolo 2, commi 2 o 3, deve concludersi il procedimento e i rimedi esperibili in caso di inerzia dell'amministrazione;

c-*ter*) nei procedimenti ad iniziativa di parte, la data di presentazione della relativa istanza;

*d)* le modalità con le quali, attraverso il punto di accesso telematico di cui all'articolo 64-*bis* del decreto legislativo 7 marzo 2005, n. 82 o con altre modalità telematiche, è possibile prendere visione degli atti, accedere al fascicolo informatico di cui all'articolo 41 dello stesso decreto legislativo n. 82 del 2005 ed esercitare in via telematica i diritti previsti dalla presente legge;

d-*bis*) l'ufficio dove è possibile prendere visione degli atti che non sono disponibili o accessibili con le modalità di cui alla lettera *d)*.

3. Qualora per il numero dei destinatari la comunicazione personale non sia possibile o risulti particolarmente gravosa, l'amministrazione provvede a rendere noti gli elementi di cui al comma 2 mediante forme di pubblicità idonee di volta in volta stabilite dall'amministrazione medesima.

4. L'omissione di taluna delle comunicazioni prescritte può esser fatta valere solo dal soggetto nel cui interesse la comunicazione è prevista.».

*Note all'art. 17:*

— Si riporta il testo dell'art. 1, comma 9, del citato decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — (*Omissis*).

9. Salvo che il fatto costituisca reato:

*a)* il mancato adempimento degli obblighi di predisposizione, di aggiornamento e di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

*b)* il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera *a)*, nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

*c)* l'inosservanza delle misure di sicurezza di cui al comma 3, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

*d)* la mancata comunicazione di cui al comma 6, lettera *a)*, nei termini prescritti, è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

*e)* l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera *b)*, in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN ovvero dai Centri di valutazione di cui al comma 6, lettera *a)*, è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

*f)* la mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera *a)*, da parte dei soggetti di cui al medesimo comma 6, lettera *b)*, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

*g)* il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica svolte ai sensi del comma 6, lettera *c)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

*h)* il mancato rispetto delle prescrizioni di cui al comma 7, lettera *b)*, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.».

**21G00060**