TESTI COORDINATI E AGGIORNATI

Testo del decreto-legge 14 giugno 2021, n. 82 (in *Gazzetta Ufficiale* - Serie generale - n. 140 del 14 giugno 2021)**, coordinato con la legge di conversione 4 agosto 2021, n. 109** (in questa stessa *Gazzetta Ufficiale* - alla pag. 1)**, recante: «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».**

AVVERTENZA:

Il testo coordinato qui pubblicato è stato redatto dal Ministero della giustizia ai sensi dell'art. 11, comma 1, 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, nonché dell'art. 10, comma 3, del medesimo testo unico, al solo fine di facilitare la lettura sia delle disposizioni del decreto-legge, integrate con le modifiche apportate dalla legge di conversione, che di quelle richiamate nel decreto, trascritte nelle note. Restano invariati il valore e l'efficacia degli atti legislativi qui riportati.

Le modifiche apportate dalla legge di conversione sono stampate con caratteri corsivi.

A norma dell'art. 15, comma 5, della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri), le modifiche apportate dalla legge di conversione hanno efficacia dal giorno successivo a quello della sua pubblicazione.

Per gli atti dell'Unione europea vengono forniti gli estremi di pubblicazione nella Gazzetta Ufficiale dell'Unione europea (GUUE).

Art. 1.

Definizioni

1. Ai fini del presente decreto si intende per:

a) cybersicurezza, l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico;

b) resilienza nazionale nello spazio cibernetico, le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera f)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;*

c) decreto-legge perimetro, il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

d) decreto legislativo NIS, il decreto legislativo 18 maggio 2018, n. 65, di 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;

e) strategia nazionale di cybersicurezza, la strategia di cui all'articolo 6 del decreto legislativo NIS.

Riferimenti normativi:

— La legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», è pubblicata nella *Gazzetta Ufficiale* 13 agosto 2007, n. 187.

— Si riporta il testo dell'articolo 1, comma 1, lettera *f)*, del 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), pubblicato nella *Gazzetta Ufficiale* 21 ottobre 2020, n. 261:

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

a) - e) omissis;

f) pregiudizio per la sicurezza nazionale, danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale di cui all'articolo 2;

g) – z) omissis.».

— Il decreto-legge 21 settembre 2019, n. 105, pubblicato nella *Gazzetta Ufficiale* 21 settembre 2019, n. 222, è stato convertito, con modificazioni, dalla legge 18 novembre 2019, recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica», pubblicata nella *Gazzetta Ufficiale* 20 novembre 2019, n. 272.

— Il decreto legislativo 18 maggio 2018, n. 65, recante «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», è pubblicato nella *Gazzetta Ufficiale* 9 giugno 2018, n. 132.

— Si riporta il testo dell'articolo 5 della citata legge n. 124 del 2007:

«Art. 5 *(Comitato interministeriale per la sicurezza della Repubblica)*. — 1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la sicurezza della Repubblica (CISR) con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza.

2. Il Comitato elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza, delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico e dal Ministro della transizione ecologica.

4. Il direttore generale del DIS svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, i direttori dell'AISE e dell'AISI, nonché altre autorità civili e militari di cui di volta in volta sia ritenuta necessaria la presenza in relazione alle questioni da trattare.».

— Il testo dell'articolo 6 del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge, è il seguente:

«Art. 6 *(Strategia nazionale di* cybersicurezza*)*. — 1. Il Presidente del Consiglio dei ministri adotta, sentito il *Comitato interministeriale per la cybersicurezza (CIC)*, la strategia nazionale di cybersicurezza per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

2. Nell'ambito della strategia nazionale di *cybersicurezza*, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto:

a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi;

b) il quadro di governance per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti;

c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;

d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;

e) i piani di ricerca e sviluppo;

f) un piano di valutazione dei rischi;

g) l'elenco dei vari attori coinvolti nell'attuazione.

3. Con la procedura di cui al comma 1 sono adottate linee di indirizzo per l'attuazione della strategia nazionale di *cybersicurezza*.

4. *L'Agenzia per la cybersicurezza* trasmette la strategia nazionale in materia di *cybersicurezza* alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.».

Art. 2.

Competenze del Presidente del Consiglio dei ministri

1. Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza;

b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;

c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5*, previa deliberazione del Consiglio dei ministri.*

2. Ai fini dell'esercizio delle competenze di cui al comma 1, lettera *a)*, e dell'attuazione della strategia nazionale di cybersicurezza, il Presidente del Consiglio dei ministri, sentito il CIC, impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale.

3. Il Presidente del Consiglio dei ministri informa preventivamente *il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), di cui all'articolo 30 della legge 3 agosto 2007, n. 124, e le Commissioni parlamentari competenti* circa le nomine di cui al comma 1, lettera c)*, del presente articolo.*

Riferimenti normativi:

— Si riporta il testo dell'articolo 30 della citata legge n. 124 del 2007:

«Art. 30 *(Comitato parlamentare per la sicurezza della Repubblica)*. — 1. È istituito il Comitato parlamentare per la sicurezza della Repubblica, composto da cinque deputati e cinque senatori, nominati entro venti giorni dall'inizio di ogni legislatura dai Presidenti dei due rami del Parlamento in proporzione al numero dei componenti dei gruppi parlamentari, garantendo comunque la rappresentanza paritaria della maggioranza e delle opposizioni e tenendo conto della specificità dei compiti del Comitato.

2. Il Comitato verifica, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione, delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni.

2-*bis*. È compito del Comitato accertare il rispetto di quanto stabilito dall'articolo 8, comma 1, nonché verificare che le attività di informazione previste dalla presente legge svolte da organismi pubblici non appartenenti al Sistema di informazione per la sicurezza rispondano ai principi della presente legge.

3. L'ufficio di presidenza, composto dal presidente, da un vicepresidente e da un segretario, è eletto dai componenti del Comitato a scrutinio segreto. Il presidente è eletto tra i componenti appartenenti ai gruppi di opposizione e per la sua elezione è necessaria la maggioranza assoluta dei componenti.

4. Se nessuno riporta tale maggioranza, si procede al ballottaggio tra i due candidati che hanno ottenuto il maggiore numero di voti.

5. In caso di parità di voti è proclamato eletto o entra in ballottaggio il più anziano di età.

6. Per l'elezione, rispettivamente, del vicepresidente e del segretario, ciascun componente scrive sulla propria scheda un solo nome. Sono eletti coloro che hanno ottenuto il maggior numero di voti. In caso di parità di voti si procede ai sensi del comma 5.».

Art. 3.

Autorità delegata

1. Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare *all'Autorità* di cui all'articolo 3 della *legge 3 agosto 2007, n. 124, ove istituita, denominata di seguito: «Autorità delegata»,* le funzioni di cui al presente decreto che non sono ad esso attribuite in via esclusiva.

2. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate ai sensi del presente decreto e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

3. L'Autorità delegata, in relazione alle funzioni delegate ai sensi del presente decreto, partecipa alle riunioni del Comitato interministeriale per la transizione digitale di cui all'articolo 8 del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55.

Riferimenti normativi:

— Si riporta il testo dell'articolo 3 della citata legge n. 124 del 2007, come modificato dalla presente legge:

«Art. 3 *(Autorità delegata)*. — 1. Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva soltanto ad un Ministro senza portafoglio o ad un Sottosegretario di Stato, di seguito denominati «Autorità delegata».

1-*bis*. L'Autorità delegata non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei Ministri a norma della presente legge *e in materia di cybersicurezza*.

2.

3. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

4. In deroga a quanto previsto dal comma 1 dell'articolo 9 della legge 23 agosto 1988, n. 400, e successive modificazioni, non è richiesto il parere del Consiglio dei ministri per il conferimento delle deleghe di cui al presente articolo al Ministro senza portafoglio.».

— Si riporta il testo dell'articolo 8 del decreto-legge 1° marzo 2021, n. 22 (Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri), pubblicato nella *Gazzetta Ufficiale* 1° marzo 2021, n. 51, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55, pubblicata nella *Gazzetta Ufficiale* 29 aprile 2021, n. 102:

«Art. 8 *(Funzioni in materia di innovazione tecnologica e transizione digitale e istituzione del Comitato interministeriale per la tran-*

sizione digitale). — 1. All'articolo 5, comma 3, della legge 23 agosto 1988, n. 400, dopo la lettera *b)*, è aggiunta la seguente:

«b-*bis*) promuove, indirizza, coordina l'azione del Governo nelle materie dell'innovazione tecnologica, dell'attuazione dell'agenda digitale italiana ed europea, della strategia italiana per la banda ultralarga, della digitalizzazione delle pubbliche amministrazioni e delle imprese, nonché della trasformazione, crescita e transizione digitale del Paese, in ambito pubblico e privato, dell'accesso ai servizi in rete, della connettività, delle infrastrutture digitali materiali e immateriali e della strategia nazionale dei dati pubblici.».

2. È istituito presso la Presidenza del Consiglio dei ministri il Comitato interministeriale per la transizione digitale (CITD), con il compito di assicurare, nelle materie di cui all'articolo 5, comma 3, lettera b-*bis*), della legge 23 agosto 1988, n. 400, come modificato dal presente decreto, il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria. Sono in ogni caso ricomprese prioritariamente nelle materie di competenza del Comitato, le attività di coordinamento e monitoraggio dell'attuazione delle iniziative relative:

a) alla strategia nazionale italiana per la banda ultralarga, alle reti di comunicazione elettronica satellitari, terrestri mobili e fisse;

b) al fascicolo sanitario elettronico e alla piattaforma dati sanitari;

c) allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della blockchain.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri o dal Ministro delegato per l'innovazione tecnologica e la transizione digitale, ove nominato, ed è composto dai Ministri per la pubblica amministrazione, ove nominato, dell'economia e delle finanze, della giustizia, dello sviluppo economico e della salute. Ad esso partecipano altresì gli altri Ministri o loro delegati aventi competenza nelle materie oggetto dei provvedimenti e delle tematiche poste all'ordine del giorno.

4. Alle riunioni del CITD, quando si trattano materie che interessano le regioni e le province autonome, partecipano il presidente della Conferenza delle regioni e delle province autonome o un presidente di regione o di provincia autonoma da lui delegato e, per i rispettivi ambiti di competenza, il presidente dell'Associazione nazionale dei comuni italiani (ANCI) e il presidente dell'Unione delle province d'Italia (UPI).

5. Il Presidente convoca il Comitato, ne determina l'ordine del giorno, ne definisce le modalità di funzionamento e ne cura, anche per il tramite della Segreteria tecnico-amministrativa di cui al comma 7, le attività propedeutiche e funzionali allo svolgimento dei lavori e all'attuazione delle deliberazioni. Il CITD garantisce adeguata pubblicità ai propri lavori.

6. Ferme restando le ordinarie competenze delle pubbliche amministrazioni sulle attività di attuazione dei singoli progetti, il CITD svolge compiti di:

a) esame delle linee strategiche, delle attività e dei progetti di innovazione tecnologica e transizione digitale di ciascuna amministrazione, anche per valorizzarli e metterli in connessione tra loro in modo da realizzare efficaci azioni sinergiche;

b) esame delle modalità esecutive più idonee a realizzare i progetti da avviare o già avviati;

c) monitoraggio delle azioni e dei progetti in corso volto a verificare lo stato dell'attuazione delle attività, individuare eventuali disfunzioni o criticità e, infine, elaborare possibili soluzioni e iniziative.

7. Presso la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale è costituita la Segreteria tecnico-amministrativa del CITD con funzioni di supporto e collaborazione per la preparazione e lo svolgimento dei lavori e per il compimento delle attività di attuazione delle deliberazioni del Comitato. La Segreteria tecnico-amministrativa è composta da personale del contingente di cui al comma 9. Possono essere chiamati a partecipare ai lavori della segreteria tecnico-amministrativa rappresentanti delle pubbliche amministrazioni partecipanti al Comitato, ai quali non sono corrisposti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

8. Restano ferme le competenze e le funzioni attribuite dalla legge, in via esclusiva, al Presidente del Consiglio dei ministri in materia di innovazione tecnologica e di transizione digitale.

9. Presso la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la transizione digitale opera un contingente composto da esperti in possesso di specifica ed elevata competenza nello studio, supporto, sviluppo e gestione di processi di trasformazione tecnologica e digitale nominati ai sensi dell'articolo 9, comma 2, del decreto legislativo 30 luglio 1999, n. 303, ovvero anche da personale non dirigenziale, collocato fuori ruolo o in posizione di comando o altra analoga posizione, prevista dagli ordinamenti di appartenenza, proveniente da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, al quale si applica la disposizione dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, nonché del personale delle forze di polizia. A tal fine è autorizzata la spesa nel limite massimo di euro 2.200.000 per l'anno 2021 e di euro 3.200.000 annui a decorrere dall'anno 2022.

10. Con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per l'innovazione tecnologica e la transizione digitale, ove nominato, sono individuati il contingente di cui al comma 9, la sua composizione ed i relativi compensi, nel limite massimo individuale annuo di 90.000 euro al lordo degli oneri a carico dell'amministrazione.

11. Il contingente di cui all'articolo 42, comma 1, del decreto-legge 30 dicembre 2019, n. 162, convertito, con modificazioni, dalla legge 28 febbraio 2020, n. 8, è incrementato di 15 unità nel limite massimo di spesa di euro 600.000 annui a decorrere dal 2021.

11-*bis*. Al fine di garantire al Ministro per l'innovazione tecnologica e la transizione digitale l'adeguato supporto delle professionalità necessarie all'esercizio delle funzioni di cui al presente articolo nonché allo svolgimento delle attività di coordinamento e di monitoraggio dell'attuazione dei progetti in materia di transizione digitale previsti dal Piano nazionale di ripresa e resilienza (PNRR), all'articolo 76 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, sono apportate le seguenti modificazioni:

a) al comma 1, le parole: «Al fine di dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus COVID-19, con particolare riferimento» sono sostituite dalle seguenti: «Al fine di provvedere» e le parole: «fino al 31 dicembre 2021» sono soppresse;

b) alla rubrica, le parole: «per l'attuazione delle misure di contrasto all'emergenza COVID-19» sono soppresse.».

Art. 4.

Comitato interministeriale per la cybersicurezza

1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

2. Il Comitato:

a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale;

b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;

c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza;

d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Mini-

stro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

4. Il direttore generale dell'Agenzia *per la cybersicurezza nazionale* svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

6. Il Comitato svolge altresì le funzioni già attribuite al *Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della legge 3 agosto 2007, n. 124,* dal decreto-legge perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro.

Riferimenti normativi:

— Per il testo dell'articolo 5 della citata legge n. 124 del 2007, si veda nei riferimenti normativi all'articolo 1.

— Si riporta il testo dell'articolo 5 del citato decreto-legge n. 105 del 2019:

«Art. 5 *(Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica)*. — 1. Il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può comunque disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

1-*bis*. Il Presidente del Consiglio dei ministri informa entro trenta giorni il Comitato parlamentare per la sicurezza della Repubblica delle misure disposte ai sensi del comma 1.».

Art. 5.

Agenzia per la cybersicurezza nazionale

1. È istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, l'Agenzia per la cybersicurezza nazionale, denominata ai fini del presente decreto «Agenzia», con sede in Roma.

2. L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal presente decreto. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono dell'Agenzia per l'esercizio delle competenze di cui al presente decreto.

3. Il direttore generale dell'Agenzia è nominato tra soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della *legge 23 agosto 1988, n. 400*, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. Il *direttore* generale ed il *vice direttore* generale, ove provenienti da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza. Per quanto previsto dal presente decreto, il direttore generale dell'Agenzia è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia. Il direttore generale ha la rappresentanza legale dell'Agenzia.

4. L'attività dell'Agenzia è regolata dal presente decreto e dalle disposizioni la cui adozione è prevista dallo stesso.

5. L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni*, delle Forze armate,* delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali.

6. Il COPASIR*, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124,* può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.

Riferimenti normativi:

— Si riporta il testo dell'articolo 18 della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri), pubblicata nella *Gazzetta Ufficiale* 12 settembre 1988, n. 214, S.O.:

«Art. 18*(Segretariato generale della Presidenza del Consiglio dei ministri)*. — 1.

2. Al Segretariato è preposto un segretario generale, nominato con decreto del Presidente del Consiglio dei ministri, tra i magistrati delle giurisdizioni superiori ordinaria ed amministrativa, gli avvocati dello Stato, i dirigenti generali dello Stato ed equiparati, i professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione. Il Presidente del Consiglio dei ministri può, con proprio decreto, nominare altresì il vicesegretario generale scelto tra le predette categorie. Con la medesima procedura può essere disposta la revoca del decreto di nomina del segretario generale e del vicesegretario generale.

3. I decreti di nomina del segretario generale, del vicesegretario generale, dei capi dei dipartimenti e degli uffici di cui all'articolo 21 cessano di avere efficacia dalla data del giuramento del nuovo Governo. Il segretario generale, il vicesegretario generale ed i capi dei dipartimenti e degli uffici di cui all'articolo 21, ove pubblici dipendenti e non appartenenti al ruolo della Presidenza del Consiglio dei ministri, sono collocati fuori ruolo nelle amministrazioni di provenienza. Sono del pari collocati obbligatoriamente fuori ruolo nelle amministrazioni di appartenenza, oltre agli esperti di cui all'articolo 3 della legge 8 marzo 1999, n. 50, i vice capi delle strutture che operano nelle aree funzionali relative al coordinamento dell'attività normativa ed amministrativa del Governo, al coordinamento degli affari economici, alla promozione dell'innovazione nel settore pubblico e coordinamento del lavoro pubblico, nonché il dirigente generale della polizia di Stato preposto all'Ispettorato generale che è adibito alla sicurezza del Presidente e delle sedi del Governo e che, per quanto attiene al suo speciale impiego, dipende funzionalmente dal Segretario generale.

4. La funzione di capo dell'ufficio stampa può essere affidata ad un elemento estraneo all'amministrazione, il cui trattamento economico è determinato in conformità a quello dei dirigenti generali dello Stato.

5.».

— Si riporta il testo dell'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro

alle dipendenze delle amministrazioni pubbliche), pubblicato nella *Gazzetta Ufficiale* 9 maggio 2001, n. 106, S.O.:

«Art. 1 *(Finalità ed ambito di applicazione)*. — 1. *omissis*.

2. Per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui aldecreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI.».

— Si riporta il testo dell'articolo 31, comma 3, della citata legge n. 124 del 2007:

«Art. 31 *(Funzioni di controllo del Comitato parlamentare per la sicurezza della Repubblica)*. — 1. - 2. (*Omissis*).

3. Il Comitato può altresì ascoltare ogni altra persona non appartenente al Sistema di informazione per la sicurezza in grado di fornire elementi di informazione o di valutazione ritenuti utili ai fini dell'esercizio del controllo parlamentare.».

Art. 6.

Organizzazione dell'Agenzia per la cybersicurezza nazionale

1. L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento che ne prevede, in particolare, l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale *nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1*.

2. Sono organi dell'Agenzia il direttore generale e il Collegio dei revisori dei conti. Con il regolamento di cui al comma 1 sono disciplinati altresì:

a) le funzioni del direttore generale e del vice direttore generale dell'Agenzia;

b) la composizione e il funzionamento del Collegio dei revisori dei conti;

c) l'istituzione di eventuali sedi secondarie.

3. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere *delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza,* del COPASIR, sentito il CIC.

Riferimenti normativi:

— Si riporta il testo dell'articolo 17 della citata legge n. 400 del 1988:

«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.».

Art. 7.

Funzioni dell'Agenzia per la cybersicurezza nazionale

1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica

sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, *paragrafo 1*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, *paragrafo 6*, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al *numero 1) della presente lettera,* al rilascio del certificato europeo di sicurezza cibernetica;

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6,lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al *Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124,* dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, *nonché quelle in materia* di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

m-bis*) assume le iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera* b)*. In particolare, l'Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali;*

m-ter*) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della di-*

sciplina dell'Unione europea e del regolamento di cui all'articolo 33-septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;*

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 8 del decreto legislativo NIS. *A tale fine, promuove iniziative di partenariato pubblico-privato, per rendere affettive tali capacità;*

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, *istituzioni ed enti*, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza *e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;*

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del *Ministero degli affari esteri* e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del *Ministero degli affari esteri* e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza *e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;*

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

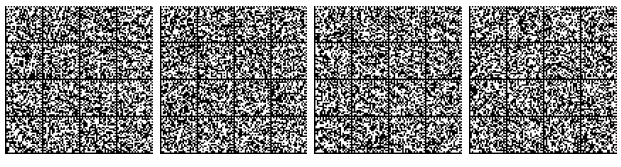
v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza*, in particolare favorendo l'attivazione di percorsi formativi universitari in materia,* anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati*; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;*

v-bis*) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;*

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

1-bis*. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere* r), s), t), u), v), z) *e* aa)*, presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.*



2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza perla cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3. Il CSIRT italiano di cui all'articolo 8 del decreto legislativo NIS è trasferito presso l'Agenzia e assume la denominazione di: «CSIRT Italia».

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

Riferimenti normativi:

— La legge 1° aprile 1981, n. 121, recante «Nuovo ordinamento dell'Amministrazione della pubblica sicurezza», è pubblicata nella *Gazzetta Ufficiale* 10 aprile 1981, n. 100, S.O..

— Si riporta il testo dell'articolo 4, comma 3, lett. *l)*, della citata legge n. 124 del 2007:

«Art. 4 *(Dipartimento delle informazioni per la sicurezza)*. — 1. - 2. (*Omissis*).

3. Il DIS svolge i seguenti compiti:

a) - *i)* (*Omissis*);

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;

m) - n-*bis*) (*Omissis*).».

— Si riporta il testo dell'articolo 9 della citata legge n. 124 del 2007:

«Art. 9 *(Tutela amministrativa del segreto e nulla osta di sicurezza)*. — 1. È istituito nell'ambito del DIS, ai sensi dell'articolo 4, comma 7, l'Ufficio centrale per la segretezza (UCSe), che svolge funzioni direttive e di coordinamento, di consulenza e di controllo sull'applicazione delle norme di legge, dei regolamenti e di ogni altra disposizione in ordine alla tutela amministrativa del segreto di Stato e alle classifiche di segretezza di cui all'articolo 42.

2. Competono all'UCSe:

a) gli adempimenti istruttori relativi all'esercizio delle funzioni del Presidente del Consiglio dei ministri quale Autorità nazionale per la sicurezza, a tutela del segreto di Stato;

b) lo studio e la predisposizione delle disposizioni esplicative volte a garantire la sicurezza di tutto quanto è coperto dalle classifiche di segretezza di cui all'articolo 42, con riferimento sia ad atti, documenti e materiali, sia alla produzione industriale;

c) il rilascio e la revoca dei nulla osta di sicurezza (NOS), previa acquisizione del parere dei direttori dei servizi di informazione per la sicurezza e, ove necessario, del Ministro della difesa e del Ministro dell'interno;

d) la conservazione e l'aggiornamento di un elenco completo di tutti i soggetti muniti di NOS.

3. Il NOS ha la durata di cinque anni per la classifica di segretissimo e di dieci anni per le classifiche segreto e riservatissimo indicate all'articolo 42, fatte salve diverse disposizioni contenute in trattati internazionali ratificati dall'Italia. A ciascuna delle tre classifiche di segretezza citate corrisponde un distinto livello di NOS.

4. Il rilascio del NOS è subordinato all'effettuazione di un preventivo procedimento di accertamento diretto ad escludere dalla conoscibilità di notizie, documenti, atti o cose classificate ogni soggetto che non dia sicuro affidamento di scrupolosa fedeltà alle istituzioni della Repubblica, alla Costituzione e ai suoi valori, nonché di rigoroso rispetto del segreto.

5. Al fine di consentire l'accertamento di cui al comma 4, le Forze armate, le Forze di polizia, le pubbliche amministrazioni e i soggetti erogatori dei servizi di pubblica utilità collaborano con l'UCSe per l'acquisizione di informazioni necessarie al rilascio dei NOS, ai sensi degli articoli 12 e 13.

6. Prima della scadenza del termine di cui al comma 3, l'UCSe può revocare il NOS se, sulla base di segnalazioni e di accertamenti nuovi, emergono motivi di inaffidabilità a carico del soggetto interessato.

7. Il regolamento di cui all'articolo 4, comma 7, disciplina il procedimento di accertamento preventivo di cui al comma 4 del presente articolo, finalizzato al rilascio del NOS, nonché gli ulteriori possibili accertamenti di cui al comma 6, in modo tale da salvaguardare i diritti dei soggetti interessati.

8. I soggetti interessati devono essere informati della necessità dell'accertamento nei loro confronti e, con esclusione del personale per il quale il rilascio costituisce condizione necessaria per l'espletamento del servizio istituzionale nel territorio nazionale e all'estero, possono rifiutarlo, rinunciando al NOS e all'esercizio delle funzioni per le quali esso è richiesto.

9. Agli appalti di lavori e alle forniture di beni e servizi, per i quali la tutela del segreto sia richiesta da norme di legge o di regolamento ovvero sia ritenuta di volta in volta necessaria, si applicano le disposizioni di cui all'articolo 17, comma 3, del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui aldecreto legislativo 12 aprile 2006, n. 163.

10. Il soggetto appaltante i lavori e le forniture di cui al comma 9, quando lo ritiene necessario, richiede, tramite l'UCSe, al Presidente del Consiglio dei ministri l'autorizzazione alla segretazione, indicandone i motivi. Contestualmente all'autorizzazione, l'UCSe trasmette al soggetto appaltante l'elenco delle ditte individuali e delle imprese munite di NOS.

11. Il dirigente preposto all'UCSe è nominato e revocato dal Presidente del Consiglio dei ministri, su proposta dell'Autorità delegata, ove istituita, sentito il direttore generale del DIS. Il dirigente presenta annualmente al direttore generale del DIS, che informa il Presidente del Consiglio dei ministri, una relazione sull'attività svolta e sui problemi affrontati, nonché sulla rispondenza dell'organizzazione e delle procedure adottate dall'Ufficio ai compiti assegnati e sulle misure da adottare per garantirne la correttezza e l'efficienza. La relazione è portata a conoscenza del CISR.».

— Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (Testo rilevante ai fini del *SEE)*, è pubblicato nella G.U.U.E. 7 giugno 2019, n. L 151.

— Si riporta il testo dell'articolo 1, comma 6, lett. *c)*, del citato decreto-legge n. 105 del 2019:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1-5 (*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) - *b)*;

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.».

— Si riporta il testo dell'articolo 3 del citato decreto del Presidente Consiglio dei ministri n. 131 del 2020:

«Art. 3 *(Settori di attività)*. — 1. Ai fini dell'inclusione nel perimetro, sono oggetto di individuazione, in applicazione del criterio di gradualità di cui all'articolo 1, comma 2, del decreto-legge, in via prioritaria, fatta salva l'estensione ad altri settori in sede di aggiornamento, i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo:

a) interno;

b) difesa;

c) spazio e aerospazio;

d) energia;

e) telecomunicazioni;

f) economia e finanza;

g) trasporti;

h) servizi digitali;

i) tecnologie critiche, di cui all'articolo 4, paragrafo 1, lettera *b)*, del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo;

l) enti previdenziali/lavoro.

2. All'espletamento delle attività di cui agli articoli 4 e 5 provvedono, per il settore governativo, le amministrazioni CISR, ciascuna nell'ambito di rispettiva competenza, e, per i settori di cui al comma 1, lettere da *a)* a *l)*, le seguenti amministrazioni:

a) per il settore interno, il Ministero dell'interno, nell'ambito delle attribuzioni di cui all'articolo 14 del decreto legislativo 30 luglio 1999, n. 300;

b) per il settore difesa, il Ministero della difesa;

c) per il settore spazio e aerospazio, la Presidenza del Consiglio dei ministri, ai sensi della legge 11 gennaio 2018, n. 7;

d) per il settore energia, il Ministero dello sviluppo economico;

e) per il settore telecomunicazioni, il Ministero dello sviluppo economico;

f) per il settore economia e finanza, il Ministero dell'economia e delle finanze;

g) per il settore trasporti, il Ministero delle infrastrutture e dei trasporti;

h) per il settore servizi digitali, il Ministero dello sviluppo economico, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione;

i) per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca;

l) per il settore enti previdenziali/lavoro, il Ministero del lavoro e delle politiche sociali.».

— Si riportano i testi degli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche), pubblicato nella *Gazzetta Ufficiale* 15 settembre 2003, n. 214, S.O.):

«Art. 16-*bis (Sicurezza e integrità)*. — 1. Fatte salve le competenze dell'Autorità previste dall'articolo 1, comma 6, lettera *a)*, numero 3), della legge 31 luglio 1997, n. 249, il Ministero, sentite le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico e tenuto conto delle misure tecniche di attuazione eventualmente adottate dalla Commissione europea, ai sensi dell'articolo 13-*bis*, comma 4, della direttiva 2002/21/CE, individua:

a) adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle reti. Tali misure sono anche finalizzate a prevenire e limitare le conseguenze per gli utenti e le reti interconnesse degli incidenti che pregiudicano la sicurezza;

b) i casi in cui le violazioni della sicurezza o perdita dell'integrità siano da considerarsi significative ai fini del corretto funzionamento delle reti o dei servizi.

2. Le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico:

a) adottano le misure individuate dal Ministero di cui al comma 1, lettera *a)*, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente, e di garantire la continuità della fornitura dei servizi su tali reti;

b) comunicano al Ministero ogni significativa violazione della sicurezza o perdita dell'integrità secondo quanto previsto al comma 1, lettera *b)*.

3. Nei casi di cui al comma 2, lettera *b)*, il Ministero informa le altre autorità nazionali eventualmente interessate per le relative iniziative di competenza, e, se del caso, informa le autorità degli altri Stati membri nonché l'ENISA.

4. Il Ministero, anche su impulso dell'Autorità, può informare il pubblico o imporre all'impresa di farlo, ove accerti che la divulgazione della violazione di cui al comma 2, lettera *b)*, sia nell'interesse pubblico. Anche a tal fine, presso il Ministero è individuato il Computer Emergency Response Team (CERT) nazionale, avvalendosi delle risorse umane, strumentali e finanziarie e disponibili, con compiti di assistenza tecnica in caso di segnalazioni da parte di utenti e di diffusione di informazioni anche riguardanti le contromisure adeguate per i tipi più comuni di incidente.

5. Il Ministero trasmette ogni anno alla Commissione europea e all'ENISA una relazione sintetica delle notifiche ricevute e delle azioni adottate conformemente al presente articolo.»

«Art. 16-*ter (Attuazione e controllo)*. — 1. Le misure adottate ai fini dell'attuazione del presente articolo e dell'articolo 16-*bis* sono approvate con decreto del Presidente del Consiglio dei ministri.

2. Ai fini del controllo del rispetto dell'articolo 16-*bis* le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico sono tenute a:

a) fornire al Ministero, e se necessario all'Autorità, le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti, in particolare i documenti relativi alle politiche di sicurezza; nonché;

b) sottostare a una verifica della sicurezza effettuata dal Ministero, anche su impulso dell'Autorità o da un organismo qualificato indipendente designato dal Ministero. L'impresa si assume l'onere finanziario della verifica

3. Il Ministero e l'Autorità hanno la facoltà di indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza e l'integrità delle reti.

4. Nel caso in cui il Ministero riscontri, anche su indicazione dell'Autorità, il mancato rispetto degliarticoli 16-*bis* o 16-*ter* ovvero delle disposizioni attuative previste dal comma 1 da parte delle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, si applicano le sanzioni di cui all'articolo 98, commi da 4 a 12.».

— Per i riferimenti del decreto legislativo NIS, si veda nei riferimenti normativi all'articolo 1.

— Si riporta il testo dell'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21 (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), pubblicato nella *Gazzetta Ufficiale* 15 marzo 2012, n. 63, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, pubblicata nella *Gazzetta Ufficiale* 14 maggio 2012, n. 111:

«Art. 1 *(Poteri speciali nei settori della difesa e della sicurezza nazionale)*. — (*Omissis*).

8. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, e successive modificazioni, previo

parere delle Commissioni parlamentari competenti, su proposta del Ministro dell'economia e delle finanze, di concerto con il Ministro degli affari esteri, il Ministro dell'interno, il Ministro della difesa e il Ministro dello sviluppo economico, sono emanate disposizioni di attuazione del presente articolo, anche con riferimento alla definizione, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico del bilancio dello Stato, delle modalità organizzative per lo svolgimento delle attività propedeutiche all'esercizio dei poteri speciali previsti dal presente articolo. Il parere di cui al primo periodo è espresso entro il termine di venti giorni dalla data di trasmissione dello schema di regolamento alle Camere. Decorso tale termine, il regolamento può essere comunque adottato. Fino all'adozione del medesimo regolamento, le competenze inerenti alle proposte per l'esercizio dei poteri speciali, di cui al comma 1, e le attività conseguenti, di cui ai commi 4 e 5, sono attribuite al Ministero dell'economia e delle finanze per le società da esso partecipate, ovvero, per le altre società, al Ministero della difesa o al Ministero dell'interno, secondo i rispettivi ambiti di competenza.».

— Si riporta il testo dell'articolo 4 della citata legge n. 124 del 2007:

«Art. 4 *(Dipartimento delle informazioni per la sicurezza)*. — 1. Per lo svolgimento dei compiti di cui al comma 3 è istituito, presso la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni per la sicurezza (DIS).

2. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza.

3. Il DIS svolge i seguenti compiti:

a) coordina l'intera attività di informazione per la sicurezza, verificando altresì i risultati delle attività svolte dall'AISE e dall'AISI, ferma restando la competenza dei predetti servizi relativamente alle attività di ricerca informativa e di collaborazione con i servizi di sicurezza degli Stati esteri;

b) è costantemente informato delle operazioni di competenza dei servizi di informazione per la sicurezza e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema di informazione per la sicurezza;

c) raccoglie le informazioni, le analisi e i rapporti provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati; ferma l'esclusiva competenza dell'AISE e dell'AISI per l'elaborazione dei rispettivi piani di ricerca operativa, elabora analisi strategiche o relative a particolari situazioni; formula valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI;

d) elabora, anche sulla base delle informazioni e dei rapporti di cui alla lettera *c)*, analisi globali da sottoporre al CISR, nonché progetti di ricerca informativa, sui quali decide il Presidente del Consiglio dei ministri, dopo avere acquisito il parere del CISR;

d-*bis*) sulla base delle direttive di cui all'articolo 1, comma 3-*bis*, nonché delle informazioni e dei rapporti di cui alla lettera *c)* del presente comma, coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

e) promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia; comunica al Presidente del Consiglio dei ministri le acquisizioni provenienti dallo scambio informativo e i risultati delle riunioni periodiche;

f) trasmette, su disposizione del Presidente del Consiglio dei ministri, sentito il CISR, informazioni e analisi ad amministrazioni pubbliche o enti, anche ad ordinamento autonomo, interessati all'acquisizione di informazioni per la sicurezza;

g) elabora, d'intesa con l'AISE e l'AISI, il piano di acquisizione delle risorse umane e materiali e di ogni altra risorsa comunque strumentale all'attività dei servizi di informazione per la sicurezza, da sottoporre all'approvazione del Presidente del Consiglio dei ministri;

h) sentite l'AISE e l'AISI, elabora e sottopone all'approvazione del Presidente del Consiglio dei ministri lo schema del regolamento di cui all'articolo 21, comma 1;

i) esercita il controllo sull'AISE e sull'AISI, verificando la conformità delle attività di informazione per la sicurezza alle leggi e ai regolamenti, nonché alle direttive e alle disposizioni del Presidente del Consiglio dei ministri. Per tale finalità, presso il DIS è istituito un ufficio ispettivo le cui modalità di organizzazione e di funzionamento sono definite con il regolamento di cui al comma 7. Con le modalità previste da tale regolamento è approvato annualmente, previo parere del Comitato parlamentare di cui all'articolo 30, il piano annuale delle attività dell'ufficio ispettivo. L'ufficio ispettivo, nell'ambito delle competenze definite con il predetto regolamento, può svolgere, anche a richiesta del direttore generale del DIS, autorizzato dal Presidente del Consiglio dei ministri, inchieste interne su specifici episodi e comportamenti verificatisi nell'ambito dei servizi di informazione per la sicurezza;

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;

m) cura le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale;

n) impartisce gli indirizzi per la gestione unitaria del personale di cui all'articolo 21, secondo le modalità definite dal regolamento di cui al comma 1 del medesimo articolo;

n-*bis*) gestisce unitariamente, ferme restando le competenze operative dell'AISE e dell'AISI, gli approvvigionamenti e i servizi logistici comuni.

4. Fermo restando quanto previsto dall'articolo 118-*bis* del codice di procedura penale, introdotto dall'articolo 14 della presente legge, qualora le informazioni richieste alle Forze di polizia, ai sensi delle lettere *c)* ed *e)* del comma 3 del presente articolo, siano relative a indagini di polizia giudiziaria, le stesse, se coperte dal segreto di cui all'articolo 329 del codice di procedura penale, possono essere acquisite solo previo nulla osta della autorità giudiziaria competente. L'autorità giudiziaria può trasmettere gli atti e le informazioni anche di propria iniziativa.

5. La direzione generale del DIS è affidata ad un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al Presidente del Consiglio dei ministri, sentito il CISR. L'incarico ha comunque la durata massima di quattro anni ed è rinnovabile con successivi provvedimenti per una durata complessiva massima di ulteriori quattro anni. Per quanto previsto dalla presente legge, il direttore del DIS è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, salvo quanto previsto dall'articolo 6, comma 5, e dall'articolo 7, comma 5, ed è gerarchicamente e funzionalmente sovraordinato al personale del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento.

6. Il Presidente del Consiglio dei ministri, sentito il direttore generale del DIS, nomina uno o più vice direttori generali; il direttore generale affida gli altri incarichi nell'ambito del Dipartimento, ad eccezione degli incarichi il cui conferimento spetta al Presidente del Consiglio dei ministri.

7. L'ordinamento e l'organizzazione del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento sono disciplinati con apposito regolamento.

8. Il regolamento previsto dal comma 7 definisce le modalità di organizzazione e di funzionamento dell'ufficio ispettivo di cui al comma 3, lettera *i)*, secondo i seguenti criteri:

a) agli ispettori è garantita piena autonomia e indipendenza di giudizio nell'esercizio delle funzioni di controllo;

b) salva specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, i controlli non devono interferire con le operazioni in corso;

c) sono previste per gli ispettori specifiche prove selettive e un'adeguata formazione;

d) non è consentito il passaggio di personale dall'ufficio ispettivo ai servizi di informazione per la sicurezza;

e) gli ispettori, previa autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, possono accedere a tutti gli atti conservati presso i servizi di informazione per la sicurezza e presso il DIS; possono altresì acquisire, tramite il direttore generale del DIS, altre informazioni da enti pubblici e privati.».

— Si riporta il testo dell'articolo 1, comma 19-*bis* del citato decreto-legge n. 105 del 2019:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 19-*bis*. Il Presidente del Consiglio dei ministri coordina la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi

con le autorità titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attività svolte.».

— Per il testo dell'articolo 5 del citato decreto-legge n. 105 del 2019, si rinvia ai riferimenti normativi dell'articolo 4.

— Si riportano i testi degli articoli 51 e 71 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), pubblicato nella *Gazzetta Ufficiale* 16 maggio 2005, n. 112, S.O.:

«Art. 51 *(Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni)*. — 1. Con le Linee guida sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture.

1-*bis*. AgID attua, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:

a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la semplificazione e la pubblica amministrazione il mancato rispetto delle regole tecniche di cui al comma 1 [(441)] da parte delle pubbliche amministrazioni

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-*bis*.

2-*ter*. I soggetti di cui all'articolo 2, comma 2, aderiscono ogni anno ai programmi di sicurezza preventiva coordinati e promossi da AgID secondo le procedure dettate dalla medesima AgID con le Linee guida.

2-*quater*. I soggetti di cui articolo 2, comma 2, predispongono, nel rispetto delle Linee guida adottate dall'AgID, piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività. Onde garantire quanto previsto, è possibile il ricorso all'articolo 15 della legge 7 agosto 1990, n. 241, per l'erogazione di servizi applicativi, infrastrutturali e di dati, con ristoro dei soli costi di funzionamento. Per le Amministrazioni dello Stato coinvolte si provvede mediante rimodulazione degli stanziamenti dei pertinenti capitoli di spesa o mediante riassegnazione alla spesa degli importi versati a tale titolo ad apposito capitolo di entrata del bilancio statale.»

«Art. 71 *(Regole tecniche)*. — 1. L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice. Le Linee guida divengono efficaci dopo la loro pubblicazione nell'apposita area del sito Internet istituzionale dell'AgID e di essa ne è data notizia nella *Gazzetta Ufficiale* della Repubblica italiana. Le Linee guida sono aggiornate o modificate con la procedura di cui al primo periodo.

1-*bis*.

1-*ter*. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.

2.».

— Si riporta il testo dell'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179 (Ulteriori misure urgenti per la crescita del Paese), pubblicato nella *Gazzetta Ufficiale* 19 ottobre 2012, n. 245, S.O., convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, pubblicata nella *Gazzetta Ufficiale* 18 dicembre 2012, n. 294, S.O.:

«Art. 33-*septies (Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese)*. — 1. -3. (*Omissis*).

4. L'Agenzia per la cybersicurezza nazionale, con proprio regolamento, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri, nel rispetto della disciplina introdotta daldecreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dallalegge 18 novembre 2019, n. 133, stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, ivi incluse le infrastrutture di cui ai commi 1 e 4-*ter*. Definisce, inoltre, le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione. Con lo stesso regolamento sono individuati i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni di cui ai commi 1 e 1-*bis*.».

— Si riporta il testo dell'articolo 8 del citato decreto legislativo n. 65 del 2018:

«Art. 8 *(Gruppi di intervento per la sicurezza informatica in caso di incidente – CSIRT)*. — 1. È istituito, presso l'Agenzia di cybersicurezza nazionale, il CSIRT Italia, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-*bis* del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

2. L'organizzazione e il funzionamento del CSIRT Italia sono disciplinati con decreto del Presidente del Consiglio dei ministri ai sensi dell'articolo 7 del decreto legislativo 30 luglio 1999, n. 303, da adottare entro il 9 novembre 2018.

3. Nelle more dell'adozione del decreto di cui al comma 2, le funzioni di CSIRT Italia sono svolte dal CERT nazionale unitamente al CERT-PA in collaborazione tra loro.

4. Il CSIRT Italia assicura la conformità ai requisiti di cui all'allegato I, punto 1, svolge i compiti di cui all'allegato I, punto 2, si occupa dei settori di cui all'allegato II e dei servizi di cui all'allegato III e dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale.

5. Il CSIRT Italia definisce le procedure per la prevenzione e la gestione degli incidenti informatici.

6. Il CSIRT Italia garantisce la collaborazione effettiva, efficiente e sicura, nella rete di CSIRT di cui all'articolo 11.

7. La Presidenza del Consiglio dei ministri comunica alla Commissione europea il mandato del CSIRT Italia e le modalità di trattamento degli incidenti a questo affidati.

8. Il CSIRT Italia, per lo svolgimento delle proprie funzioni, può avvalersi anche dell'Agenzia per l'Italia digitale.

9. Le funzioni svolte dal Ministero dello sviluppo economico in qualità di CERT nazionale ai sensi dell'articolo 16-*bis*, del decreto legislativo 1° agosto 2003, n. 259, nonché quelle svolte da Agenzia per l'Italia digitale in qualità di CERT-PA, ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, sono trasferite al CSIRT Italia a far data dalla entrata in vigore del decreto di cui al comma 2.

10. Per le spese relative al funzionamento del CSIRT Italia è autorizzata la spesa di 2.000.000 di euro annui a decorrere dall'anno 2020. A tali oneri si provvede ai sensi dell'articolo 22.».

— Il Regolamento (CE) n. 2021/887/UE del Parlamento europeo e del Consiglio 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento, è pubblicato nella G.U.U.E. 8 giugno 2021, n. L 202.

Art. 8.

Nucleo per la cybersicurezza

1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia *o, per sua delega, dal vice direttore generale* ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, *dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della*

legge 3 agosto 2007, n. 124, dell'Agenzia informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

3. I componenti *del Nucleo* possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza.

4. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10.

4-bis*. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.*

Riferimenti normativi:

— Si riporta il testo degli articoli 6 e 7 della citata legge n. 124 del 2007:

«Art. 6 *(Agenzia informazioni e sicurezza esterna)*. — 1. È istituita l'Agenzia informazioni e sicurezza esterna (AISE), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero.

2. Spettano all'AISE inoltre le attività in materia di controproliferazione concernenti i materiali strategici, nonché le attività di informazione per la sicurezza, che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISE individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISE può svolgere operazioni sul territorio nazionale soltanto in collaborazione con l'AISI, quando tali operazioni siano strettamente connesse ad attività che la stessa AISE svolge all'estero. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISE risponde al Presidente del Consiglio dei ministri.

6. L'AISE informa tempestivamente e con continuità il Ministro della difesa, il Ministro degli affari esteri e il Ministro dell'interno per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri, con proprio decreto, nomina e revoca il direttore dell'AISE, scelto tra dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha comunque la durata massima di quattro anni ed è rinnovabile con successivi provvedimenti per una durata complessiva massima di ulteriori quattro anni.

8. Il direttore dell'AISE riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISE, uno o più vice direttori. Il direttore dell'AISE affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISE sono disciplinati con apposito regolamento.»

«Art. 7 *(Agenzia informazioni e sicurezza interna)*. — 1. È istituita l'Agenzia informazioni e sicurezza interna (AISI), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

2. Spettano all'AISI le attività di informazione per la sicurezza, che si svolgono all'interno del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISI individuare e contrastare all'interno del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISI può svolgere operazioni all'estero soltanto in collaborazione con l'AISE, quando tali operazioni siano strettamente connesse ad attività che la stessa AISI svolge all'interno del territorio nazionale. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISI risponde al Presidente del Consiglio dei ministri.

6. L'AISI informa tempestivamente e con continuità il Ministro dell'interno, il Ministro degli affari esteri e il Ministro della difesa per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri nomina e revoca, con proprio decreto, il direttore dell'AISI, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha comunque la durata massima di quattro anni ed è rinnovabile con successivi provvedimenti per una durata complessiva massima di ulteriori quattro anni.

8. Il direttore dell'AISI riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISI, uno o più vice direttori. Il direttore dell'AISI affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISI sono disciplinati con apposito regolamento.».

— Per il testo dell'articolo 9 della citata legge n. 124 del 2007, si veda nei riferimenti normativi all'articolo 7.

Art. 9.

Compiti del Nucleo per la cybersicurezza

1. Per le finalità di cui all'articolo 8, il Nucleo per la cybersicurezza svolge i seguenti compiti:

a) può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia;

b) promuove, sulla base delle direttive di cui all'articolo 2, comma 2, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto dall'articolo 7-*bis*, comma 5, *del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198;*

c) promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale

a esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

d) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

e) acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dagli organismi di informazione di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno di cui all'articolo 7-*bis* del *decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155*, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (Computer Emergency Response Team–CERT) istituiti ai sensi della normativa vigente;

f) riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

g) valuta se gli eventi di cui alle lettere *e)* e *f)* assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla situazione in atto e allo svolgimento delle attività di raccordo e coordinamento di cui all'articolo 10, nella composizione ivi prevista.

Riferimenti normativi:

— Si riporta il testo dell'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174 (Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione), pubblicato nella *Gazzetta Ufficiale* 30 ottobre 2015, n. 253, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, pubblicata nella *Gazzetta Ufficiale* 16 dicembre 2015, n. 292:

«Art. 7-*bis (Disposizioni in materia di intelligence)*. — 1. Il Presidente del Consiglio dei ministri, acquisito il parere del Comitato parlamentare per la sicurezza della Repubblica, emana, ai sensi dell'articolo 1, comma 3, della legge 3 agosto 2007, n. 124, disposizioni per l'adozione di misure di intelligence di contrasto, in situazioni di crisi o di emergenza all'estero che coinvolgano aspetti di sicurezza nazionale o per la protezione di cittadini italiani all'estero, con la cooperazione di forze speciali della Difesa con i conseguenti assetti di supporto della Difesa stessa.

2. Il Presidente del Consiglio dei ministri informa il Comitato parlamentare per la sicurezza della Repubblica, con le modalità indicate nell'articolo 33, comma 4, della legge 3 agosto 2007, n. 124, delle misure di intelligence di cui al comma 1 del presente articolo.

3. Al personale delle Forze armate impiegato nell'attuazione delle attività di cui al comma 1 del presente articolo si applicano le disposizioni dell'articolo 5 del decreto-legge 30 dicembre 2008, n. 209, convertito, con modificazioni, dalla legge 24 febbraio 2009, n. 12, e successive modificazioni, dell'articolo 4, commi 1-*sexies* e 1-*septies*, del decreto-legge 4 novembre 2009, n. 152, convertito, con modificazioni, dalla legge 29 dicembre 2009, n. 197, e, ove ne ricorrano i presupposti, dell'articolo 17, comma 7, della legge 3 agosto 2007, n. 124.

4. Il comma 3 del presente articolo non si applica in nessun caso ai crimini previsti dagli articoli 5 e seguenti dello statuto istitutivo della Corte penale internazionale, adottato a Roma il 17 luglio 1998, ratificato ai sensi della legge 12 luglio 1999, n. 232.

5. Il Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124, e successive modificazioni, può essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, secondo modalità stabilite con apposito regolamento ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124.

6. Il Comitato parlamentare per la sicurezza della Repubblica, trascorsi ventiquattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, trasmette alle Camere una relazione sull'efficacia delle norme contenute nel presente articolo.».

— Per i testi degli articoli 4, 6 e 7, della citata legge n. 124 del 2007, si vedano rispettivamente i riferimenti normativi agli articoli 7 e 8.

— Si riporta il testo dell'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale), pubblicato nella *Gazzetta Ufficiale* 27 luglio 2005, n. 173, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, pubblicata nella *Gazzetta Ufficiale* 1° agosto 2005, n. 177:

«7-*bis (Sicurezza telematica)*. — 1. Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n. 801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

2. Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, gli ufficiali di polizia giudiziaria appartenenti all'organo di cui al comma 1 possono svolgere le attività di cui all'articolo 4, commi 1 e 2, del decreto-legge 18 ottobre 2001, n. 374, convertito, con modificazioni, dalla legge 15 dicembre 2001, n. 438, e quelle di cui all'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati.».

Art. 10.

Gestione delle crisi che coinvolgono aspetti di cybersicurezza

1. Nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia.

2. (*soppresso*)

3. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile, autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati. Per la partecipazione non sono

previsti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

4. È compito del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 3, assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi *di natura cibernetica* vengano espletate in maniera coordinata secondo quanto previsto dall'articolo 9, comma 1, lettera *b)*.

5. Il Nucleo, per l'espletamento delle proprie funzioni e fermo restando quanto previsto ai sensi dell'articolo 7-*bis*, comma 5, del *decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198*:

a) mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;

e) partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, *dell'Unione europea* o di organizzazioni internazionali di cui l'Italia fa parte.

Riferimenti normativi:

— Per il testo dell'articolo 7-*bis*, comma 5, del citato decreto-legge n. 174 del 2015, si veda nei riferimenti normativi all'articolo 9.

Art. 11.

Norme di contabilità e disposizioni finanziarie

1. *Con la legge di bilancio* è determinato lo stanziamento annuale da assegnare all'Agenzia da iscrivere sul capitolo di cui all'articolo 18, comma 1, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR.

2. Le entrate dell'Agenzia sono costituite da:

a) dotazioni finanziarie e contributi ordinari di cui all'articolo 18 del presente decreto;

b) corrispettivi per i servizi prestati a soggetti pubblici o privati;

c) proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;

d) altri proventi patrimoniali e di gestione;

e) contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione;

f) proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS, dal decreto-legge perimetro e dal decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

g) ogni altra eventuale entrata.

3. Il regolamento di contabilità dell'Agenzia, che ne assicura l'autonomia gestionale e contabile, è adottato con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentito il CIC, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme di contabilità generale dello Stato e nel rispetto dei princìpi fondamentali da esse stabiliti, nonché delle seguenti disposizioni:

a) il bilancio preventivo e il bilancio consuntivo adottati dal direttore generale dell'Agenzia sono approvati con decreto del Presidente del Consiglio dei ministri, previo parere del CIC, e sono trasmessi alla Corte dei conti che esercita il controllo previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20;

b) il bilancio consuntivo e la relazione della Corte dei conti *sono trasmessi alle Commissioni parlamentari competenti e al* COPASIR.

4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme in materia di contratti pubblici, previo parere del COPASIR e sentito il CIC, sono definite le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, ferma restando la disciplina dell'articolo 162 del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50.

Riferimenti normativi:

— Per i riferimenti del decreto legislativo 18 maggio 2018, n. 65 e del decreto-legge 21 settembre 2019, si rinvia ai riferimenti normativi all'articolo 1.

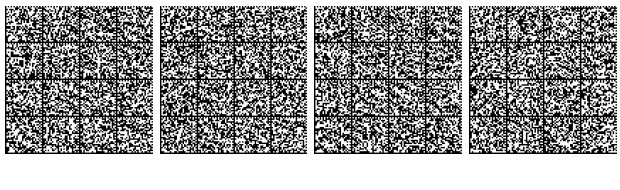
— Per i riferimenti del decreto legislativo 1° agosto 2003, n. 259, si veda nei riferimenti normativi all'articolo 7.

— Per il testo dell'articolo 17 della citata legge n. 400 del 1988, si veda nei riferimenti normativi all'articolo 6.

— Il testo dell'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20 (Disposizioni in materia di giurisdizione e controllo della Corte dei conti), pubblicata nella *Gazzetta Ufficiale* 14 gennaio 1994, n. 10, è il seguente:

«Art. 3 *(Norme in materia di controllo della Corte dei conti)*. — (*Omissis*).

4. La Corte dei conti svolge, anche in corso di esercizio, il controllo successivo sulla gestione del bilancio e del patrimonio delle amministrazioni pubbliche, nonché sulle gestioni fuori bilancio e sui fondi di provenienza comunitaria, verificando la legittimità e la regolarità delle gestioni, nonché il funzionamento dei controlli interni a ciascuna amministrazione. Accerta, anche in base all'esito di altri controlli, la rispondenza dei risultati dell'attività amministrativa agli obiettivi stabiliti dalla legge, valutando comparativamente costi, modi e tempi dello svolgimento dell'azione amministrativa. La Corte definisce annualmente i programmi e i criteri di riferimento del controllo sulla base delle priorità previamente deliberate dalle competenti Commissioni parlamentari a norma dei rispettivi regolamenti, anche tenendo conto, ai fini di referto per il coordinamento del sistema di finanza pubblica, delle relazioni redatte dagli organi, collegiali o monocratici, che esercitano funzioni di controllo o vigilanza su amministrazioni, enti pubblici, autorità amministrative indipendenti o società a prevalente capitale pubblico.».



— Si riporta il testo dell'articolo 162 del decreto legislativo 18 aprile 2016, n. 50, recante «Codice dei contratti pubblici», pubblicato nella *Gazzetta Ufficiale* 19 aprile 2016, n. 91, S.O.:

«Art. 162 *(Contratti secretati)*. — 1. Le disposizioni del presente codice relative alle procedure di affidamento possono essere derogate:

a) per i contratti al cui oggetto, atti o modalità di esecuzione è attribuita una classifica di segretezza;

b) per i contratti la cui esecuzione deve essere accompagnata da speciali misure di sicurezza, in conformità a disposizioni legislative, regolamentari o amministrative.

2. Ai fini della deroga di cui al comma 1, lettera *a)*, le amministrazioni e gli enti usuari attribuiscono, con provvedimento motivato, le classifiche di segretezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124, ovvero di altre norme vigenti. Ai fini della deroga di cui al comma 1, lettera *b)*, le amministrazioni e gli enti usuari dichiarano, con provvedimento motivato, i lavori, i servizi e le forniture eseguibili con speciali misure di sicurezza individuate nel predetto provvedimento.

3. I contratti di cui al comma 1 sono eseguiti da operatori economici in possesso dei requisiti previsti dal presente decreto e del nulla osta di sicurezza, ai sensi e nei limiti di cui all'articolo 42, comma 1-*bis*, della legge n. 124 del 2007.

4. L'affidamento dei contratti di cui al presente articolo avviene previo esperimento di gara informale a cui sono invitati almeno cinque operatori economici, se sussistono in tale numero soggetti qualificati in relazione all'oggetto del contratto e sempre che la negoziazione con più di un operatore economico sia compatibile con le esigenze di segretezza e sicurezza.

5. La Corte dei conti, tramite un proprio ufficio organizzato in modo da salvaguardare le esigenze di riservatezza, esercita il controllo preventivo sulla legittimità e sulla regolarità dei contratti di cui al presente articolo, nonché sulla regolarità, correttezza ed efficacia della gestione. Dell'attività di cui al presente comma è dato conto entro il 30 giugno di ciascun anno in una relazione al Parlamento.».

Art. 12.

Personale

1. Con apposito regolamento è dettata, nel rispetto dei princìpi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia, tenuto conto delle funzioni *volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia*. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia *di cui al comma 2, lettera* a)*,* un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La predetta equiparazione, *con riferimento sia* al trattamento economico in servizio che *al trattamento* previdenziale, produce effetti avendo riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

2. Il regolamento determina, *nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, comma 1,* in particolare:

a) l'istituzione di un ruolo del personale e la disciplina generale del rapporto d'impiego alle dipendenze dell'Agenzia;

b) la possibilità di procedere, oltre che ad assunzioni a tempo indeterminato attraverso modalità concorsuali, ad assunzioni a tempo determinato, con contratti di diritto privato, di soggetti in possesso di alta e particolare specializzazione debitamente documentata, individuati attraverso adeguate modalità selettive, per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia o per specifiche progettualità da portare a termine in un arco di tempo prefissato;

c) la possibilità di avvalersi di un contingente di esperti, non superiore a cinquanta unità, composto da personale, collocato fuori ruolo o in posizione di comando o altra *analoga posizione prevista* dagli ordinamenti di appartenenza, proveniente da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n.165, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, ovvero da personale non appartenente alla pubblica amministrazione, in possesso di specifica ed elevata competenza in materia di cybersicurezza e di tecnologie digitali innovative, nello sviluppo e gestione di processi complessi di trasformazione tecnologica e delle correlate iniziative di comunicazione e dissemina;

d) la determinazione della percentuale massima dei dipendenti che è possibile assumere a tempo determinato;

e) la possibilità di impiegare personale del Ministero della difesa, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri;

f) le ipotesi di incompatibilità;

g) le modalità di progressione di carriera all'interno dell'Agenzia;

h) la disciplina e il procedimento per la definizione degli aspetti giuridici e, limitatamente ad eventuali compensi accessori, economici del rapporto di impiego del personale oggetto di negoziazione con le rappresentanze del personale;

i) le modalità applicative delle disposizioni del decreto legislativo 10 febbraio 2005, n. 30, recante il Codice della proprietà industriale, ai prodotti dell'ingegno ed alle invenzioni dei dipendenti dell'Agenzia;

l) i casi di cessazione dal servizio del personale assunto a tempo indeterminato ed i casi di anticipata risoluzione dei rapporti a tempo determinato;

m) quali delle disposizioni possono essere oggetto di revisione per effetto della negoziazione con le rappresentanze del personale.

3. Qualora le assunzioni di cui al comma 2, lettera *b)*, riguardino professori universitari di ruolo o ricercatori universitari confermati si applicano le disposizioni di cui all'articolo 12 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, anche per quanto riguarda il collocamento in aspettativa.

4. In sede di prima applicazione delle disposizioni di cui al presente decreto, il numero di posti previsti dalla dotazione organica dell'Agenzia è individuato nella misura complessiva di trecento unità, di cui fino a un massimo di otto di livello dirigenziale generale, fino a un massimo di 24 di livello dirigenziale non generale e fino a un massimo di 268 unità di personale non dirigenziale.

5. Con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, la dotazione organica può essere rideterminata nei limiti delle risorse finanziarie destinate alle spese per il perso-

nale di cui all'articolo 18, comma 1. Dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione *alle Commissioni parlamentari competenti e al* COPASIR.

6. Le assunzioni effettuate in violazione delle disposizioni del presente decreto o del regolamento di cui al presente articolo sono nulle, ferma restando la responsabilità personale, patrimoniale e disciplinare dichi le ha disposte.

7. Il personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia è tenuto, anche dopo la cessazione di tale attività, al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni.

8. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere *delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza,* del COPASIR e sentito il CIC.

Riferimenti normativi:

— Per il testo dell'articolo 1, comma 2 del citato decreto legislativo n. 165 del 2001, si veda nei riferimenti normativi all'articolo 5.

— Il decreto legislativo 10 febbraio 2005, n. 30, recante «Codice della proprietà industriale, a norma dell'articolo 15 della legge 12 dicembre 2002, n. 273», è pubblicato nella *Gazzetta Ufficiale* 4 marzo 2005, n. 52, S.O.

— Si riporta il testo dell'articolo 12 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382 (Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica), pubblicato nella *Gazzetta Ufficiale* 31 luglio 1980, n. 209, S.O.:

«Art. 12 *(Direzione di istituti e laboratori extrauniversitari di ricerca)*. — Con decreto del Ministro della pubblica istruzione, su conforme parere del rettore e dei consigli delle facoltà interessate, i professori ordinari, straordinari ed associati possono essere autorizzati a dirigere istituti e laboratori e centri del Consiglio nazionale delle ricerche o istituti ed enti di ricerca a carattere nazionale o regionale.

I professori di ruolo possono essere collocati a domanda in aspettativa per la direzione di istituti e laboratori extrauniversitari di ricerca nazionali e internazionali.

I professori chiamati a dirigere istituti o laboratori del Consiglio nazionale delle ricerche e di altri enti pubblici di ricerca possono essere collocati in aspettativa con assegni.

L'aspettativa è concessa con decreto del Ministro della pubblica istruzione, su parere del Consiglio universitario nazionale, che considererà le caratteristiche e le dimensioni dell'istituto o laboratorio nonché l'impegno che la funzione direttiva richiede.

Durante il periodo dell'aspettativa ai professori ordinari competono eventualmente le indennità a carico degli enti o istituti di ricerca ed eventualmente la retribuzione ove l'aspettativa sia senza assegni.

Il periodo dell'aspettativa è utile ai fini della progressione della carriera, ivi compreso il conseguimento dell'ordinariato e ai fini del trattamento di previdenza e di quiescenza secondo le disposizioni vigenti.

Ai professori collocati in aspettativa è garantita, con le modalità di cui al quinto comma del successivoart. 13, la possibilità di svolgere, presso l'Università in cui sono titolari, cicli di conferenze, attività seminariali e attività di ricerca, anche applicativa. Si applica nei loro confronti, per la partecipazione agli organi universitari cui hanno titolo, la previsione di cui ai comma terzo e quarto dell'art. 14 della legge 18 marzo 1958, n. 311.

La direzione dei centri del Consiglio nazionale delle ricerche e dell'Istituto nazionale di fisica nucleare operanti presso le università può essere affidata ai professori di ruolo come parte delle loro attività di ricerca e senza limitazione delle loro funzioni universitarie. Essa è rinnovabile con il rinnovo del contratto con il Consiglio nazionale delle ricerche e con l'Istituto nazionale di fisica nucleare.

Le disposizioni di cui al precedente comma si applicano anche con riferimento alla direzione di centri di ricerca costituiti presso le università per contratto o per convenzione con altri enti pubblici che non abbiano la natura di enti pubblici economici.».

— Per il testo dell'articolo 17 della citata legge n. 400 del 1988, si veda nei riferimenti normativi all'articolo 6.

Art. 13.

Trattamento dei dati personali

1. Il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione del presente decreto è effettuato ai sensi dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196.

Riferimenti normativi:

— Si riporta il testo dell'articolo 58 del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, elativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), pubblicato nella *Gazzetta Ufficiale* 29 luglio 2003, n. 174, S.O.:

«Art. 58 *(Trattamenti di dati personali per fini di sicurezza nazionale o difesa)*. — 1. Ai trattamenti di dati personali effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento, ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui all'articolo 160, comma 4, nonché, in quanto compatibili, le disposizioni di cui agli articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo 18 maggio 2018, n. 51.

2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonché quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.

3. Con uno o più regolamenti sono individuate le modalità di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-*quaterdecies*, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.

4. Con uno o più regolamenti adottati con decreto del Presidente della Repubblica su proposta del Ministro della difesa, sono disciplinate le misure attuative del presente decreto in materia di esercizio delle funzioni di difesa e sicurezza nazionale da parte delle Forze armate.».

Art. 14.

Relazioni annuali

1. Entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri trasmette al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale.

2. Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia *negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato.*

Art. 15.

Modificazioni al decreto legislativo NIS

1. Al decreto legislativo NIS, sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 2, lettera *a)*, le parole: «strategia nazionale di sicurezza cibernetica» sono sostituite dalle seguenti: «strategia nazionale di cybersicurezza»;

b) all'articolo 1, comma 2, lettera *b)*, le parole: «delle autorità nazionali competenti» sono sostituite dalle seguenti: «dell'autorità nazionale competente NIS, delle autorità di settore»;

c) all'articolo 3, lettera *a)*, le parole da: «autorità competente NIS» a: «per settore,» sono sostituite dalle seguenti: «autorità nazionale competente NIS, l'autorità nazionale unica, competente»;

d) all'articolo 3, dopo la lettera *a)*, è inserita la seguente: «a-*bis*) autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da *a)* a *e)*»;

e) all'articolo 4, il comma 6 è sostituito dal seguente:

«6. L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni dopo il 9 maggio 2018, con le seguenti modalità:

a) le autorità di settore, in relazione ai settori di competenza, propongono all'autorità nazionale competente NIS le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri di cui ai commi 2 e 3;

b) le proposte sono valutate *ed eventualmente integrate, d'intesa con le autorità di settore,* dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore.»;

f) all'articolo 6, nella rubrica, le parole: «sicurezza cibernetica» sono sostituite *dalla seguente: «cybersicurezza*»; ai commi 1, 2 e 3, le parole: «sicurezza cibernetica» sono sostituite dalla seguente: «cybersicurezza»; al comma 4, le parole: «La Presidenza del Consiglio dei ministri» sono sostituite dalle seguenti: «L'Agenzia per la cybersicurezza» e le parole: «sicurezza cibernetica» sono sostituite *dalla seguente: «cybersicurezza*»;

g) l'articolo 7 è sostituito dal seguente:

«Art. 7 (Autorità nazionale competente e punto di contatto unico). - 1. L'Agenzia per la cybersicurezza nazionale è designata quale autorità nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III. Sono designate quali autorità di settore:

a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;

b) il Ministero delle infrastrutture e della mobilità sostenibili, 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 *dalle Regioni* o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;

f) il Ministero della transizione ecologica 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. L'autorità nazionale competente NIS è responsabile dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigila sull'applicazione del presente decreto a livello nazionale, esercitando altresì le relative potestà ispettive e sanzionatorie.

3. L'Agenzia per la cybersicurezza nazionale è designata 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 dell'autorità nazionale competente 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. L'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente NIS e di punto di contatto unico, consulta, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collabora con essi.

7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella dell'autorità nazionale competente 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 *annui a decorrere dall'anno* 2018, si provvede ai sensi dell'articolo 22.»;

h) all'articolo 8, comma 1, le parole da: «la Presidenza» a: «la sicurezza» sono sostituite dalle seguenti: «*l'Agenzia per la cybersicurezza* nazionale»;

i) l'articolo 9, comma 1, è sostituito dal seguente:

«1. Le autorità di settore collaborano con l'autorità nazionale competente NIS per l'adempimento degli ob-

blighi di cui al presente decreto. A tal fine è istituito presso l'Agenzia per la cybersicurezza *nazionale un* Comitato tecnico di raccordo. Il Comitato è presieduto dall'autorità nazionale competente NIS ed è composto dai rappresentanti delle amministrazioni statali individuate quali autorità di settore e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o *di* spese.»;

l) all'articolo 12, comma 5, le parole da: «e, per conoscenza,» a: «NIS,» sono soppresse;

m) all'articolo 14, comma 4, le parole da: «e, per conoscenza,» a: «NIS,» sono soppresse;

n) all'articolo 19, comma 1, le parole: «dalle autorità competenti NIS» sono sostituite dalle seguenti: «dall'autorità nazionale competente NIS»;

o) all'articolo 19, il comma 2 è abrogato;

p) all'articolo 20, comma 1, le parole da: «Le autorità competenti NIS» a: «sono competenti» sono sostituite da: «L'autorità nazionale competente NIS è competente»;

q) all'allegato I:

1) al punto 1, dopo la lettera *d)* è aggiunta la seguente: «d-*bis*) il CSIRT Italia conforma i propri servizi e la propria attività alle migliori pratiche internazionalmente riconosciute in materia di prevenzione, gestione e risposta rispetto a eventi di natura cibernetica»;

2) al punto 2, lettera *c)*, dopo la parola: «standardizzate» sono inserite le seguenti: «, secondo le migliori pratiche internazionalmente riconosciute,».

2. Nel decreto legislativo NIS:

a) ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui all'articolo 7, comma 1, lettera *a)*, del medesimo decreto legislativo*, come sostituito dal comma 1, lettera* g)*, del presente articolo;*

b) ogni riferimento al DIS, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

c) ogni riferimento alle autorità competenti NIS, ovunque ricorra, deve intendersi riferito all'autorità nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo*, come modificato dalla lettera* d) *del presente comma;*

d) all'articolo 5, comma 1, alinea, le parole: «le autorità competenti NIS» sono sostituite dalle seguenti: «l'autorità nazionale competente NIS e le autorità di settore»;

e) agli articoli 6 e 12, le parole: «Comitato interministeriale per la sicurezza della Repubblica (CISR)» sono sostituite dalle seguenti: «Comitato interministeriale per la cybersicurezza (CIC)».

Riferimenti normativi:

— Si riporta il testo dell'articolo 1, comma 2, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 1 *(Oggetto e ambito di applicazione)*. — (*Omissis*).

2. Ai fini del comma 1, il presente decreto prevede:

a) l'inclusione nella *strategia nazionale di cybersicurezza* di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;

b) la designazione *dell'autorità nazionale competente NIS, delle autorità di settore* e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di cui all'allegato I;

c) il rispetto di obblighi da parte degli operatori di servizi essenziali e dei fornitori di servizi digitali relativamente all'adozione di misure di sicurezza e di notifica degli incidenti con impatto rilevante;

d) la partecipazione nazionale al gruppo di cooperazione europeo, nell'ottica della collaborazione e dello scambio di informazioni tra Stati membri dell'Unione europea, nonché dell'incremento della fiducia tra di essi;

e) la partecipazione nazionale alla rete CSIRT nell'ottica di assicurare una cooperazione tecnico-operativa rapida ed efficace.».

— Si riporta il testo vigente dell'articolo 3, lettera *a)*, del citato decreto legislativo n. 65 del 2018:

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

a) autorità nazionale competente NIS, l'autorità nazionale unica, competente in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;

a-bis*) autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da* a) *a e)*;».

— Si riporta il testo dell'articolo 4, comma 6, del citato decreto legislativo n. 65 del 2018 come modificato dalla presente legge:

«Art. 4 *(Identificazione degli operatori di servizi essenziali)*. — *6. L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni dopo il 9 maggio 2018, con le seguenti modalità:*

a) *le autorità di settore, in relazione ai settori di competenza, propongono all'autorità nazionale competente NIS le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri di cui ai commi 2 e 3;*

b) *le proposte sono valutate ed eventualmente integrate, d'intesa con le autorità di settore, dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore.*».

— Per il testo dell'articolo 6 del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge, si rimanda nei riferimenti normativi all'articolo 1.

— Si riporta il testo dell'articolo 8, comma 1, del citato decreto legislativo n. 65 del 2018 come modificato dalla presente legge:

«Art. 8 *(Gruppi di intervento per la sicurezza informatica in caso di incidente - CSIRT)*. — 1. È istituito, presso *l'Agenzia per la cybersicurezza nazionale*, il CSIRT Italia, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-*bis* del decreto legislativo 1 agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.

— Si riporta il testo dell'articolo 9, comma 1, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 9 *(Cooperazione a livello nazionale)*. — 1. *Le autorità di settore collaborano con l'autorità nazionale competente NIS per l'adempimento degli obblighi di cui al presente decreto. A tal fine è istituito presso l'Agenzia per la cybersicurezza nazionale un Comitato tecnico di raccordo. Il Comitato è presieduto dall'autorità nazionale competente NIS ed è composto dai rappresentanti delle amministrazioni statali individuate quali autorità di settore e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi di rimborsi spese.*

(*Omissis*).».

— Si riporta il testo dell'articolo 12, comma 5, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 12 *(Obblighi in materia di sicurezza e notifica degli incidenti)*. — 1.-4. (*Omissis*).

5. Gli operatori di servizi essenziali notificano al CSIRT Italia senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.».

— Si riporta il testo dell'articolo 14, comma 4, del citato decreto legislativo n. 65 del 2018:

«Art. 14 (Obblighi in materia di sicurezza e notifica degli incidenti). — 1.-3. (*Omissis*).

4. I fornitori di servizi digitali notificano al CSIRT Italia senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.».

— Si riporta il testo dell'articolo 19, commi 1 e 2, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 19 *(Poteri ispettivi)*. — 1. L'attività di ispezione e verifica necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte *dall'autorità nazionale competente NIS*.

2. (*Abrogato*).».

— Si riporta il testo dell'articolo 20, comma 1, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 20 *(Autorità competente e regime dell'accertamento e dell'irrogazione delle sanzioni amministrative)*. — 1. *L'autorità nazionale competente NIS è competente* per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto.

(*Omissis*).».

— Si riporta il testo dell'Allegato I del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Allegato I

Requisiti e compiti dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)

(di cui all'art. 8)

I requisiti e i compiti del CSIRT sono adeguatamente e chiaramente definiti ai sensi del presente decreto e del decreto del Presidente del Consiglio dei ministri di cui all'art. 8, comma 2. Essi includono quanto segue:

1. Requisiti per il CSIRT

a) Il CSIRT garantisce un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.

b) I locali del CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri.

c) Continuità operativa:

i. il CSIRT è dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;

ii. il CSIRT dispone di personale sufficiente per garantirne l'operatività 24 ore su 24;

iii. il CSIRT opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup.

d) Il CSIRT ha la possibilità, se lo desidera, di partecipare a reti di cooperazione internazionale;

d-bis*) il CSIRT Italia conforma i propri servizi e la propria attività alle migliori pratiche internazionalmente riconosciute in materia di prevenzione, gestione e risposta rispetto a eventi di natura cibernetica.*

2. Compiti del CSIRT

a) I compiti del CSIRT comprendono almeno:

i. monitoraggio degli incidenti a livello nazionale;

ii. emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;

iii. intervento in caso di incidente;

iv. analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale;

v. partecipazione alla rete dei CSIRT;

b) Il CSIRT stabilisce relazioni di cooperazione con il settore privato;

c) per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate*, secondo le migliori pratiche internazionalmente riconosciute,* nei seguenti settori:

i. procedure di trattamento degli incidenti e dei rischi;

ii. sistemi di classificazione degli incidenti, dei rischi e delle informazioni.».

— Si riporta il testo dell'articolo 5, comma 1, del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 5 *(Effetti negativi rilevanti)*. — 1. Ai fini della determinazione della rilevanza degli effetti negativi di cui all'articolo 4, comma 2, lettera *c)*, *l'autorità nazionale competente NIS e le autorità di settore* considerano i seguenti fattori intersettoriali:

a) il numero di utenti che dipendono dal servizio fornito dal soggetto interessato;

b) la dipendenza di altri settori di cui all'allegato II dal servizio fornito da tale soggetto;

c) l'impatto che gli incidenti potrebbero avere, in termini di entità e di durata, sulle attività economiche e sociali o sulla pubblica sicurezza;

d) la quota di mercato di detto soggetto;

e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;

f) l'importanza del soggetto per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.».

— Per il testo dell'articolo 6 del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge, si veda nei riferimenti normativi all'articolo 1.

— Si riporta il testo dell'articolo 12 del citato decreto legislativo n. 65 del 2018, come modificato dalla presente legge:

«Art. 12 *(Obblighi in materia di sicurezza e notifica degli incidenti)*. — 1. Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni. Tenuto conto delle conoscenze più aggiornate in materia, dette misure assicurano un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente.

2. Gli operatori di servizi essenziali adottano misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali, al fine di assicurare la continuità di tali servizi.

3. Nell'adozione delle misure di cui ai commi 1 e 2, gli operatori di servizi essenziali tengono conto delle linee guida predisposte dal gruppo di cooperazione di cui all'articolo 10, nonché delle linee guida di cui al comma 7.

4. Fatto salvo quanto previsto dai commi 1, 2 e 3, le autorità competenti NIS possono, se necessario, definire specifiche misure, sentiti gli operatori di servizi essenziali.

5. Gli operatori di servizi essenziali notificano al CSIRT Italia senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

6. Il CSIRT Italia inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il *Comitato interministeriale per la cybersicurezza (CIC)*, delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.

7. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente. Le autorità competenti NIS possono predisporre linee guida per la notifica degli incidenti.

8. Per determinare la rilevanza dell'impatto di un incidente si tiene conto in particolare dei seguenti parametri:

a) il numero di utenti interessati dalla perturbazione del servizio essenziale;

b) la durata dell'incidente;

c) la diffusione geografica relativamente all'area interessata dall'incidente.

9. Sulla base delle informazioni fornite nella notifica da parte dell'operatore di servizi essenziali, il CSIRT Italia informa gli eventuali altri Stati membri interessati in cui l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali.

10. Ai fini del comma 9, il CSIRT Italia preserva, conformemente al diritto dell'Unione europea e alla legislazione nazionale, la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali, nonché la riservatezza delle informazioni fornite nella notifica secondo quanto previsto dall'articolo 1, comma 5.

11. Ove le circostanze lo consentano, il CSIRT Italia fornisce all'operatore di servizi essenziali, che effettua la notifica, le pertinenti informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente.

12. Su richiesta dell'autorità competente NIS o del CSIRT Italia, il punto di contatto unico trasmette, previa verifica dei presupposti, le notifiche ai punti di contatto unici degli altri Stati membri interessati.

13. Previa valutazione da parte dell'organo di cui al comma 6, l'autorità competente NIS, d'intesa con il CSIRT Italia, dopo aver consultato l'operatore dei servizi essenziali notificante, può informare il pubblico in merito ai singoli incidenti, qualora ne sia necessaria la sensibilizzazione per evitare un incidente o gestire un incidente in corso.

14. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Gli operatori di servizi essenziali provvedono agli adempimenti previsti dal presente articolo a valere sulle risorse finanziarie disponibili sui propri bilanci.».

Art. 16.

Altre modificazioni

1. All'articolo 3, comma 1-*bis*, della *legge 3 agosto 2007, n. 124*, dopo le parole: «della presente legge» sono aggiunte le seguenti: «e in materia di cybersicurezza».

2. All'articolo 38 della legge n. 124 del 2007, il comma 1-*bis* è abrogato *a decorrere dal 1° gennaio 2023.*

3. La denominazione: «CSIRT Italia» sostituisce, ad ogni effetto e ovunque presente in provvedimenti legislativi e regolamentari, la denominazione: «CSIRT Italiano».

4. Nel decreto-legge perimetro le parole: «Comitato interministeriale per la sicurezza della Repubblica (CISR)» e «CISR», ovunque ricorrano, sono rispettivamente sostituite dalle seguenti: «Comitato interministeriale per la cybersicurezza (CIC)» e «CIC», fatta eccezione per le disposizioni di cui all'articolo 5 del medesimo decreto-legge.

5. Nel decreto-legge perimetro ogni riferimento al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale*, fatta eccezione per le disposizioni dell'articolo 1, commi 2, lettera* b)*, e 2-*ter*, del medesimo decreto-legge perimetro,* e ogni riferimento al Nucleo per la sicurezza cibernetica è da intendersi riferito al Nucleo per la cybersicurezza.

6. Nel decreto-legge perimetro:

a) ogni riferimento al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 1, comma 8, lettera *a)*, le parole da: «definite dalla Presidenza del Consiglio dei ministri» a: «decreto legislativo 18 maggio 2018, n. 65» sono sostituite dalle seguenti: «definite dall'Agenzia per la cybersicurezza nazionale»;

c) all'articolo 1, comma 8, lettera *b)*, le parole: «all'autorità competente» sono sostituite dalle seguenti: «autorità nazionale competente NIS».

7. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al CISR e al DIS deve intendersi rispettivamente riferito al CIC e all'Agenzia per la cybersicurezza nazionale.

8. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al Ministero dello sviluppo economico e alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni *di cui all'articolo 3 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131*.

9. Al decreto-legge perimetro sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 6, lettera *a)*, dopo il primo periodo è inserito il seguente: «L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operatività del CVCN e comunque dal 30giugno 2022.»;

a-bis*) all'articolo 1, comma 7, lettera* c)*, le parole: «dell'organismo tecnico di supporto al CISR» sono sostituite dalle seguenti: «del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131»;*

a-ter*) all'articolo 1, comma 2, la lettera* b) *è sostituita dalla seguente:*

« 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, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; 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 citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia*

per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per 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, accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale »;*

a-quater*) all'articolo 1, dopo il comma 2*-bis *è inserito il seguente:*

«2-ter. *Gli elenchi dei soggetti di cui alla lettera* a) *del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3*-bis*, 4, 6 e 7 della legge 3 agosto 2007, n. 124»;*

b) all'articolo 3, il comma 2 è abrogato;

c) a decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dalla lettera *a)*, all'articolo 3:

1) il comma 1 è sostituito dal seguente: «1.I soggetti che intendono procedere all'acquisizione, a qualsiasi titolo, di beni, servizi e componenti di cui all'articolo 1-*bis*, comma 2, del decreto-legge 15 marzo 2012, n.21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, sono obbligati ad effettuare la comunicazione di cui all'articolo 1, comma 6, lettera *a)*, per lo svolgimento delle verifiche di sicurezza da parte del CVCN sulla base delle procedure, modalità e termini previsti dal regolamento di attuazione. Ai fornitori *dei predetti* beni, servizi e componenti si applica l'articolo 1, comma 6, lettera *b)*.»;

2) il comma 3 è abrogato;

10. A decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dal comma 9, lettera *a)*, al decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, il comma 3-*bis* dell'articolo 1-*bis* è sostituito dal seguente: «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, contenente anche la comunicazione del Centro di valutazione e certificazione nazionale (CVCN), relativa all'esito della valutazione e alle eventuali prescrizioni, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni. Qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN, il termine di cui al primo periodo decorre dalla comunicazione di esito positivo della valutazione effettuata dal CVCN. Entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunica l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. 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 in materia di sanzioni al 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, ovvero abbia eseguito il contratto o accordo in violazione del decreto di esercizio dei poteri speciali, il Governo può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore. 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 *del pagamento di una somma* 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».

11. All'articolo *135, comma 1, del Codice del processo amministrativo, di cui all'allegato 1 al decreto legislativo* 2 luglio 2010, n. 104, dopo la lettera *h)*, è aggiunta la seguente: «h-*bis*) le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale;» *e alla lettera* o) *le parole: «e dell'AISE» sono sostituite dalle seguenti: «, dell'AISE e dell'Agenzia per la cybersicurezza nazionale».*

12. Alla legge 22 aprile 2021, n. 53, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 1, lettera *b)*, dopo le parole: «Ministero dello sviluppo economico» sono aggiunte le seguenti: «e l'Agenzia perla cybersicurezza nazionale»;

b) all'articolo 18, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale.

13. All'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, le parole: «L'AgID» sono sostituite dalle seguenti: «L'Agenzia per

la cybersicurezza nazionale» *e sono aggiunte, infine, le seguenti parole: «nonché le modalità del procedimento di qualificazione dei servizi cluod per la pubblica amministrazione».*

14. Al decreto legislativo 1° agosto 2003, n. 259, sono apportate le seguenti modificazioni:

a) agli articoli 16-*bis* e 16-*ter*, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 16-*ter*, comma 1, le parole: «Ministro dello sviluppo economico» sono sostituite dalle seguenti: «Presidente del Consiglio dei ministri»;

c) all'articolo 16-*ter*, comma 2, lettera *b)*, le parole: «, in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico,» sono soppresse.

Riferimenti normativi:

— Per il testo dell'articolo 3, comma 1-*bis*, della citata legge n. 124 del 2007, come modificato dalla presente legge, si veda nei riferimenti normativi all'articolo 3.

— Si riporta il testo dell'articolo 38 della citata legge n. 124 del 2007, come modificato dalla presente legge:

«Art. 38 *(Relazione al Parlamento)*. — 1. Entro il mese di febbraio di ogni anno il Governo trasmette al Parlamento una relazione scritta, riferita all'anno precedente, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti.

1-*bis*. (*Abrogato a decorrere dal 1° gennaio 2023*).».

— Per il testo dell'articolo 5 della citata legge n. 124 del 2007, si veda nei riferimenti normativi all'articolo 1.

— Si riporta il testo dell'articolo 1, comma 2, lett.b), del citato decreto-legge n. 105 del 2019:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1.(*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 cybersicurezza (CIC):

a) (*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 CIC, 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.».

— Si riporta il testo dell'articolo 1, comma 8, del citato decreto-legge n. 105 del 2019, come modificato dalla presente legge:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 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 dall'Agenzia per la cybersicurezza nazionale*, 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 Italia inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera *a)*, *autorità nazionale competente NIS* di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65.».

— Per il testo dell'articolo 3 del citato decreto del Presidente del Consiglio dei ministri n. 131 del 2020, si rinvia ai riferimenti normativi all'articolo 7.

— Il testo dell'articolo 1, comma 6, lett. *a)* e comma 7, lettera *c)*, del citato decreto-legge n. 105 del 2019, come modificato dalla presente legge, è il seguente:

«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. *L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella* Gazzetta Ufficiale *della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operatività del CVCN e comunque dal 30 giugno 2022.* 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 moda-

lità 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;

(*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) – b (*Omissis*).

c) elabora e adotta, previo conforme avviso *del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131*, 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'articolo 3, commi 1, 2 e 3 del citato decreto-legge n. 105 del 2019, come modificato dalla presente legge:

«Art. 3 *(Disposizioni in materia di reti di telecomunicazione elettronica a banda larga con tecnologia)*. *— 1. I soggetti che intendono procedere all'acquisizione, a qualsiasi titolo, di beni, servizi e componenti di cui all'articolo 1*-bis*, comma 2, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, sono obbligati ad effettuare la comunicazione di cui all'articolo 1, comma 6, lettera* a)*, per lo svolgimento delle verifiche di sicurezza da parte del CVCN sulla base delle procedure, modalità e termini previsti dal regolamento di attuazione. Ai fornitori dei predetti beni, servizi e componenti si applica l'articolo 1, comma 6, lettera* b).

2. - 3. (*Abrogati*).».

— Si riporta il testo dell'articolo 1-*bis*, comma 3-*bis*, del citato decreto-legge n. 21 del 2012, come modificato dalla presente legge:

«Art. 1-*bis (Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G)*. — (*Omissis*).

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, contenente anche la comunicazione del Centro di valutazione e certificazione nazionale (CVCN), relativa all'esito della valutazione e alle eventuali prescrizioni, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni. Qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN, il termine di cui al primo periodo decorre dalla comunicazione di esito positivo della valutazione effettuata dal CVCN. Entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunica l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. 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 in materia di sanzioni al 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, ovvero abbia eseguito il contratto o accordo in violazione del decreto di esercizio dei poteri speciali, il Governo può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore. 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 del pagamento di una somma 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*.».

— Si riporta l'articolo 135, comma 1, del decreto legislativo 2 luglio 2010, n. 104 (Attuazione dell'articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo), pubblicato nella *Gazzetta Ufficiale* 7 luglio 2010, n. 156, S.O., come modificato dalla presente legge:

«Art. 135 *(Competenza funzionale inderogabile del Tribunale amministrativo regionale del Lazio, sede di Roma)*. — 1. Sono devolute alla competenza inderogabile del Tribunale amministrativo regionale del Lazio, sede di Roma, salvo ulteriori previsioni di legge:

a) le controversie relative ai provvedimenti riguardanti i magistrati ordinari adottati ai sensi dell'articolo 17, primo comma, della legge 24 marzo 1958, n. 195, nonché quelle relative ai provvedimenti riguardanti i magistrati amministrativi adottati dal Consiglio di Presidenza della Giustizia Amministrativa;

b) le controversie aventi ad oggetto i provvedimenti dell'Autorità garante per la concorrenza ed il mercato e quelli dell'Autorità per le garanzie nelle comunicazioni;

c) le controversie di cui all'articolo 133, comma 1, lettera *l)* , fatta eccezione per quelle di cui all'articolo 14, comma 2, nonché le controversie di cui all'articolo 104, comma 2, del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;

d) le controversie contro i provvedimenti ministeriali di cui all'articolo 133, comma 1, lettera *m)*, nonché i giudizi riguardanti l'assegnazione di diritti d'uso delle frequenze, la gara e le altre procedure di cui ai commi da 8 al 13 dell'articolo 1, della legge 13 dicembre 2010, n. 220, incluse le procedure di cui all'articolo 4 del decreto-legge 31 marzo 2011, n. 34, convertito, con modificazioni, dalla legge 26 maggio 2011, n. 75;

e) le controversie aventi ad oggetto le ordinanze e i provvedimenti commissariali adottati in tutte le situazioni di emergenza dichiarate ai sensi dell'articolo 5, comma 1, della legge 24 febbraio 1992, n. 225 nonché gli atti, i provvedimenti e le ordinanze emanati ai sensi dell'articolo 5, commi 2 e 4 della medesima legge n. 225 del 1992;

f) le controversie di cui all'articolo 133, comma 1, lettera *o)* , limitatamente a quelle concernenti la produzione di energia elettrica da fonte nucleare, i rigassificatori, i gasdotti di importazione, le centrali termoelettriche di potenza termica superiore a 400 MW nonché quelle relative ad infrastrutture di trasporto ricomprese o da ricomprendere nella rete di trasmissione nazionale o rete nazionale di gasdotti, salvo quanto previsto dall'articolo 14, comma 2;

g) le controversie di cui all'articolo 133, comma 1, lettera *z)*;

h) le controversie relative all'esercizio dei poteri speciali inerenti alle attività di rilevanza strategica nei settori della difesa e della sicurezza nazionale e nei settori dell'energia, dei trasporti e delle comunicazioni;

h-bis*) le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale;*

i) le controversie aventi ad oggetto i provvedimenti di espulsione di cittadini extracomunitari per motivi di ordine pubblico o di sicurezza dello Stato;

l) le controversie avverso i provvedimenti di allontanamento di cittadini comunitari per motivi di sicurezza dello Stato o per motivi di ordine pubblico di cui all'articolo 20, comma 1, del decreto legislativo 6 febbraio 2007, n. 30, e successive modificazioni;

m) le controversie avverso i provvedimenti previsti dal decreto legislativo 22 giugno 2007, n. 109;

n) le controversie disciplinate dal presente codice relative alle elezioni dei membri del Parlamento europeo spettanti all'Italia;

o) le controversie relative al rapporto di lavoro del personale del DIS, dell'AISI*, dell'AISE e dell'Agenzia per la cybersicurezza nazionale*;

p) le controversie attribuite alla giurisdizione del giudice amministrativo derivanti dall'applicazione del Titolo II del Libro III del decreto legislativo 6 settembre 2011, n. 159, relative all'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata;

q) le controversie relative ai provvedimenti adottati ai sensi degliarticoli 142e143 del testo unico delle leggi sull'ordinamento degli enti locali, di cui al decreto legislativo 18 agosto 2000, n. 267;

q-*bis*) le controversie di cui all'articolo 133, comma 1, lettera z-*bis*);

q-*ter*) le controversie di cui all'articolo 133, comma 1, lettera z-*ter*);

q-*quater*) le controversie aventi ad oggetto i provvedimenti emessi dall'Amministrazione autonoma dei monopoli di Stato in materia di giochi pubblici con vincita in denaro e quelli emessi dall'Autorità di polizia relativi al rilascio di autorizzazioni in materia di giochi pubblici con vincita in denaro;

q-*quinquies*) le controversie relative alle decisioni adottate ai sensi dell'articolo 24, paragrafo 2, lettera *b)*, del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio del 20 dicembre 2006 sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS *II)*;

q-*sexies*) le controversie relative ai provvedimenti di ammissione ed esclusione dalle competizioni professionistiche delle società o associazioni sportive professionistiche, o comunque incidenti sulla partecipazione a competizioni professionistiche.

2. Restano esclusi dai casi di competenza inderogabile di cui al comma 1 le controversie sui rapporti di lavoro dei pubblici dipendenti, salvo quelle di cui alla lettera *o)* dello stesso comma 1.».

— Si riporta l'articolo 4, comma 1, lett. *b)*, della legge 22 aprile 2021, n. 53 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020), pubblicata nella *Gazzetta Ufficiale* 23 aprile 2021, n. 97, come modificato dalla presente legge:

«Art. 4 *(Princìpi e criteri direttivi per l'attuazione della direttiva (UE) 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche)*. — Nell'esercizio della delega per l'attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, il Governo osserva, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge n. 234 del 2012, anche i seguenti princìpi e criteri direttivi specifici:

a) (*Omissis*)

b) prevedere l'assegnazione delle nuove competenze affidate all'Autorità per le garanzie nelle comunicazioni quale Autorità nazionale indipendente di regolamentazione del settore e alle altre autorità amministrative competenti, tra cui il Ministero dello sviluppo economico *e l'Agenzia per la cybersicurezza nazionale*, nel rispetto del principio di stabilità dell'attuale riparto di competenze sancito dall'articolo 5 della direttiva (UE) 2018/1972;».

Art. 17.

Disposizioni transitorie e finali

1. Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, l'Agenzia può provvedere, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per 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.

2. Per lo svolgimento delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, l'Agenzia provvede con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per 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.

3. Il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, riveste la qualifica di pubblico ufficiale.

4. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per 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, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale.

5. Con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, da adottare entro centottanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono definiti i termini e le modalità:

a) per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni del presente decreto;

b) mediante opportune intese con le amministrazioni interessate, *nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento,* per il trasferimento delle funzioni di cui all'articolo 7, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata, per l'attuazione delle disposizioni del presente decreto e la corrispondente riduzione di risorse finanziarie ed umane da parte delle amministrazioni cedenti.

5-bis*. Fino alla scadenza dei termini indicati nel decreto o nei decreti di cui al comma 5, lettera* b)*, la gestione delle risorse finanziarie relative alle funzioni trasferite, compresa la gestione dei residui passivi e perenti, è esercitata dalle amministrazioni cedenti. A decorrere dalla medesima data sono trasferiti in capo all'Agenzia i rapporti giuridici attivi e passivi relativi alle funzioni trasferite.*

6. In relazione al trasferimento delle funzioni di cui all'articolo 7, comma 1, lettera *m)*, dall'AgID all'Agenzia, i decreti di cui al comma 5 definiscono, altresì, i raccordi tra le due amministrazioni, per le funzioni che restano di competenza *dell'AgID. Nelle more dell'adozione dei decreti di cui al comma 5, il regolamento di cui all'articolo 33*-septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, è adottato dall'AgID, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri.*

7. *Al fine di assicurare la prima operatività dell'Agenzia, il direttore generale dell'Agenzia, fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 4, identifica, assume e liquida gli impegni di spesa che saranno pagati a cura del DIS, nell'ambito delle risorse destinate all'Agenzia. A tale fine è istituito un apposito capitolo nel bilancio del DIS.* Entro 90 giorni dall'approvazione dei regolamenti di cui all'articolo 11, *commi 3 e 4, il Presidente del Consiglio dei ministri dà informazione al COPASIR delle spese effettuate ai sensi del presente comma.*

8. *Al fine di assicurare la prima operatività dell'Agenzia, dalla data della nomina del direttore generale dell'Agenzia e nel limite del 30 per cento della dotazione organica complessiva iniziale di cui all'articolo 12, comma 4:*

a) *il DIS mette a disposizione il personale impiegato nell'ambito delle attività relative allo svolgimento delle funzioni oggetto di trasferimento, con modalità da definire mediante intese con lo stesso Dipartimento;*

b) *l'Agenzia si avvale, altresì, di unità di personale appartenenti al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, ad altre pubbliche amministrazioni e ad autorità indipendenti, per un periodo massimo di sei mesi, prorogabile una sola volta per un massimo di ulteriori sei mesi, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate mediante intese con le rispettive amministrazioni di appartenenza.*

8-bis*. Gli oneri derivanti dall'attuazione del comma 8 restano a carico dell'amministrazione di appartenenza.*

9. Il regolamento di cui all'articolo 12, comma 1, prevede apposite modalità selettive per l'inquadramento, nella misura massima del 50 per cento della dotazione organica complessiva, del personale di cui al comma 8 *del presente articolo* e del personale di cui all'articolo 12, comma 2, lettera *b)*, ove già appartenente alla pubblica amministrazione, nel contingente di personale addetto all'Agenzia di cui al medesimo articolo 12, che tengano conto delle mansioni svolte e degli incarichi ricoperti durante il periodo di servizio presso l'Agenzia, nonché delle competenze possedute e dei requisiti di professionalità ed esperienza richiesti per le specifiche posizioni. *Il personale di cui al comma 8, lettera* a)*, è inquadrato, a decorrere dal 1° gennaio 2022 nel ruolo di cui all'articolo 12, comma 2, lettera* a)*, secondo le modalità definite dal regolamento di cui all'articolo 12, comma 1.* Gli inquadramenti conseguenti alle procedure selettive di cui al presente comma, relative al personale di cui al comma 8, lettera *b)*, decorrono allo scadere dei sei mesi o della relativa proroga e, comunque, non oltre il 30 giugno 2022.

10. L'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del testo unico approvato con regio decreto 30 ottobre 1933, n. 1611.

10-bis*. In sede di prima applicazione del presente decreto:*

a) *la prima relazione di cui all'articolo 14, comma 1, è trasmessa entro il 30 novembre 2022;*

b) *entro il 31 ottobre 2022, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione che dà conto dello stato di attuazione, al 30 settembre 2022, delle disposizioni di cui al presente decreto, anche al fine di formulare eventuali proposte in materia.*

10-ter*. I pareri delle Commissioni parlamentari competenti per materia e per i profili finanziari e del COPASIR previsti dal presente decreto sono resi entro il termine di trenta giorni dalla trasmissione dei relativi schemi di decreto, decorso il quale il Presidente del Consiglio dei ministri può comunque procedere all'adozione dei relativi provvedimenti.*

Riferimenti normativi:

— Per il testo dell'articolo 7-*bis* del citato decreto-legge 27 luglio 2005, n. 144, si rinvia ai riferimenti normativi dell'articolo 9.

— Per il testo dell'articolo 5 del citato decreto-legge n. 105 del 2019, si rinvia ai riferimenti normativi dell'articolo 4.

— Il testo dell'articolo 331 del codice di procedura penale è il seguente:

«Art. 331 *(Denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio)*. — 1. Salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio [c.p. 358] che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito.

2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria.

3. Quando più persone sono obbligate alla denuncia per il medesimo fatto, esse possono anche redigere e sottoscrivere un unico atto.

4. Se, nel corso di un procedimento civile o amministrativo, emerge un fatto nel quale si può configurare un reato perseguibile di ufficio, l'autorità che procede redige e trasmette senza ritardo la denuncia al pubblico ministero.».

— Per il testo dell'articolo 33-*septies*, comma 4, del citato decreto-legge 18 ottobre 2012, n. 179, si veda nei riferimenti normativi all'articolo 7.

— Il testo dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611(Approvazione del T.U. delle leggi e delle norme giuridiche sulla rappresentanza e difesa in giudizio dello Stato e sull'ordinamento dell'Avvocatura dello Stato), pubblicato nella *Gazzetta Ufficiale* 12 dicembre 1933, n. 286, è il seguente:

«Art. 1. La rappresentanza, il patrocinio e l'assistenza in giudizio delle Amministrazioni dello Stato, anche se organizzate ad ordinamento autonomo, spettano alla Avvocatura dello Stato.

Gli avvocati dello Stato, esercitano le loro funzioni innanzi a tutte le giurisdizioni ed in qualunque sede e non hanno bisogno di mandato, neppure nei casi nei quali le norme ordinarie richiedono il mandato speciale, bastando che consti della loro qualità.».

Art. 18.

Disposizioni finanziarie

1. Per l'attuazione degli articoli da 5 a 7 è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025,110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027.

2. Agli oneri di cui al comma 1, si provvede mediante *corrispondente* riduzione *del Fondo* di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

3. Le risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni ridefinite ai sensi del presente decreto a decorrere *dall'inizio del funzionamento* dell'Agenzia di cui all'articolo 5, sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili, e portate ad incremento del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, anche mediante versamento all'entrata del bilancio dello Stato e successiva riassegnazione *alla spesa*.

4. I proventi di cui all'articolo 11, comma 2, sono versati all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di cui al comma 1 *del presente articolo*.

5. Ai fini dell'immediata attuazione delle disposizioni del presente decreto il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, anche in conto residui, le occorrenti variazioni di bilancio.

Riferimenti normativi:

— Si riporta il comma 200 dell'articolo 1, della legge 23 dicembre 2014, n. 190 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2015), pubblicata nella *Gazzetta Ufficiale* 29 dicembre 2014, n. 300, S.O.:

«200. Nello stato di previsione del Ministero dell'economia e delle finanze è istituito un Fondo per far fronte ad esigenze indifferibili che si manifestano nel corso della gestione, con la dotazione di 27 milioni di euro per l'anno 2015 e di 25 milioni di euro annui a decorrere dall'anno 2016. Il Fondo è ripartito annualmente con uno o più decreti del Presidente del Consiglio dei ministri su proposta del Ministro dell'economia e delle finanze. Il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio.».

Art. 19.

Entrata in vigore

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana e sarà presentato alle Camere per la conversione in legge.

21A04841

ESTRATTI, SUNTI E COMUNICATI

MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE

Istituzione di un vice Consolato onorario in Shymkent (Kazakhstan)

IL DIRETTORE GENERALE
PER LE RISORSE E L'INNOVAZIONE

(*Omissis*);

Decreta:

Articolo unico

È istituito in Shymkent (Kazakhstan) un vice Consolato onorario, posto alle dipendenze dell'Ambasciata d'Italia in Nur-Sultan, con la seguente circoscrizione territoriale: la città di Shymkent e la circostante regione del Turkistan.

Il presente decreto viene pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 23 luglio 2021

Il direttore generale: VARRIALE

21A04617

LAURA ALESSANDRELLI, *redattore* DELIA CHIARA, *vice redattore*

(WI-GU-2021-GU1-185) Roma, 2021 - Istituto Poligrafico e Zecca dello Stato S.p.A.

* 4 5 - 4 1 0 1 0 0 2 1 0 8 0 4 *

€ 1,00