tare), 10ª (Industria, commercio, turismo), 11ª (Lavoro pubblico e privato, previdenza sociale), 12ª (Igiene e sanità), 13ª (Territorio, ambiente, beni ambientali), 14ª (Politiche dell'Unione europea) e per le questioni regionali.

Esaminato dalla 5ª commissione (Bilancio), in sede referente, il 12 e il 13 luglio 2022.

Esaminato in aula e approvato definitamente il 14 luglio 2022.

AVVERTENZA:

Il decreto-legge 17 maggio 2022, n. 50, è stato pubblicato nella *Gazzetta Ufficiale* - Serie generale - n. 114 del 17 maggio 2022.

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 presente legge di conversione hanno efficacia dal giorno successivo a quello della sua pubblicazione.

Il testo del decreto-legge coordinato con la legge di conversione è pubblicato in questa stessa *Gazzetta Ufficiale* alla pag. 81.

22G00104

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 18 maggio 2022, n. **92**.

Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri;

Visto il decreto-legge 21 settembre 2019, n. 105, 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 e, in particolare, l'articolo 1, comma 7, lettera *b)*;

Vista la legge 1° aprile 1981, n. 121, recante nuovo ordinamento dell'Amministrazione della Pubblica sicurezza e, in particolare, l'articolo 16;

Visto il decreto legislativo 8 giugno 2001, n. 231, recante disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;

Visto il decreto legislativo 30 dicembre 2003, n. 366, recante modifiche ed integrazioni al decreto legislativo 30 luglio 1999, n. 300, concernenti le funzioni e la struttura organizzativa del Ministero delle comunicazioni, a norma dell'articolo 1 della legge 6 luglio 2002, n. 137, e, in particolare, l'articolo 6;

Vista la legge 31 dicembre 2009, n. 196, recante legge di contabilità e finanza pubblica e, in particolare, l'articolo 1, comma 3;

Visto il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale;

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

Visto il decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

Visto il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza;

Visto il decreto del Ministro delle comunicazioni 15 febbraio 2006, pubblicato nella *Gazzetta Ufficiale* n. 82 del 7 aprile 2006;

Visto il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante direttiva concernente indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella *Gazzetta ufficiale* della Repubblica italiana n. 87 del 13 aprile 2017;

Visto il decreto del Ministro dello sviluppo economico 15 febbraio 2019, recante l'istituzione del Centro di Valutazione e Certificazione Nazionale;

Visto il decreto del Presidente del Consiglio dei ministri 15 giugno 2021 recante l'individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera *a)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, pubblicato nella GU n. 198 del 19 agosto 2021;

Ritenuto di dover stabilire i criteri di accreditamento dei laboratori di prova da parte del CVCN e i raccordi, ivi compresi i contenuti, le modalità e i termini delle comunicazioni, tra il CVCN e i predetti laboratori, nonché tra il CVCN e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, anche al fine di assicurare il coordinamento delle rispettive attività e garantire la massima convergenza e la non duplicazione delle valutazioni in presenza di medesimi condizioni e livelli di rischio;

Udito il parere del Consiglio di Stato n. 01584 del 1° ottobre 2021 espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 7 settembre 2021;

Sulla proposta del Comitato interministeriale per la cybersicurezza;

ADOTTA
il seguente regolamento:

Capo I
DEFINIZIONI, COMPITI DEL CVCN E AREE DI ACCREDITAMENTO

Art. 1.
Definizioni

1. Ai fini del presente decreto si intende per:

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

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

c) soggetti inclusi nel perimetro, i soggetti inseriti nell'elenco di cui all'articolo 1, comma 2-*bis*, del decreto-legge;

d) DPR, il decreto del Presidente della Repubblica 5 febbraio 2021, n. 54, di cui all'articolo 1, comma 6, del decreto-legge;

e) rete, sistema informativo:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera *vv)*, del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale;

3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione, compresi i programmi di cui al numero 2);

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

g) bene ICT (*information and communication technology*), un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, di qualunque natura, considerato unitariamente ai fini dello svolgimento di funzioni essenziali dello Stato o per l'erogazione di servizi essenziali, ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante il regolamento di cui all'articolo 1, comma 2, del decreto-legge;

h) categorie, le tipologie di beni, sistemi o servizi ICT destinati ad essere impiegati sui beni ICT individuate dal decreto del Presidente del Consiglio dei ministri 15 giugno 2021, sulla base di criteri tecnici di cui all'articolo 13 del DPR, la cui acquisizione è subordinata alla valutazione del CVCN o dei CV, ai sensi dell'articolo 1, comma 6, lettera *a)*, del decreto-legge;

i) oggetto della fornitura, bene, sistema o servizio ICT appartenente alle categorie che il soggetto incluso nel perimetro intende acquisire, destinato all'impiego sui beni ICT individuati ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

l) Agenzia, l'Agenzia per la cybersicurezza nazionale, istituita a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, con decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

m) CVCN, il Centro di Valutazione e Certificazione Nazionale di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge, come modificato dal decreto-legge 14 giugno 2021, n. 82, che opera secondo modalità, termini e procedure definiti nel DPR;

n) CV, i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge;

o) oggetto della valutazione, l'oggetto della fornitura sottoposto al procedimento di valutazione da parte del CVCN o dei CV secondo modalità, termini e procedure definiti nel DPR;

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

q) LAP, laboratorio di prova che ha ottenuto l'accreditamento dal CVCN ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge;

r) accreditamento, il riconoscimento formale dell'indipendenza, affidabilità e competenza tecnica di un laboratorio di prova o CV, ai fini dell'esecuzione dei *test* di cui all'articolo 5, comma 3, del DPR, secondo le pertinenti modalità di cui all'articolo 7 del medesimo DPR;

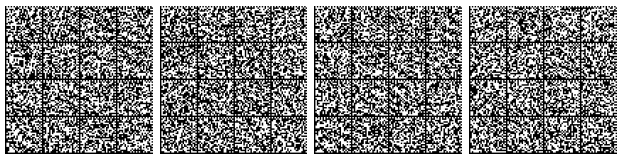
s) determinazione tecnica del CVCN, documento elaborato dal CVCN, concordato con i CV per gli aspetti di loro competenza, contenente regole, requisiti, specifiche tecniche, procedure per l'accreditamento dei laboratori di prova e il raccordo tra il CVCN, i LAP e i CV;

t) rapporto di prova, documento su cui sono registrati gli esiti analitici e le informazioni necessarie all'interpretazione dei risultati dei *test* eseguiti, redatto in conformità alle prescrizioni della norma EN ISO/IEC 17025;

u) rapporto di valutazione, documento redatto dal CVCN e dai CV sulla base del rapporto di prova di cui all'articolo 8, commi 1 e 2, del DPR;

v) responsabile del laboratorio di prova, la persona che ha la responsabilità e l'autorità definite per l'esecuzione di tutte le operazioni gestionali e tecniche relative alle funzioni per cui il laboratorio di prova è accreditato;

z) responsabile del sistema di gestione per la qualità, la persona che ha la responsabilità e l'autorità definite per garantire che il sistema di gestione per la qualità sia attuato, seguito e migliorato in modo continuativo;



aa) responsabile per i rapporti con il CVCN, la persona che ha la responsabilità e l'autorità definite per curare i rapporti con il CVCN;

bb) richiedente, il soggetto che ha presentato domanda per l'accreditamento di un laboratorio di prova;

cc) amministrazione pubblica, amministrazione pubblica individuata nell'elenco di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;

dd) titolare di un laboratorio di prova, la persona fisica o giuridica che, quale proprietario, o nell'esercizio d'impresa o in base a ogni altro titolo, eserciti il controllo o la gestione del laboratorio;

ee) verifica, attività di analisi e controllo documentale delle evidenze al fine di accertare il rispetto e il mantenimento dei requisiti necessari per l'accreditamento;

ff) ispezione, attività di tipo ricognitivo e valutativo che si articola nell'analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto al fine di accertare il rispetto e il mantenimento dei requisiti necessari per l'accreditamento;

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

hh) CSIRT Italia, il *Computer security incident response team* istituito ai sensi dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65.

Art. 2.

Oggetto

1. Il presente decreto, in attuazione dell'articolo 1, comma 7, lettera *b)*, del decreto-legge, definisce:

a) le procedure, le modalità ed i termini da seguire per l'accreditamento dei CV e dei laboratori di prova, ciascuno nell'ambito delle rispettive competenze, in ordine all'esecuzione dei *test* di cui all'articolo 5, comma 3, del DPR, secondo le pertinenti modalità di cui all'articolo 7 del medesimo DPR;

b) le procedure, le modalità ed i termini da seguire in ordine alla gestione dei raccordi del CVCN con i LAP e i CV, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio.

Art. 3.

Organismo di accreditamento

1. L'organismo di accreditamento è il CVCN, che opera in conformità ai requisiti della norma UNI CEI EN ISO/IEC 17011 - «Valutazione della conformità - Requisiti per gli organismi di accreditamento che accreditano organismi di valutazione della conformità».

Art. 4.

Compiti del CVCN

1. Ai fini del presente decreto il CVCN:

a) accredita i laboratori di prova, in possesso dei requisiti di cui agli articoli 8 e 9, per l'esecuzione dei *test* di cui all'articolo 5, comma 3, del DPR;

b) intraprende iniziative al fine di garantire il mantenimento del livello di qualità dei LAP e la corretta attuazione delle determinazioni tecniche di cui alla lettera *e)*, delle specifiche tecniche e della redazione dei rapporti di prova;

c) stabilisce le metodologie di *test* di cui all'articolo 5, comma 4, del DPR;

d) vigila sull'attività dei LAP nel corso delle attività di *test* effettuando verifiche intermedie o a campione per la verifica del mantenimento dei requisiti di accreditamento;

e) adotta, in conformità e in attuazione di quanto previsto dal presente regolamento, specifiche determinazioni tecniche, assicurandone, nell'ambito delle proprie competenze, il rispetto e curandone l'aggiornamento. In particolare, tali determinazioni definiscono:

1) i requisiti tecnici e logistici, tra cui quelli relativi alla dotazione strumentale per l'esecuzione dei *test* e alla protezione degli ambienti di *test*;

2) le specifiche misure di sicurezza informatica;

3) i requisiti di competenza ed esperienza necessari per l'accreditamento dei laboratori di prova ivi comprese le modalità di redazione del curriculum professionale da presentare nella domanda di accreditamento;

4) le aree di accreditamento di cui all'articolo 7;

5) i *test* da eseguire di cui all'articolo 5, comma 3, del DPR;

6) le attività relative all'esecuzione dei *test* soggette al divieto di divulgazione di cui all'articolo 13, comma 2;

7) le modalità di notifica delle limitazioni di operatività superiori a 24 ore di cui all'articolo 13, comma 1, lettera *f)*;

8) le modalità tecniche per l'applicazione dei raccordi di cui all'articolo 21 tra il CVCN e i CV, concordandoli con questi ultimi per gli aspetti di loro competenza;

9) le modalità esecutive delle comunicazioni con i LAP e i termini tecnici e organizzativi mediante i quali i raccordi trovano effettiva applicazione di cui all'articolo 21;

f) cura i raccordi con i LAP e i CV, anche al fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio;

g) redige e aggiorna periodicamente la lista dei beni, sistemi e servizi ICT oggetto di valutazione, per i quali sia stato emesso un rapporto di prova;

h) gestisce la piattaforma informatica di cui all'articolo 6, commi 1 e 6, del DPR, anche ai fini di cui all'articolo 21, in particolare per la conservazione e condivisione:

1) di un elenco dei LAP contenente il nominativo del responsabile del laboratorio di prova, del responsabile del sistema di gestione per la qualità e del responsabile per i rapporti con il CVCN, nonché la durata e l'area dell'accreditamento;

2) della documentazione di sintesi relativa ai rapporti di prova.

Art. 5.

Commissione di accreditamento

1. Per le finalità di cui al presente decreto è istituita presso il CVCN una commissione di accreditamento, con compiti consultivi, composta dal presidente designato dall'Agenzia e da due rappresentanti designati, rispettivamente, dal Ministero dell'interno e dal Ministero della difesa, in possesso di competenze tecnico-specialistiche nel campo della certificazione di processo e della sicurezza informatica. Il CVCN assicura le attività di segreteria e di supporto per il funzionamento della commissione.

2. La commissione di accreditamento esprime i pareri obbligatori previsti dagli articoli 12, 15 e 16.

3. Per la partecipazione alla commissione di accreditamento non sono previsti gettoni di presenza, compensi o rimborsi di spese.

Art. 6.

Collaborazione con le Forze di polizia

1. Per la verifica della sussistenza e del mantenimento dei requisiti di cui all'articolo 9, commi 1, 2, 3 e 6, il CVCN può richiedere di effettuare i necessari riscontri alle Forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121, le quali operano nell'ambito delle autonome competenze istituzionali loro attribuite dalla normativa vigente.

Art. 7.

Aree di accreditamento

1. I laboratori di prova sono accreditati per una o più aree, indicate dal CVCN con la determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 4), in relazione alle categorie, alle tipologie e ai livelli di severità dei *test* individuati dal CVCN. I laboratori di prova indicano le aree per cui chiedono di essere accreditati nella domanda di cui agli articoli 10 e 11.

Capo II

ACCREDITAMENTO DEI LABORATORI DI PROVA

Art. 8.

Requisiti generali per l'accreditamento

1. Possono richiedere l'accreditamento le amministrazioni pubbliche e gli enti pubblici, nonché i soggetti privati aventi sede legale nel territorio nazionale, iscritti, ove previsto dalla normativa vigente, nel registro delle imprese della Camera di commercio, industria, artigianato e agricoltura, titolari di un laboratorio di prova.

2. Ai sensi dell'articolo 1, comma 7, lettera *b)*, del decreto-legge i laboratori istituiti presso le amministrazioni centrali dello Stato, accreditati secondo le modalità di cui agli articoli 11 e 12, possono, su incarico del CVCN, eseguire i *test* su oggetti di fornitura in acquisizione presso le medesime amministrazioni.

3. Ai fini dell'accreditamento, il richiedente deve essere in possesso dei seguenti requisiti:

a) disponibilità sul territorio nazionale di locali e mezzi adeguati nei quali verranno svolte le funzioni per le quali il laboratorio di prova sarà accreditato in conformità all'articolo 4, comma 1, lettera *e)*, numero 1);

b) conoscenze, competenze ed esperienza necessarie per l'esercizio delle funzioni connesse all'accreditamento, in conformità all'articolo 4, comma 1, lettera *e)*, numero 3);

c) rispondenza ai criteri specificati nelle norme relative alla gestione dei laboratori di *test* e alla gestione dei dati UNI CEI EN ISO/IEC 17025, UNI CEI EN ISO/IEC 27001 e nelle determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*;

d) capacità di mantenere nel tempo i requisiti in virtù dei quali sono stati accreditati;

e) capacità di attuare le misure di sicurezza indicate nella determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 2);

4. Ai fini dell'accreditamento dei laboratori di prova di cui sono titolari soggetti privati, è altresì valutato il possesso della capacità di garantire imparzialità, indipendenza, riservatezza e obiettività nello svolgimento delle funzioni connesse all'accreditamento.

Art. 9.

Requisiti soggettivi e motivi ostativi ai fini dell'accreditamento dei laboratori di prova

1. Ai fini dell'accreditamento dei laboratori di prova, il legale rappresentante del laboratorio di prova, nonché il responsabile del laboratorio di prova, il responsabile del sistema di gestione per la qualità, il responsabile per i rapporti con il CVCN, il responsabile della sicurezza e il personale chiamato a svolgere le attività per le quali il laboratorio di prova può essere accreditato che comportano l'accesso alle informazioni di cui all'articolo 13, comma 2, devono possedere la cittadinanza italiana e rispetto ai medesimi non deve ricorrere una delle seguenti circostanze:

a) stato di interdizione, inabilitazione, fallimento;

b) condanna, con sentenza anche non definitiva, o decreto penale di condanna o sentenza di applicazione della pena su richiesta ai sensi dell'articolo 444 del codice di procedura penale per uno dei seguenti reati:

1) delitti, consumati o tentati, indicati all'articolo 80, comma 1, del codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50;

2) delitti, consumati o tentati, previsti dal Libro II, Titolo I, del codice penale;

3) delitti, consumati o tentati, di cui agli articoli 615-*bis*, 615-*ter*, 615-*quater*, 615-*quinquies*, 616, 617, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 617-*septies* 618, 619, 620, 621, 622, 623, 623-*bis* del codice penale;

4) ogni altro delitto da cui derivi, quale pena accessoria, l'interdizione dai pubblici uffici o l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese o l'incapacità di contrarre con la pubblica amministrazione;

c) sussistenza di cause di decadenza, di sospensione o di divieto previste dall'articolo 67 del decreto legislativo 6 settembre 2011, n. 159, e di un tentativo di infiltrazione mafiosa di cui all'articolo 84, comma 4, del medesimo decreto.

2. Relativamente ai laboratori di prova di cui all'articolo 10 costituisce motivo ostativo all'accreditamento l'applicazione all'ente delle sanzioni amministrative di cui al Capo I, Sezione III, del decreto legislativo 8 giugno 2001, n. 231.

3. Ferma restando la previsione di cui al comma 4, non può essere riconosciuto l'accreditamento al laboratorio:

a) che interviene direttamente nella progettazione, fabbricazione, costruzione, commercializzazione, installazione, utilizzo o manutenzione di beni, sistemi o servizi ICT rientranti nelle categorie o i cui dirigenti o personale sono il progettista, il fabbricante, il fornitore, l'installatore, l'acquirente, il proprietario, il rappresentante autorizzato o l'utente dei beni, sistemi o servizi ICT stessi;

b) appartenente a un'associazione d'imprese o ad una federazione professionale che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura di beni, sistemi o servizi ICT rientranti nelle categorie;

c) che, singolarmente o in quanto componente di consorzio, eserciti un controllo, diretto o indiretto, anche congiuntamente, su un soggetto o un'associazione di imprese o una federazione professionale che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura di beni, sistemi o servizi ICT rientranti nelle categorie;

d) sottoposto al controllo, diretto o indiretto, anche congiuntamente, da parte di un altro soggetto, singolo o componente di consorzio che rappresenta imprese coinvolte nella progettazione, nella fabbricazione, nella fornitura di beni, sistemi o servizi ICT rientranti nelle categorie;

e) sottoposto al controllo, diretto o indiretto, anche congiuntamente, da parte di un soggetto che a sua volta controlla, anche in via indiretta e/o congiunta, un altro partecipante, singolo o componente di consorzio coinvolto nella progettazione, nella fabbricazione, nella fornitura di beni, sistemi o servizi ICT rientranti nelle categorie.

4. Le disposizioni di cui al comma 3 non si applicano ai laboratori di prova aventi sede nel territorio nazionale e di cui sono titolari soggetti inclusi nel perimetro. Le attività svolte da detti laboratori non possono in ogni caso riguardare beni, sistemi e servizi ICT prodotti, forniti o acquisiti dal soggetto stesso ai sensi dell'articolo 1, comma 6, lettera *a)*, del decreto-legge, nonché beni, sistemi e servizi ICT prodotti, forniti o acquisiti da soggetti operanti nell'ambito del medesimo settore di attività.

5. Non è in ogni caso consentito l'accreditamento ove sussistano motivi ostativi inerenti alla sicurezza della Repubblica.

6. Ai fini di cui al comma 5 è oggetto di valutazione, tra l'altro, se il soggetto privato richiedente sia controllato, direttamente o indirettamente, da persone fisiche o giuridiche, incluse amministrazioni pubbliche, che abbiano la residenza, la dimora abituale, la sede legale o dell'amministrazione ovvero il centro di attività principale fuori dal territorio della Repubblica ovvero sia direttamente o indirettamente sottoposto all'influenza di dette persone fisiche o giuridiche, anche attraverso l'erogazione di finanziamenti consistenti.

Art. 10.

Domanda di accreditamento di laboratori di prova di cui è titolare un soggetto privato

1. La domanda di accreditamento, nel caso in cui titolare del laboratorio di prova sia un soggetto privato, deve essere firmata dal legale rappresentante con firma elettronica qualificata e inviata al CVCN tramite posta elettronica certificata, o altro servizio elettronico di recapito certificato qualificato, corredata dei seguenti elementi:

a) numero di iscrizione, ove prevista, al registro imprese della Camera di commercio, industria, artigianato e agricoltura e visura camerale storica o altro documento attestante l'identità giuridica del laboratorio di prova;

b) denominazione o ragione sociale del laboratorio di prova;

c) indirizzo della sede del laboratorio di prova in cui vengono eseguite le prove;

d) identificazione del legale rappresentante del laboratorio di prova;

e) nome, cognome, curriculum professionale redatto secondo quanto previsto dalla determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 3), e certificato del casellario giudiziale e dei carichi pendenti del responsabile del laboratorio di prova, del responsabile del sistema di gestione per la qualità, del responsabile per i rapporti con il CVCN e del responsabile della sicurezza;

f) nome, cognome, curriculum professionale redatto secondo quanto previsto dalla determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 3), e certificato del casellario giudiziale e dei carichi pendenti del personale coinvolto nelle attività di valutazione del laboratorio di prova e che sarà autorizzato ad accedere alle informazioni, necessarie per lo svolgimento delle stesse attività, individuate nella determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 6);

g) sulla base delle prescrizioni contenute nella determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*:

1) area di accreditamento di cui all'articolo 7, per la quale il laboratorio di prova chiede di essere accreditato, con riferimento al numero 4) dell'articolo 4, comma 1, lettera *e)*;

2) descrizione dei requisiti tecnici e logistici, con riferimento al numero 1) dell'articolo 4, comma 1, lettera *e)*;

3) descrizione delle conoscenze, competenze ed esperienza in possesso del personale assegnato alle attività di esecuzione dei *test*, con riferimento al numero 3) dell'articolo 4, comma 1, lettera *e)*;

4) indicazione delle misure di sicurezza attuate, con riferimento al numero 2) dell'articolo 4, comma 1, lettera *e)*;

h) impegno sottoscritto di non divulgazione di quanto oggetto di comunicazione, formale e informale, con il CVCN e delle informazioni di carattere tecnico-scientifico concernenti le metodologie di *test*, le specifiche tecniche e l'elaborazione dei rapporti di prova, con riferimento all'articolo 4, comma 1, lettera *e)*, numero 6). L'atto di non divulgazione prevede l'indicazione del personale del richiedente che potrà avere accesso alle informazioni strettamente necessarie all'espletamento della procedura di accreditamento. L'atto contiene altresì una clausola penale relativa all'importo che il richiedente è tenuto a corrispondere in caso di violazione degli impegni assunti.

i) manuale della qualità che descrive la rispondenza ai criteri specificati nelle norme relative alla gestione dei laboratori di prova e alla gestione dei dati UNI CEI EN ISO/IEC 17025, UNI CEI EN ISO/IEC 27001;

l) dichiarazione di assunzione dell'impegno al pagamento delle spese di istruttoria calcolate sulla base di quanto previsto dall'articolo 19;

m) dichiarazione di assunzione di responsabilità per la corretta esecuzione dei *test* definiti dalla determinazione tecnica del CVCN di cui all'articolo 4, comma 1, lettera *e)*, numero 5);

n) dichiarazione attestante il possesso dei requisiti soggettivi e la non sussistenza dei motivi ostativi di cui all'articolo 9;

o) estremi della polizza di assicurazione per la responsabilità civile con massimale non inferiore a euro 2.500.000,00, per ogni anno e per ogni sinistro, per rischi derivanti dall'esercizio dell'attività professionale.

2. La domanda e le relative dichiarazioni che attestano il possesso dei requisiti di cui al comma 1 sono sottoscritte ai sensi e per gli effetti di quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Art. 11.

Domanda di accreditamento di laboratori di prova istituiti presso amministrazioni o enti pubblici

1. La domanda di accreditamento del laboratorio di prova istituito presso una amministrazione o ente pubblico deve essere firmata dal dirigente responsabile, con firma elettronica qualificata, inviata al CVCN tramite posta elettronica certificata, o altro servizio elettronico di recapito certificato qualificato, corredata delle seguenti informazioni:

a) documentazione attestante l'identità giuridica del laboratorio di prova e comprovante l'appartenenza ad una amministrazione o ente pubblico;

b) identificazione del responsabile del laboratorio di prova;

c) denominazione o ragione sociale del laboratorio di prova;

d) indirizzo della sede del laboratorio di prova in cui vengono eseguite le prove;

e) nome, cognome, curriculum professionale redatto secondo quanto previsto dalla determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 3), e certificato del casellario giudiziale e dei carichi pendenti del responsabile del laboratorio di prova, del responsabile del sistema di gestione per la qualità, del responsabile per i rapporti con il CVCN e dal responsabile della sicurezza;

f) nome, cognome, curriculum professionale redatto secondo quanto previsto dagli atti di cui all'articolo 4, comma 1, lettera *e)*, relativi alle competenze e certificato del casellario giudiziale e dei carichi pendenti del personale coinvolto nelle attività di *test* del laboratorio di prova e che sarà autorizzato ad accedere alle informazioni, necessarie per lo svolgimento delle stesse attività, individuate nella determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 6;

g) sulla base delle prescrizioni contenute nelle determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*:

1) area di accreditamento di cui all'articolo 7, per la quale il laboratorio di prova chiede di essere accreditato con riferimento al numero 4) dell'articolo 4, comma 1, lettera *e)*;

2) descrizione dei requisiti tecnici e logistici, con riferimento al numero 1) dell'articolo 4, comma 1, lettera *e)*;

3) descrizione delle conoscenze, competenze ed esperienza in possesso del personale assegnato alle attività di esecuzione dei *test*, con riferimento al numero 3) dell'articolo 4, comma 1, lettera *e)*;

4) indicazione delle misure di sicurezza attuate, con riferimento al numero 2) dell'articolo 4, comma 1, lettera *e)*;

h) impegno sottoscritto di non divulgazione di quanto oggetto di comunicazione, formale e informale, con il CVCN e delle informazioni di carattere tecnico-scientifico concernenti le metodologie di *test*, le specifiche tecniche e l'elaborazione dei rapporti di prova, con riferimento all'articolo 4, comma 1, lettera *e)*, numero 6). L'atto di non divulgazione prevede l'indicazione del personale del richiedente che potrà avere accesso alle informazioni strettamente necessarie all'espletamento della procedura di accreditamento. L'atto contiene altresì una clausola penale relativa all'importo che il richiedente è tenuto a corrispondere in caso di violazione degli impegni assunti;

i) manuale della qualità che descrive la rispondenza ai criteri specificati nelle norme relative alla gestione dei laboratori di prova e alla gestione dei dati UNI CEI EN ISO/IEC 17025, UNI CEI EN ISO/IEC 27001;

l) dichiarazione di assunzione dell'impegno al pagamento delle spese di istruttoria calcolate sulla base di quanto previsto dall'articolo 19;

m) dichiarazione di assunzione di responsabilità per la corretta esecuzione dei *test* definiti dalle determinazioni tecniche del CVCN di cui all'articolo 4, comma 1, lettera *e)*;

n) indicazione delle misure di sicurezza attuate ai sensi della determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 4);

o) garanzia della tutela da responsabilità civile del personale nell'esercizio delle funzioni.

2. La domanda e le relative dichiarazioni che attestano il possesso dei requisiti a corredo di cui al comma 1 sono sottoscritte ai sensi e per gli effetti di quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Art. 12.

Procedura di accreditamento dei laboratori di prova

1. La procedura di accreditamento si articola nelle seguenti fasi:

a) verifiche e adempimenti preliminari:

1) ricevuta la domanda di accreditamento, il CVCN verifica la completezza della documentazione presentata dal richiedente rispetto agli elementi indicati dagli articoli 9, 10 e 11;

2) nel caso in cui la documentazione risulti incompleta il CVCN ne dà comunicazione al laboratorio di prova assegnando un termine al fine di provvedere alle eventuali integrazioni. Nel caso in cui il laboratorio di prova non fornisca riscontro entro tale termine o comunque in caso di perdurante incompletezza della documentazione il CVCN comunica al richiedente i motivi ostativi all'accoglimento dell'istanza ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241;

3) in caso di esito positivo della verifica di completezza della documentazione, il CVCN trasmette al richiedente un elenco dei *test* corrispondenti all'area o alle aree di accreditamento indicate nella domanda e richiede, assegnando un termine per l'adempimento, di confermare la capacità di effettuare in tutto o in parte detti *test* e di indicare le modalità a tal fine seguite dal laboratorio di prova;

4) ricevuto riscontro dal richiedente in relazione a quanto previsto al numero 3) il CVCN conferisce l'incarico per le verifiche di cui alle lettere *b)* e *c)* del presente comma a personale dell'Agenzia in possesso di specifiche competenze tecnico-specialistiche nel campo della certificazione di processo e della sicurezza informatica;

b) verifica tecnico documentale:

1) il personale incaricato esamina il manuale della qualità e la documentazione tecnica e trasmette al CVCN il rapporto di verifica contenente gli esiti delle attività eseguite;

2) nel caso in cui, sulla base del rapporto di verifica, il CVCN ritenga necessarie integrazioni o modifiche del manuale e dei relativi documenti tecnici, ne dà comunicazione al laboratorio di prova assegnando un termine per la revisione della documentazione. Il laboratorio di prova, ricevuta la comunicazione, effettua le modifiche necessarie del manuale e della relativa documentazione o, in alternativa, può richiedere di ridurre l'area di accreditamento. Nel caso in cui il laboratorio di prova non fornisca riscontro entro il termine stabilito o comunque nel caso in cui il laboratorio di prova non proceda alle modifiche richieste il CVCN comunica al richiedente i motivi ostativi all'accoglimento dell'istanza ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241;

3) nel caso in cui il CVCN valuti con esito positivo la documentazione di cui ai punti 1) e 2), ne dà comunicazione al laboratorio di prova, fornendo contestualmente le indicazioni per lo svolgimento della visita ispettiva presso la sede del laboratorio di prova ai fini della verifica dell'effettiva conformità ai requisiti previsti e della capacità del laboratorio di eseguire i *test* per i quali ha richiesto l'accreditamento, ai sensi della lettera *c)*;

c) visita ispettiva e verifica della capacità tecnica del laboratorio di prova:

1) il personale incaricato effettua una verifica presso il laboratorio di prova al fine di accertare il possesso dei requisiti di cui all'articolo 8 e la conformità rispetto a quanto descritto nelle determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*, e, infine, richiede al laboratorio di effettuare uno o più *test* e di produrre il relativo rapporto di prova;

2) all'esito della visita ispettiva il personale incaricato redige un processo verbale sottoscritto unitamente al rappresentante legale del laboratorio di prova, al responsabile del laboratorio di prova ed al responsabile del sistema di gestione per la qualità. Qualora il rappresentante legale del laboratorio di prova rifiuti di sottoscrivere il processo verbale, il personale incaricato ne dà evidenza nel rapporto riportando le motivazioni del diniego. Una copia del verbale è sempre rilasciata al rappresentante legale del laboratorio di prova;

3) il personale incaricato trasmette al CVCN il processo verbale corredato di tutta la documentazione prodotta o acquisita nel corso delle attività svolte;

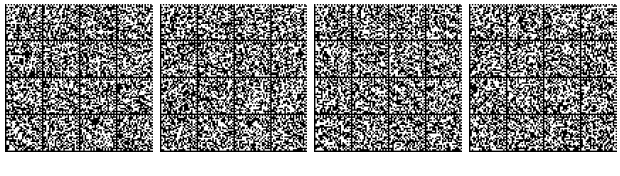
4) qualora, sulla base del processo verbale, il CVCN valuti con esito negativo la capacità tecnica del laboratorio di prova, il CVCN comunica i motivi ostativi all'accoglimento dell'istanza ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241;

d) parere della commissione di accreditamento:

1) all'esito delle fasi di cui alle lettere *a)*, *b)* e *c)*, il CVCN inoltra alla commissione di accreditamento, ai fini della formulazione del parere di cui all'articolo 5, comma 2, tutta la documentazione relativa alla domanda presentata ed alle verifiche svolte, ivi comprese quelle espletate ai sensi dell'articolo 6. Entro 30 giorni dalla ricezione di detta documentazione la commissione di accreditamento esprime un parere in merito all'idoneità del richiedente ad effettuare i compiti previsti dall'accreditamento, nonché sugli eventuali motivi ostativi di cui all'articolo 9, comma 6, e lo trasmette al CVCN;

e) rilascio o diniego dell'accreditamento:

1) il CVCN, acquisito il parere della commissione di accreditamento, in caso di valutazione positiva, rilascia al richiedente il certificato di accreditamento, che ha dura-



ta triennale ed è rinnovabile. In caso di valutazione negativa il CVCN comunica al laboratorio di prova richiedente un motivato diniego all'accoglimento dell'istanza ai sensi dell'articolo 10-*bis* della legge 7 agosto 1990, n. 241;

2) il certificato di accreditamento riporta il nome e l'indirizzo dell'organizzazione accreditata, nonché l'area di accreditamento.

2. Qualora, in qualunque fase del procedimento, il laboratorio di prova comunichi di rinunciare all'accreditamento o non fornisca riscontro alle richieste nei termini previsti, il CVCN procede all'archiviazione dell'istanza.

3. Il CVCN conclude la procedura di accreditamento entro 180 giorni dalla ricezione della domanda di accreditamento.

4. Nei casi di cui al comma 1, lettera *a)*, numeri 2) e 3), lettera *b)*, numero 2), lettera *c)*, numero 4), e lettera *e)*, numero 1), il termine di cui al comma 3 è sospeso fino all'acquisizione della documentazione richiesta.

Art. 13.

Obblighi dei LAP

1. Ai fini del mantenimento dell'accreditamento, i LAP sono tenuti a:

a) operare sulla base di quanto previsto nelle determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*;

b) informare tempestivamente il CVCN di qualsiasi variazione concernente le informazioni presentate a corredo della domanda di accreditamento quali variazioni dell'assetto societario, del personale autorizzato ad accedere alle informazioni, necessarie per lo svolgimento delle attività di *test* del laboratorio di prova, individuate nella determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 5), della sede del laboratorio di prova, nonché di elementi che comportano l'emissione di una nuova versione del manuale della qualità;

c) trasmettere il rapporto di prova al CVCN entro i termini fissati;

d) svolgere le attività connesse all'accreditamento esclusivamente presso la sede collocata sul territorio nazionale e indicata nella domanda di accreditamento;

e) assicurare adeguata formazione al proprio personale ai fini del rispetto dell'impegno di non divulgazione di cui agli articoli 10, comma 1, lettera *h)*, e 11, comma 1, lettera *h)*;

f) fermo restando quanto previsto all'articolo 22, dare comunicazione al CVCN e all'eventuale CV interessato, qualora il LAP abbia trattato dati o sistemi inerenti quest'ultimo, di ogni limitazione della operatività superiore a 24 ore, entro le successive 24 ore. Le modalità di notifica saranno indicate nelle determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*.

2. È fatto obbligo a coloro che ne vengano a conoscenza nell'ambito dello svolgimento delle attività per le quali il laboratorio di prova è accreditato, quale dovere inerente alla funzione o al servizio, di non rivelare a terzi, direttamente o indirettamente, informazioni, cognizioni, documenti, esperienze tecnico-industriali e dati tecnici relativi alle suddette attività. Al fine di assicurare il rispetto dell'obbligo di cui al presente comma e dell'impegno di non divulgazione di cui agli articoli 10, comma 1, lettera *h)*, e 11, comma 1, lettera *h)*, il LAP adotta adeguate misure di sicurezza ed esercita opportune attività di vigilanza.

Art. 14.

Vigilanza sull'attività dei LAP

1. Il CVCN dispone l'effettuazione di verifiche con cadenza periodica al massimo ogni 18 mesi, per la verifica del mantenimento dei requisiti di accreditamento.

2. Il CVCN può effettuare visita ispettiva a campione per la verifica del soddisfacimento delle condizioni per il mantenimento dell'accreditamento.

3. Il CVCN, con almeno due mesi di anticipo rispetto alla data fissata, comunica al LAP la data programmata per la visita ispettiva di vigilanza, richiedendo un'eventuale integrazione della documentazione qualora siano intervenute variazioni che abbiano comportato la necessità della revisione della documentazione di sistema.

4. Il personale incaricato, dopo aver effettuato la verifica della documentazione, effettua l'ispezione presso il LAP al fine di valutarne i requisiti previsti.

5. Al termine dell'ispezione il personale incaricato trasmette al CVCN il rapporto di verifica relativo al mantenimento dei requisiti del LAP con riferimento all'area di accreditamento.

6. Nel caso in cui la verifica effettuata dal personale incaricato dia esito positivo il CVCN comunica il risultato al LAP.

7. Nel caso in cui la verifica effettuata dal personale incaricato dia esito negativo, il CVCN comunica il risultato al LAP, fissando eventualmente modalità e termini per la rimozione delle non conformità come indicato nell'articolo 15.

Art. 15.

Sospensione e revoca dell'accreditamento

1. Qualora sia dimostrato il mancato rispetto degli obblighi di cui all'articolo 13 e di cui all'articolo 22, il CVCN, sentita la commissione di accreditamento, intima al LAP non più conforme di porre in essere, entro il termine di 10 giorni, le misure necessarie ai fini del superamento delle difformità riscontrate. Qualora entro il termine fissato il laboratorio non abbia apportato le richieste azioni correttive, l'accreditamento è sospeso. Decorsi tre mesi dalla disposizione della sospensione senza che siano state rimosse le difformità, l'accreditamento è revocato.

2. In caso di non conformità riguardante gli obblighi di cui alla lettera *a)*, con riferimento alle misure di sicurezza indicate dal CVCN, e alle lettere *c)* e *f)* del comma 1 dell'articolo 13, nonché l'obbligo di cui al comma 1 dell'articolo 22, il CVCN, sentita la commissione di accreditamento, può disporre con provvedimento motivato la revoca dell'accreditamento.

Art. 16.

Rinnovo dell'accreditamento

1. Entro sei mesi antecedenti la scadenza del certificato di accreditamento, il LAP può presentare al CVCN richiesta di rinnovo dell'accreditamento per un ulteriore triennio, eventualmente integrando la documentazione qualora siano intervenute variazioni che abbiano comportato la necessità della revisione della documentazione.

2. Il CVCN esamina la domanda e dispone una visita ispettiva per la verifica della sussistenza dei requisiti richiesti per l'accreditamento. Nel caso in cui il personale incaricato esprima avviso favorevole, il CVCN, sentita la commissione accreditamento, rilascia il certificato di rinnovo dell'accreditamento.

3. Nel caso in cui il personale incaricato non esprima avviso favorevole, il CVCN comunica il risultato al LAP, fissando modalità e termini per la rimozione delle non conformità riscontrate, ove eliminabili.

4. In caso di non conformità non eliminabili, sentita la commissione accreditamento, il CVCN non rinnova l'accreditamento.

Art. 17.

Variazione dell'area di accreditamento

1. Il LAP può presentare domanda di estensione dell'accreditamento ad altre aree, in coincidenza con il termine di cui all'articolo 14, comma 1, ed in fase di rinnovo di cui all'articolo 16. L'istanza è considerata alla stregua di una domanda di accreditamento con l'esclusione delle verifiche di cui all'articolo 12, comma 1, lettera *a)*.

2. Il LAP può chiedere di ridurre la portata dell'area di accreditamento di cui all'articolo 7.

Art. 18.

Responsabilità

1. I LAP sono responsabili delle loro attività, dei risultati delle prove che hanno effettuato e dei rapporti di prova che hanno rilasciato.

Art. 19.

Corrispettivi

1. L'accreditamento e la vigilanza effettuati dal CVCN avvengono a titolo oneroso. Ai fini del calcolo dei relativi compensi, nelle more dell'adozione di una specifica determinazione tecnica adottata dall'Agenzia in attuazione del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, si applica l'articolo 3 del decreto del Ministero delle comunicazioni 15 febbraio 2006, pubblicato nella *Gazzetta ufficiale* n. 82 del 7 aprile 2006, recante individuazioni delle prestazioni, eseguite dal Ministero delle comunicazioni per conto terzi, ai sensi dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366.

2. Copia della attestazione del versamento deve essere trasmessa al CVCN.

Capo III

ACCREDITAMENTO DEI CV

Art. 20.

Accreditamento dei CV

1. Ai fini del presente decreto, i CV sono accreditati, ai sensi dell'articolo 1, commi 6, lettera *a)*, e 7, lettera *b)*, del decreto-legge, per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note relativamente alle forniture di beni, sistemi e servizi ICT da impiegare sulle reti, sui sistemi informativi e sui servizi informatici, individuati ai sensi dell'articolo 1, comma 2, lettera *b)*, del decreto-legge, dei rispettivi Ministeri, conformemente alle metodologie di verifica e di *test* definite dal CVCN.

2. Il CVCN procede all'accreditamento dei CV sulla base della comunicazione effettuata, tramite posta elettronica certificata, o altro servizio elettronico di recapito certificato qualificato, dai Ministeri dell'interno e della difesa, ciascuno nell'ambito di rispettiva competenza.

3. Ai fini dell'accreditamento, il CV emette una dichiarazione di conformità ai requisiti di cui all'articolo 8, comma 3, ed ai requisiti soggettivi di cui all'articolo 9, comma 1, e comunica al CVCN:

a) l'indirizzo della sede del laboratorio in cui verranno eseguite le prove;

b) la direzione generale/ente presso cui è istituito il CV;

c) il manuale della qualità e le misure di sicurezza attuate, con riferimento all'articolo 4, comma 1, lettera *e)*, numero 2).

Capo IV

RACCORDI CON IL CVCN

Art. 21.

Raccordi

1. Il CVCN assicura i raccordi con:

a) i CV, per verificare se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni con l'obiettivo di assicurare il coordinamento delle attività e garantire la massima convergenza e non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio. I CV e il CVCN alimentano e consultano la piattaforma informatica di cui all'articolo 4, comma 1, lettera *h)*, conformemente alle modalità indicate dall'articolo 6 del DPR;

b) i LAP, per affidare l'esecuzione dei *test* di cui all'articolo 5, comma 3, del DPR al LAP o ai LAP, nei casi in cui il CVCN intenda avvalersene ai sensi dell'articolo 4, comma 7, del medesimo DPR. Il CVCN e i LAP si raccordano secondo le modalità di cui all'articolo 7 del DPR;

c) i CV e i LAP, per affidare l'esecuzione dei *test* al LAP o ai LAP nei casi in cui i CV ritengano di non poter svolgere autonomamente i *test* di cui all'articolo 5, comma 3, del DPR. In tal caso, i CV comunicano l'esi-

genza al CVCN, fornendo le necessarie informazioni, tra cui quelle relative ai LAP di cui intendono avvalersi. Il CVCN affida, ai sensi dell'articolo 6, comma 4, lettera *a)*, del DPR, l'esecuzione dei *test* al LAP o ai LAP indicati dai CV e comunica l'avvio dei *test* al soggetto incluso nel perimetro e al fornitore. L'esecuzione dei *test* avviene conformemente all'articolo 7 del DPR. Al termine dei *test* il LAP o i LAP incaricati trasmettono al CVCN, previa verifica ed eventuale espunzione da parte del CV richiedente in caso di esistenza di dati non divulgabili ai fini della tutela della sicurezza nazionale, il rapporto di prova entro i termini fissati dall'articolo 7, comma 7, del DPR. Il CVCN inserisce la documentazione di sintesi relativa ai rapporti di prova nella piattaforma informatica di cui all'articolo 4, comma 1, lettera *h)*. I CV redigono il rapporto di valutazione conformemente all'articolo 8 del DPR.

2. Il CVCN assicura i raccordi di cui al comma 1 attraverso la piattaforma informatica di cui all'articolo 4, comma 1, lettera *h)*.

3. Il CVCN, con la determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 8), disciplina le modalità esecutive delle comunicazioni con i CV ed i termini tecnici ed organizzativi mediante i quali i raccordi trovano effettiva applicazione. Il CVCN con la determinazione tecnica di cui all'articolo 4, comma 1, lettera *e)*, numero 9), disciplina le modalità esecutive delle comunicazioni con i LAP ed i termini tecnici ed organizzativi mediante i quali i raccordi trovano effettiva applicazione.

4. Le determinazioni tecniche di cui all'articolo 4, comma 1, lettera *e)*, sono aggiornati ogni qualvolta l'evoluzione delle valutazioni e delle prove lo richiede.

Capo V
NOTIFICA DEGLI INCIDENTI

Art. 22.
Notifica degli incidenti

1. Il CVCN, i CV e i LAP, al verificarsi di un incidente sulle reti, sui sistemi informativi e sui servizi informatici di pertinenza deputati allo svolgimento delle funzioni oggetto dell'accreditamento, in termini di compromissione della integrità o riservatezza dei dati e delle informazioni trattati, procedono alla notifica al CSIRT Italia secondo le modalità indicate dal CSIRT stesso entro il termine di sei ore dal momento in cui sono venuti a conoscenza dell'incidente.

2. Qualora il CVCN, i CV o i LAP vengano a conoscenza di nuovi elementi significativi, tra cui le specifiche vulnerabilità sfruttate, la rilevazione di eventi comunque correlati all'incidente oggetto di notifica, ovvero gli indicatori di compromissione (IOC) rilevati, la notifica di cui al comma 1 è integrata tempestivamente dal momento in cui ne sono venuti a conoscenza, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

3. Su richiesta del CSIRT Italia, il CVCN, i CV o i LAP che hanno proceduto a effettuare una notifica ai sensi dei commi 1 e 2 provvedono, secondo le modalità indicate dal CSIRT stesso, ed entro sei ore dalla richiesta, a effettuare un aggiornamento della notifica, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

4. I CV e i LAP assicurano che dell'avvenuta notifica sia fornita notizia al CVCN, nonché, nel caso di notifica da parte del LAP, all'eventuale CV interessato, qualora i LAP abbiano trattato dati o sistemi inerenti a quest'ultimo.

Capo VI
DISPOSIZIONI FINANZIARIE

Art. 23.
Clausola di invarianza

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. L'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

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

Roma, 18 maggio 2022

Il Presidente: DRAGHI

Visto, *il Guardasigilli:* CARTABIA

Registrato alla Corte dei conti l'11 luglio 2022
Ufficio di controllo sugli atti della Presidenza del Consiglio, del Ministero della giustizia e del Ministero degli affari esteri, reg.ne n. 1785

NOTE

AVVERTENZA:

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

Note alle premesse

— La legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri), è pubblicata nella *Gazzetta Ufficiale* 12 settembre 1988, n. 214, S.O. n. 86.

— Si riporta il testo dell'articolo 1, comma 7, lett. *b)*, del decreto-legge 21 settembre 2019, n. 105 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica), pubblicato nella *Gazzetta Ufficiale* 21 settembre 2019, n. 222, e convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. – 6. (*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) (*omissis*);

b) ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attività di cui al comma 6, lettera *a)*, dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del CIC, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni. Con lo stesso decreto sono altresì stabiliti i raccordi, ivi compresi i contenuti, le modalità e i termini delle comunicazioni, tra il CVCN e i predetti laboratori, nonché tra il medesimo CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa, di cui al comma 6, lettera *a)*, anche la fine di assicurare il coordinamento delle rispettive attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesimi condizioni e livelli di rischio;».

— Si riporta il testo dell'articolo 16 della legge 1° aprile 1981, n. 121 (Nuovo ordinamento dell'Amministrazione della pubblica sicurezza), pubblicato nella *Gazzetta Ufficiale* 10 aprile 1981, n. 100, S.O:

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

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

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

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

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

— Il decreto legislativo 8 giugno 2001, n. 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300), è pubblicato nella *Gazzetta Ufficiale* 19 giugno 2001, n. 140.

— Si riporta il testo dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366 (Modifiche ed integrazioni al decreto legislativo 30 luglio 1999, n. 300, concernenti le funzioni e la struttura organizzativa del Ministero delle comunicazioni, a norma dell'articolo 1 della legge 6 luglio 2002, n. 137), pubblicato nella *Gazzetta Ufficiale* 8 gennaio 2004, n. 5:

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

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

— Si riporta il testo dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196 (Legge di contabilità e finanza pubblica), pubblicata nella *Gazzetta Ufficiale* 31 dicembre 2009, n. 303, S.O. n. 245:

«Art. 1 *(Principi di coordinamento e ambito di riferimento)*. — 1. - 2. (*omissis*)

3. La ricognizione delle amministrazioni pubbliche di cui al comma 2 è operata annualmente dall'ISTAT con proprio provvedimento e pubblicata nella *Gazzetta Ufficiale* entro il 30 settembre.».

— Il decreto-legge 14 giugno 2021, n. 82 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), è pubblicato nella *Gazzetta Ufficiale* 14 giugno 2021, n. 140, e convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

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

— Il decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 (Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133), è pubblicato nella *Gazzetta Ufficiale* 23 aprile 2021, n. 97.

— Il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81 (Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza), è pubblicato nella *Gazzetta Ufficiale* 11 giugno 2021, n. 138.

Note all'art. 1:

— Si riporta il testo dell'articolo 1, commi 1 e 2-*bis*, del citato decreto-legge 21 settembre 2019, n. 105 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica):

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica.

2. (*omissis*).

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

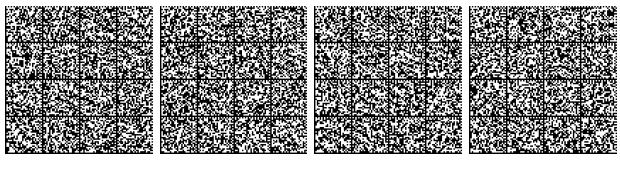
— Per il decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 1, comma 6, del citato decreto-legge 21 settembre 2019, n. 105:

«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) 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 modalità stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera *b)*. Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera *b)*, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati;

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

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

— Si riporta il testo dell'articolo 2, comma 1, lettera *vv)*, del decreto legislativo 1º agosto 2003, n. 259 (Codice delle comunicazioni elettroniche), pubblicato nella *Gazzetta Ufficiale* 15 settembre 2003, n. 214, S.O. n. 150:

«Art. 2 *(Definizioni)* (ex art. 2 eecc e art. 1 Codice 2003). — 1. Ai fini del presente decreto si intende per:

a) – uu) (*omissis*)

vv). reti di comunicazione elettronica: i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;».

— Si riporta il testo dell'articolo 3, comma 1, lettera *aa)*, del decreto legislativo 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione), pubblicato nella *Gazzetta Ufficiale* 9 giugno 2018, n. 132:

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

a) – z) (*omissis*)

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

— Si riporta il testo dell'articolo 7 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):

«Art. 7 *(Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici)*. — 1. Ai sensi dell'articolo 1, comma 2, del decreto-legge, i soggetti inclusi nel perimetro predispongono e aggiornano, con cadenza almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono, osservando i criteri individuati nel successivo comma.

2. Ricevuta la comunicazione prevista dall'articolo 1, comma 2-*bis*), secondo periodo, del decreto-legge, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale di cui all'articolo 4, comma 1, lettera *c)*, provvedono:

a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati:

1) l'impatto di un incidente sul bene ICT, in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali;

2) le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione;

b) a predisporre l'elenco dei beni ICT di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge. In fase di prima applicazione e fino all'aggiornamento del presente decreto, ai sensi dell'articolo 1,

comma 5, del decreto-legge, sono individuati, all'esito dell'analisi del rischio, in ossequio al principio di gradualità, i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

3. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate si applica quanto previsto dall'articolo 1, comma 2, lettera *b)*, del decreto-legge.».

— Si riporta il testo dell'articolo 1, comma 2, del citato decreto-legge 21 settembre 2019, n. 105:

«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) sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell'individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

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

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;

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

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.».

— Per il decreto del Presidente del Consiglio dei ministri 15 giugno 2021 si veda nelle premesse.

— Si riporta il testo dell'articolo 13 del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 (Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133):

«Art. 13 *(Criteri tecnici per l'individuazione delle categorie)*. — 1. Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate sulla base dell'esecuzione o svolgimento delle seguenti funzioni:

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

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

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

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

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

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

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

— Per il decreto-legge 14 giugno 2021, n. 82 si veda nelle note alle premesse.

— Per il testo dell'articolo 1, comma 7, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105 si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 5, comma 3, dell'articolo 7 e dell'articolo 8, commi 1 e 2, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54:

«Art. 5 *(Verifiche preliminari, individuazione di condizioni e test)*. — 1.-2. (*omissis*).

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

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

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

«Art. 7 *(Esecuzione dei test)*. — 1. Concluse le attività preliminari di cui all'articolo 6, il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel perimetro e al fornitore. I test si concludono entro i termini individuati dall'articolo 4, comma 5.

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

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

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

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

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

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

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

«Art. 8 *(Esito della valutazione e prescrizioni di utilizzo)*. — 1. Sulla base del rapporto di prova di cui all'articolo 7, commi 6 e 7, il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test. Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro i termini di cui all'articolo 4, comma 5.

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

— Per il testo dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196 si veda nelle note alle premesse.

— Si riporta il testo vigente dell'articolo 8 del citato decreto legislativo 18 maggio 2018, n. 65:

«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.

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.».

Note all'art. 2:

— Per il testo dell'articolo 1, comma 7, lett. *b)*, del decreto-legge 21 settembre 2019, n. 105 si veda nelle note alle premesse.

— Per il testo dell'articolo 5, comma 3, e dell'articolo 7, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 si veda nelle note all'articolo 1.

Note all'art. 4:

— Per il testo dell'articolo 5, comma 3, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 si veda nelle note all'articolo 1.

— Si riporta il testo dell'articolo 5, comma 4 e dell'articolo 6, commi 1 e 6, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54:

«Art. 5 *(Verifiche preliminari, individuazione di condizioni e test)*. — 1.-3. (*omissis*)

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

«Art. 6 *(Preparazione all'esecuzione dei test)*. — 1. A seguito della comunicazione di cui al comma 9 dell'articolo 5, il CVCN e i CV verificano, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni, secondo le modalità dell'articolo 7. Nel caso in cui:

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

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

2.-5. (*omissis*)

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

Note all'art. 6:

— Per il testo dell'articolo 16 della legge 1° aprile 1981, n. 121 si veda nelle note alle premesse.

Note all'art. 8:

— Per il testo dell'articolo 1, comma 7, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105 si veda nelle note alle premesse.

Note all'art. 9:

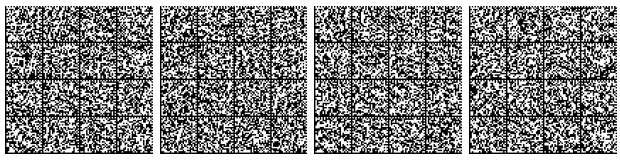
— Si riporta il testo dell'art. 444 del Codice di procedura penale, approvato con decreto del Presidente della Repubblica 22 settembre 1998, n. 447, pubblicato nella *Gazzetta Ufficiale* 24 ottobre 1988, n. 250, S.O n. 92:

«Art. 444 *(Applicazione della pena su richiesta)*. — 1. L'imputato e il pubblico ministero possono chiedere al giudice l'applicazione, nella specie e nella misura indicata, di una sanzione sostitutiva o di una pena pecuniaria, diminuita fino a un terzo, ovvero di una pena detentiva quando questa, tenuto conto delle circostanze e diminuita fino a un terzo, non supera cinque anni soli o congiunti a pena pecuniaria.

1-*bis*. Sono esclusi dall'applicazione del comma 1 i procedimenti per i delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater*, i procedimenti per i delitti di cui agli articoli 600-*bis*, 600-*ter*, primo, secondo, terzo e quinto comma, 600-*quater*, secondo comma, 600-*quater*.1, relativamente alla condotta di produzione o commercio di materiale pornografico, 600-*quinquies*, nonché 609-*bis*, 609-*ter*, 609-*quater* e 609-*octies* del codice penale, nonché quelli contro coloro che siano stati dichiarati delinquenti abituali, professionali e per tendenza, o recidivi ai sensi dell'articolo 99, quarto comma, del codice penale, qualora la pena superi due anni soli o congiunti a pena pecuniaria.

1-*ter*. Nei procedimenti per i delitti previsti dagli articoli 314, 317, 318, 319, 319-*ter*, 319-*quater* e 322-*bis* del codice penale, l'ammissibilità della richiesta di cui al comma 1 è subordinata alla restituzione integrale del prezzo o del profitto del reato.

2. Se vi è il consenso anche della parte che non ha formulato la richiesta e non deve essere pronunciata sentenza di proscioglimento a norma dell'articolo 129, il giudice, sulla base degli atti, se ritiene corrette la qualificazione giuridica del fatto, l'applicazione e la comparazione delle circostanze prospettate dalle parti, nonché congrua la pena indicata, ne dispone con sentenza l'applicazione enunciando nel dispositivo che vi è stata la richiesta delle parti. Se vi è costituzione di parte civile, il giudice non decide sulla relativa



domanda; l'imputato è tuttavia condannato al pagamento delle spese sostenute dalla parte civile, salvo che ricorrano giusti motivi per la compensazione totale o parziale. Non si applica la disposizione dell'articolo 75, comma 3. Si applica l'articolo 537-*bis*.

3. La parte, nel formulare la richiesta, può subordinarne l'efficacia, alla concessione della sospensione condizionale della pena. In questo caso il giudice, se ritiene che la sospensione condizionale non può essere concessa, rigetta la richiesta.

3-*bis*. Nei procedimenti per i delitti previsti dagli articoli 314, primo comma, 317, 318, 319, 319-*ter*, 319-*quater*, primo comma, 320, 321, 322, 322-*bis* e 346-*bis* del codice penale, la parte, nel formulare la richiesta, può subordinarne l'efficacia all'esenzione dalle pene accessorie previste dall'articolo 317-*bis* del codice penale ovvero all'estensione degli effetti della sospensione condizionale anche a tali pene accessorie. In questi casi il giudice, se ritiene di applicare le pene accessorie o ritiene che l'estensione della sospensione condizionale non possa essere concessa, rigetta la richiesta.».

— Si riporta il testo vigente dell'articolo 80, comma 1, del decreto legislativo 18 aprile 2016, n. 50 (Codice dei contratti pubblici), pubblicato nella *Gazzetta Ufficiale* 19 aprile 2016, n. 91, S.O. n. 10:

«Art. 80 *(Motivi di esclusione)*. —1. Costituisce motivo di esclusione di un operatore economico dalla partecipazione a una procedura d'appalto o concessione, la condanna con sentenza definitiva o decreto penale di condanna divenuto irrevocabile o sentenza di applicazione della pena su richiesta ai sensi dell'articolo 444 del codice di procedura penale per uno dei seguenti reati:

a) delitti, consumati o tentati, di cui agli articoli 416,416-*bis* del codice penale ovvero delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-*bis* ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti, consumati o tentati, previsti dall'articolo 74 del decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, dall'articolo 291-*quater* del decreto del Presidente della Repubblica 23 gennaio 1973, n. 43 e dall'articolo 260 del decreto legislativo 3 aprile 2006, n. 152, in quanto riconducibili alla partecipazione a un'organizzazione criminale, quale definita all'articolo 2 della decisione quadro 2008/841/GAI del Consiglio;

b) delitti, consumati o tentati, di cui agli articoli 317, 318, 319, 319-*ter*, 319-*quater*, 320, 321, 322, 322-*bis*, 346-*bis*, 353, 353-*bis*, 354, 355 e 356 del codice penale nonché all'articolo 2635 del codice civile;

b-*bis*) false comunicazioni sociali di cui agli articoli 2621 e 2622 del codice civile;

c) frode ai sensi dell'articolo 1 della convenzione relativa alla tutela degli interessi finanziari delle Comunità europee;

d) delitti, consumati o tentati, commessi con finalità di terrorismo, anche internazionale, e di eversione dell'ordine costituzionale reati terroristici o reati connessi alle attività terroristiche;

e) delitti di cui agli articoli 648-*bis*, 648-*ter* e 648-*ter*.1 del codice penale, riciclaggio di proventi di attività criminose o finanziamento del terrorismo, quali definiti all'articolo 1 del decreto legislativo 22 giugno 2007, n. 109 e successive modificazioni;

f) sfruttamento del lavoro minorile e altre forme di tratta di esseri umani definite con il decreto legislativo 4 marzo 2014, n. 24;

g) ogni altro delitto da cui derivi, quale pena accessoria, l'incapacità di contrattare con la pubblica amministrazione.».

— Si riporta il testo degli articoli 615-*bis*, 615-*ter*, 615-*quater*, 615-*quinquies*, 616, 617, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 617-*septies* 618, 619, 620, 621, 622, 623, 623-*bis* del codice penale:

«Art. 615-*bis (Interferenze illecite nella vita privata)*. — Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.

Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.».

«Art. 615-*ter (Accesso abusivo ad un sistema informatico o telematico)*. — Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.».

«Art. 615-*quater (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)*. — Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-*quater*.».

«Art. 615-*quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*. — Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.».

«Art. 616 *(Violazione, sottrazione e soppressione di corrispondenza)*. — Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.

Il delitto è punibile a querela della persona offesa.

Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.».

«Art. 617 *(Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche)*. — Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da un anno e sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo.

I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.».

«Art. 617-*bis (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche)*. — Chiunque, fuori dei casi consentiti dalla legge, al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti o parti di apparati o di strumenti idonei a intercettare, impedire o interrompere comunicazioni o conversazioni telefoniche o telegrafiche tra altre persone, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.».

«Art. 617-*ter (Falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche)*. — Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.».

«Art. 617-*quater (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)*. — Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.».

«Art. 617-*quinquies (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)*. — Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater*.».

«Art. 617-*sexies (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)*. — Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater*.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.».

«Art. 617-*septies (Diffusione di riprese e registrazioni fraudolente)*. — Chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni.

La punibilità è esclusa se la diffusione delle riprese o delle registrazioni deriva in via diretta ed immediata dalla loro utilizzazione in un procedimento amministrativo o giudiziario o per l'esercizio del diritto di difesa o del diritto di cronaca.

Il delitto è punibile a querela della persona offesa.».

«Art. 618 *(Rivelazione del contenuto di corrispondenza)*. — Chiunque, fuori dei casi preveduti dall'articolo 616, essendo venuto abusivamente a cognizione del contenuto di una corrispondenza a lui non diretta, che doveva rimanere segreta, senza giusta causa lo rivela, in tutto o in parte, è punito, se dal fatto deriva nocumento, con la reclusione fino a sei mesi o con la multa da euro 103 a euro 516.

Il delitto è punibile a querela della persona offesa.».

«Art. 619 *(Violazione, sottrazione e soppressione di corrispondenza commesse da persona addetta al servizio delle poste, dei telegrafi o dei telefoni)*. — L'addetto al servizio delle poste, dei telegrafi o dei telefoni, il quale, abusando di tale qualità, commette alcuno dei fatti preveduti dalla prima parte dell'articolo 616, è punito con la reclusione da sei mesi a tre anni.

Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, qualora il fatto non costituisca un più grave reato, con la reclusione da sei mesi a cinque anni e con la multa da euro 30 a euro 516.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa.».

«Art. 620 *(Rivelazione del contenuto di corrispondenza, commessa da persona addetta al servizio delle poste, dei telegrafi o dei telefoni)*. — L'addetto al servizio delle poste, dei telegrafi o dei telefoni, che, avendo notizia, in questa sua qualità, del contenuto di una corrispondenza aperta, o di una comunicazione telegrafica, o di una conversazione telefonica, lo rivela senza giusta causa ad altri che non sia il destinatario ovvero a una persona diversa da quelle tra le quali la comunicazione o la conversazione è interceduta, è punito con la reclusione da sei mesi a tre anni. Il delitto è punibile a querela della persona offesa.».

«Art. 621 *(Rivelazione del contenuto di documenti segreti)*. — Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.

Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.

Il delitto è punibile a querela della persona offesa.».

«Art. 622 *(Rivelazione di segreto professionale)*. —Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.

La pena è aggravata se il fatto è commesso da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci o liquidatori o se è commesso da chi svolge la revisione contabile della società.

Il delitto è punibile a querela della persona offesa.».

«Art. 623 *(Rivelazione di segreti scientifici o commerciali)*. — Chiunque, venuto a cognizione per ragioni del suo stato o ufficio, o della sua professione o arte, di segreti commerciali o di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, li rivela o li impiega a proprio o altrui profitto, è punito con la reclusione fino a due anni.

La stessa pena si applica a chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o altrui profitto.

Se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata.

Il colpevole è punito a querela della persona offesa.».

«Art. 623-*bis (Altre comunicazioni e conversazioni)*. — Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati.».

— Si riporta il testo dell'articolo 67 e dell'articolo 84, comma 4, del decreto legislativo 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della legge 13 agosto 2010, n. 136), pubblicato nella *Gazzetta Ufficiale* 28 settembre 2011, n. 226, S.O. n. 214:

«Art. 67 *(Effetti delle misure di prevenzione)*. — 1. Le persone alle quali sia stata applicata con provvedimento definitivo una delle misure di prevenzione previste dal libro I, titolo I, capo II non possono ottenere:

a) licenze o autorizzazioni di polizia e di commercio;

b) concessioni di acque pubbliche e diritti ad esse inerenti nonché concessioni di beni demaniali allorché siano richieste per l'esercizio di attività imprenditoriali;

c) concessioni di costruzione e gestione di opere riguardanti la pubblica amministrazione e concessioni di servizi pubblici;

d) iscrizioni negli elenchi di appaltatori o di fornitori di opere, beni e servizi riguardanti la pubblica amministrazione, nei registri della camera di commercio per l'esercizio del commercio all'ingrosso e nei registri di commissionari astatori presso i mercati annonari all'ingrosso;

e) attestazioni di qualificazione per eseguire lavori pubblici;

f) altre iscrizioni o provvedimenti a contenuto autorizzatorio, concessorio, o abilitativo per lo svolgimento di attività imprenditoriali, comunque denominati;

g) contributi, finanziamenti o mutui agevolati ed altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee, per lo svolgimento di attività imprenditoriali;

h) licenze per detenzione e porto d'armi, fabbricazione, deposito, vendita e trasporto di materie esplodenti.

2. Il provvedimento definitivo di applicazione della misura di prevenzione determina la decadenza di diritto dalle licenze, autorizzazioni, concessioni, iscrizioni, attestazioni, abilitazioni ed erogazioni di cui al comma 1, nonché il divieto di concludere contratti pubblici di lavori, servizi e forniture, di cottimo fiduciario e relativi subappalti e subcontratti, compresi i cottimi di qualsiasi tipo, i noli a caldo e le forniture con posa in opera. Le licenze, le autorizzazioni e le concessioni sono ritirate e le iscrizioni sono cancellate ed è disposta la decadenza delle attestazioni a cura degli organi competenti.

3. Nel corso del procedimento di prevenzione, il tribunale, se sussistono motivi di particolare gravità, può disporre in via provvisoria i divieti di cui ai commi 1 e 2 e sospendere l'efficacia delle iscrizioni, delle erogazioni e degli altri provvedimenti ed atti di cui ai medesimi commi. Il provvedimento del tribunale può essere in qualunque momento revocato dal giudice procedente e perde efficacia se non è confermato con il decreto che applica la misura di prevenzione.

4. Il tribunale, salvo quanto previsto all'articolo 68, dispone che i divieti e le decadenze previsti dai commi 1 e 2 operino anche nei confronti di chiunque conviva con la persona sottoposta alla misura di prevenzione nonché nei confronti di imprese, associazioni, società e consorzi di cui la persona sottoposta a misura di prevenzione sia amministratore o determini in qualsiasi modo scelte e indirizzi. In tal caso i divieti sono efficaci per un periodo di cinque anni.

5. Per le licenze ed autorizzazioni di polizia, ad eccezione di quelle relative alle armi, munizioni ed esplosivi, e per gli altri provvedimenti di cui al comma 1 le decadenze e i divieti previsti dal presente articolo possono essere esclusi dal giudice nel caso in cui per effetto degli stessi verrebbero a mancare i mezzi di sostentamento all'interessato e alla famiglia.

6. Salvo che si tratti di provvedimenti di rinnovo, attuativi o comunque conseguenti a provvedimenti già disposti, ovvero di contratti derivati da altri già stipulati dalla pubblica amministrazione, le licenze, le autorizzazioni, le concessioni, le erogazioni, le abilitazioni e le iscrizioni indicate nel comma 1 non possono essere rilasciate o consentite e la conclusione dei contratti o subcontratti indicati nel comma 2 non può essere consentita a favore di persone nei cui confronti è in corso il procedimento di prevenzione senza che sia data preventiva comunicazione al giudice competente, il quale può disporre, ricorrendone i presupposti, i divieti e le sospensioni previsti a norma del comma 3. A tal fine, i relativi procedimenti amministrativi restano sospesi fino a quando il giudice non provvede e, comunque, per un periodo non superiore a venti giorni dalla data in cui la pubblica amministrazione ha proceduto alla comunicazione.

7. Dal termine stabilito per la presentazione delle liste e dei candidati e fino alla chiusura delle operazioni di voto, alle persone sottoposte, in forza di provvedimenti definitivi, alla misura della sorveglianza speciale di pubblica sicurezza è fatto divieto di svolgere le attività di propaganda elettorale previste dalla legge 4 aprile 1956, n. 212, in favore o in pregiudizio di candidati partecipanti a qualsiasi tipo di competizione elettorale.

8. Le disposizioni dei commi 1, 2 e 4 si applicano anche nei confronti delle persone condannate con sentenza definitiva o, ancorché non definitiva, confermata in grado di appello, per uno dei delitti di cui all'articolo 51, comma 3-*bis*, del codice di procedura penale nonché per i reati di cui all'articolo 640, secondo comma, n. 1), del codice penale, commesso a danno dello Stato o di un altro ente pubblico, e all'articolo 640-*bis* del codice penale.».

«Art. 84 *(Definizioni)*. — 1. - 3. (*omissis*)

4. Le situazioni relative ai tentativi di infiltrazione mafiosa che danno luogo all'adozione dell'informazione antimafia interdittiva di cui al comma 3 sono desunte:

a) dai provvedimenti che dispongono una misura cautelare o il giudizio, ovvero che recano una condanna anche non definitiva per taluni dei delitti di cui agli articoli 353, 353-*bis*, 603-*bis*, 629, 640-*bis*, 644, 648-*bis*, 648-*ter* del codice penale, dei delitti di cui all'articolo 51, comma 3-*bis*, del codice di procedura penale e di cui all'articolo 12-*quinquies* del decreto-legge 8 giugno 1992, n. 306 convertito, con modificazioni, dalla legge 7 agosto 1992, n. 356;

b) dalla proposta o dal provvedimento di applicazione di taluna delle misure di prevenzione;

c) salvo che ricorra l'esimente di cui all'articolo 4 della legge 24 novembre 1981, n. 689, dall'omessa denuncia all'autorità giudiziaria dei reati di cui agli articoli 317 e 629 del codice penale, aggravati ai sensi dell'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, da parte dei soggetti indicati nella lettera *b)* dell'articolo 38 del decreto legislativo 12 aprile 2006, n. 163, anche in assenza nei loro confronti di un procedimento per l'applicazione di una misura di prevenzione o di una causa ostativa ivi previste;

d) dagli accertamenti disposti dal prefetto anche avvalendosi dei poteri di accesso e di accertamento delegati dal Ministro dell'interno ai sensi del decreto-legge 6 settembre 1982, n. 629, convertito, con modificazioni, dalla legge 12 ottobre 1982, n. 726, ovvero di quelli di cui all'articolo 93 del presente decreto;

e) dagli accertamenti da effettuarsi in altra provincia a cura dei prefetti competenti su richiesta del prefetto procedente ai sensi della lettera *d)*;

f) dalle sostituzioni negli organi sociali, nella rappresentanza legale della società nonché nella titolarità delle imprese individuali ovvero delle quote societarie, effettuate da chiunque conviva stabilmente con i soggetti destinatari dei provvedimenti di cui alle lettere *a)* e *b)*,

con modalità che, per i tempi in cui vengono realizzati, il valore economico delle transazioni, il reddito dei soggetti coinvolti nonché le qualità professionali dei subentranti, denotino l'intento di eludere la normativa sulla documentazione antimafia.».

— Per il decreto legislativo 8 giugno 2001, n. 231 si veda nelle note alle premesse.

— Per il testo dell'articolo 1, comma 6, lett. *a)* del citato decreto-legge 21 settembre 2019, n. 105 si veda nelle note all'articolo 1.

Note all'art. 10:

— Il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo *A)*), è pubblicato nella *Gazzetta Ufficiale* 20 febbraio 2001, n. 42, S.O. n. 30.

Note all'art. 11:

— Per il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 si veda nella nota all'articolo 10.

Note all'art. 12:

— Si riporta il testo dell'articolo 10-*bis*, della legge 7 agosto 1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi), pubblicata nella *Gazzetta Ufficiale* 18 agosto 1990, n. 192:

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

Note all'art. 19:

— Per il decreto-legge 14 giugno 2021, n. 82 si veda nelle note alle premesse.

— Per il testo dell'articolo 6 del decreto legislativo 30 dicembre 2003, n. 366 si veda nelle note alle premesse.

Note all'art. 20:

— Per il testo dell'articolo 1, comma 2, lett. *b)* e comma 6, lett. *a)* del citato decreto-legge 21 settembre 2019, n. 105 si veda nelle note all'articolo 1.

— Per il testo dell'articolo 1, comma 7, lett. *b)* del citato decreto-legge 21 settembre 2019, n. 105 si veda nelle note alle premesse.

Note all'art. 21:

— Si riporta il testo dell'articolo 4, comma 7, dell'articolo 6 e dell'articolo 8, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54:

«Art. 4 *(Procedimento di verifica e valutazione)*. — 1.-6. (*omissis*)

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

«Art. 6 *(Preparazione all'esecuzione dei test)*. — 1. A seguito della comunicazione di cui al comma 9 dell'articolo 5, il CVCN e i CV verificano, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se sono in corso valutazioni, secondo le modalità dell'articolo 7. Nel caso in cui:

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

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

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

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

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

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

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

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

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

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

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

«Art. 8 *(Esito della valutazione e prescrizioni di utilizzo)*. — 1. Sulla base del rapporto di prova di cui all'articolo 7, commi 6 e 7, il CVCN e i CV redigono il rapporto di valutazione contenente l'esito dei test. Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro i termini di cui all'articolo 4, comma 5.

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

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

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

— Per il testo dell'articolo 5, comma 3, e dell'articolo7, del citato decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 si veda nelle note all'articolo 1.

22G00099